

As per  
New  
Syllabus  
2017-18

# APPLIED MATHEMATICS - IV

Information Technology

S. E. Semester-IV

*G. V. Kumbhojkar*

*H. V. Kumbhojkar*



P. Jamnadas LLP.

**SYLLABUS**  
**Applied Mathematics - IV**  
**(Information Technology)**

**S. E. Semester - IV**

(University of Mumbai - Effective From June 2017)

---

**Prerequisite** (02 hrs.)  
Basic of Set, Permutations, Combination and Probability.

**Module 1 :Elements of Number Theory I** (06 hrs.)  
Modular Arithmetic, Divisibility and Euclid Algorithm, Primes and the Sieve of Eratosthenes, Testing for primes, Prime Number Theorem.

**Module 2 :Elements of Number Theory II** (06 hrs.)  
Euler's, Fermat's Little theorems, Congruences, Computing Inverse in Congruences, Legendre and Jacobi Symbols, Chinese Remainder Theorem.

**Module 3 :Probability** (08 hrs.)  
**Statistics** : Formal concept, Sample space, Outcomes, Events.  
**Random Variables** : Discrete & Continuous random variables, Expectation, Variance, Probability Density Function & Cumulative Density Function.  
Moments, Moment Generating Function.  
**Probability Distribution** : Binomial distribution, Poisson & Normal distribution.

**Module 4 :Sampling theory** (10 hrs.)  
Test of Hypothesis, Level of significance, Critical region, One Tailed and Two Tailed test, Test of significance for Large Samples : Means of the samples and test of significance of means of two large samples.  
Test of significance of small samples : Students  $t$ -distribution for dependent and independent samples.  
Chi-square test : Test of goodness of fit and independence of attributes, Contingency table.  
Correlation, Scattered diagrams, Karl Pearson's coefficient of correlation, Spearman's Rank correlation.  
Regression Lines.

**Module 5 :Graph & Groups Theory** (12 hrs.)  
Introduction to graphs, Graph terminology, Representing graphs and graph isomorphism, Connectivity, Euler's and Hamilton's paths, Planar graphs, Graph coloring, Introduction to trees, Application of trees.

Groups, Subgroups, Generators and evaluation of powers, Cosets and Lagrange's theorem, Permutation groups and Burnside's theorem, Isomorphism, Automorphisms, Homomorphism and normal subgroups, Rings, Integral domains and fields.

### Module 6 : Lattice theory

(08 h)  
Lattices and algebras systems, Principles of duality, Basic properties of algebraic systems defined by lattices, Distributive and complemented lattices, Boolean lattices and Boolean algebras, Uniqueness of finite Boolean expressions, Prepositional calculus.

Coding theory : Coding of binary information and error detection, Decoding and Error correction.



## 1. Preliminaries

Set Theory

(1) Inclusion relation

(6) Venn diagram

of A Set

Two Sets

(18) Product set

Permutation

(1) Inverse

(5) Partial

Restriction

Probability

(1) Independence

Probability

## 2. Principles of Mathematics

(1) Irrational numbers

Eratosthenes

## 3. Euclidean Algorithm

(1) Irreducibility

Euclid's algorithm

## 4. Modular Arithmetic

(1) Inverse

Congruence

Chinese remainder theorem

## 5. Solving Linear Equations

(1) Inverse

Symmetry

(7) Cramer's rule

Reciprocity

(11) Determinants

## 6. Rational Approximation

(1) Irrational

Variables

Variables

# **CONTENTS**

<b>1. Prerequisite</b>	<b>1-1 to 1-32</b>
<b>Set Theory :</b>	
(1) Introduction, (2) Notation, (3) Finite and Infinite Set, (4) Null Set, (5) Universal Set, (6) Venn-Euler Diagram, (7) Subsets, (8) Equality, (9) Operations on Sets, (10) Complement of A Set, (11) Union of Sets, (12) Intersection of Sets, (13) Disjoint Sets, (14) Difference of Two Sets, (15) Symmetric Difference ( $A \oplus B$ ), (16) Distribution, (17) De Morgan's Laws, (18) Class of Sets, (19) Power Set, (20) Partition of Sets, (21) Ordered Set, (22) Cartesian Product.	
<b>Permutation and Combination :</b>	
(1) Introduction, (2) Basic Rules, (3) Permutations, (4) Factorial Notation (Meaning of $n!$ ), (5) Permutations of Things not all Different, (6) Combinations, (7) Combinations with Restrictions (Conditional Combinations).	
<b>Probability :</b>	
(1) Introduction, (2) Theorems on Probability of Events, (3) Laws of Probability, (4) Conditional Probability, (5) Independent Events.	
<b>2. Prime Numbers</b>	<b>2-1 to 2-10</b>
(1) Introduction, (2) Divisibility, (3) Division Algorithm, (4) Prime Numbers, (5) Sieve of Eratosthenes, (6) The Prime Number Theorem,	
<b>3. Euclidean Algorithm</b>	<b>3-1 to 3-13</b>
(1) Introduction, (2) Greatest Common Divisor, (3) Additional Properties of Primes, (4) The Euclidean Algorithm, (5) Solving Diophantine Equations	
<b>4. Modular Arithmetic</b>	<b>4-1 to 4-37</b>
(1) Introduction, (2) Congruence, (3) Computing Inverse in Conguences, (4) Solving Linear Congruence $ax \equiv b \pmod{m}$ , (5) Fermat's Little Theorem, (6) Euler's Theorem, (7) The Chinese Remainder Theorem.	
<b>5. Solvability of Quadratic Congruences</b>	<b>5-1 to 5-36</b>
(1) Introduction, (2) Quadratic Residue, (3) Legendre Symbol, (4) Properties of Legendre Symbols, (5) Gauss' Lemma, (6) Solving $x^2 \equiv a \pmod{pq}$ using Chinese Remainder Theorem, (7) Quadratic Congruence with Composite Moduli (Continued), (8) The Law of Quadratic Reciprocity, (9) The Jacobi Symbol, (10) An Efficient Algorithm for Jacobi Symbols, (11) General Problem $ax^2 + bx + c \equiv 0 \pmod{p}$ .	
<b>6. Random Variables</b>	<b>6-1 to 6-51</b>
(1) Introduction (2) Random Variable (3) Probability Distribution of A Discrete Random Variable (4) Distribution Function of A Discrete Random Variable $X$ (5) Continuous Random Variable (6) Probability Density Function of A Continuous Random Variable (7) Continuous	

Distribution Function (8) Expectation (9) Expectation of A Random Variable (10) Expectation of A Function of A Random Variable  $X$  (11) Mean and Variance (12) Moments (13) Moment Generating Function.

## 7. Some Standard Distributions

7-1 to 7-71

(1) Introduction (2) Binomial Distribution (3) Poisson Distribution (4) Normal Distribution.

## 8. Large Sample Tests

8-1 to 8-19

(1) Introduction (2) Methods of Sampling (3) Central Limit Theorem (4) Sampling Distribution of Means ( $\sigma$  known) (5) Critical Region (6) Procedure of Testing A Hypothesis (7) Errors in Testing of Hypothesis (8) Sampling of Variables (9) Testing the Hypothesis that the Population Mean =  $\mu$  (10) Testing the Difference Between Means.

## 9. Small Sample Tests

9-1 to 9-45

(1) Introduction (2) Student's  $t$  - distribution (3) Properties of  $t$  - distribution (4) Distribution of Sample Mean (5) Testing The Hypothesis That The Population Mean is  $\mu$  (6) Testing The Difference Between Means (7) Non-parametric Tests (8) Definition of  $\chi^2$  (9) Degrees of Freedom (10) Conditions for  $\chi^2$  Test (11) Yate's Correction (12) Uses of  $\chi^2$  Test (13) Hypothesis Concerning Several Proportions.

## 10. Correlation

10-1 to 10-23

(1) Introduction (2) Types of Correlation (3) Scatter Diagram (4) Karl Pearson's Coefficient of Correlation (5) Interpretation of the Coefficient of Correlation (6) Computation of Coefficient of Correlation : (*Ungrouped Data*) (7) Direct Method of Calculating Coefficient of Correlation (8) Spearman's Rank Correlation.

## 11. Regression

11-1 to 11-26

(1) Introduction (2) Lines of Regression (3) The Method of Scatter Diagram (4) The Method of Least Square (5) Calculations of the Equations of the Lines of Regression (6) Regression Coefficients (7) Properties of Coefficients of Regression.

## 12. Graphs

12-1 to 12-26

(1) Introduction, (2) Basic Terms, (3) Adjacency And Incidence, (4) Types of Graphs, (5) Isomorphism.

## 13. Eulerian and Hamiltonian Graphs

13-1 to 13-19

(1) Introduction, (2) Definitions, (3) Euler's Theorem, (4) Hamiltonian Graph, (5) Travelling Salesperson Problem (T.S.P.).

## 14. Trees

14-1 to 14-13

(1) Introduction, (2) Isomorphism of Trees, (3) Some Properties of Trees, (4) Rooted Trees, (5) Properties of Binary Trees, (6) Height of a Binary Tree, (7) Prefix Code, (8) Coding and Decoding of a Message.

<b>15. Planar Graphs</b>	<b>15-1 to 15-14</b>
(1) Introduction, (2) Maps And Regions, (3) Euler's Formula, (4) Planar Graphs, (5) Graph Colouring, (6) Rules of Chromatic Numbers, (7) Welch-Powell Algorithm.	
<b>16. Some Algebraic Structures</b>	<b>16-1 to 16-66</b>
(1) Introduction, (2) Binary Operation, (3) Properties of Binary Operations, (4) Semi-Group, (5) Monoid, (6) Isomorphism, Automorphism And Homo-morphism, (7) Group, (8) Generators and Evaluation of Powers, (9) Cosets and Lagrange's Theorem, (10) Permutation Groups and Bunsides Theorem, (11) Elementary Properties of a Group, (12) Isomorphism and Homomorphism, (13) Ring, (14) Integral Domain, (15) Field.	
<b>17. Equivalence Relations and Posets</b>	<b>17-1 to 17-42</b>
(1) Introduction, (2) Cartesian Product, (3) Partition of a Set, (4) Relation, (5) Diagram of a Relation, (6) Matrix of a Relation, (7) Digraph of a Relation, (8) Types of Relations, (9) Properties of Relations, (10) Symmetric, Asymmetric And Anti-symmetric Relations, (11) Transitive Relations, (12) Equivalence Relations, (13) Partially Ordered Sets (Posets), (14) Hasse Diagram, (15) Dual of Poset, (16) Extremal Elements of Posets,	
<b>18. Lattices</b>	<b>18-1 to 18-39</b>
(1) Introduction, (2) Lattices, (3) Dual in a Lattice, (4) Special Types of Lattices, (5) Boolean Lattice and Boolean Algebra, (6) Finite Boolean Algebra, (7) Propositional Calculus.	
<b>19. Coding Theory</b>	<b>19-1 to 19-21</b>
(1) Coding : Introduction, (2) Group Codes, Decoding and Error Correction, (3) Mod-2 Boolean Product, (4) Maximum Likelihood Decoding Technique.	
◆ <b>Statistical Tables</b>	<b>3</b>
◆ <b>A List of Primes</b>	<b>2</b>
◆ <b>Values of Euler's Phi-Functions</b>	<b>1</b>
◆ <b>Index of Biographical Sketches</b>	<b>1</b>
<b>Total pages</b>	<b>610</b>



# Prerequisite

## SET THEORY

### 1. Introduction

You have already studied set theory to some extent. Here, we shall take a brief review of what you have learnt.

A set is a collection having the property that given 'anything' we can say whether 'that thing' is in the set or not. Although a **set is an undefined term**, given an element we should be able to say whether the element is in the set or not. The edifice of modern mathematics rests on the concept of 'Sets'. The pioneering work on set theory was done by German Mathematician George Cantor (1845-1918).

#### Georg Cantor (1845 - 1918)



The eminent German mathematician was born in St. Petersburg. His father a successful merchant and broker wanted his son to be an engineer. But Georg Cantor pursued his studies in Mathematics and got his Ph.D. from Berlin University at the age of 22 in number theory. In 1869 he started his career as an unsalaried lecturer at University of Halle and published his revolutionary work on set theory five years later. Deeply religious, Cantor took deep interest in art, music and philosophy.

Bertrand Russel, another well known mathematician and philosopher, described him as "one of the greatest intellect of the nineteenth century". Although his theory is now used in many theoretical and practical fields, in his own time it was not accepted by contemporary mathematicians. This intensified his manic depression and he died in a mental hospital in Halle in 1918.

### 2. Notation

Consider a set  $A$  whose members are 2, 3, 6, 8. The fact that 2 is in the set is stated as **2 belongs to A** and is written symbolically as  $2 \in A$ . The fact that 5 is not in the set is stated as **5 does not belong to A** and is written as  $5 \notin A$ .

We usually denote elements of sets by small letters  $a, b, c, \dots, x, y, z$  and sets by capital letters  $A, B, C, \dots, X, Y, Z$ . If  $x$  is an element and  $A$  is a set, the statement that  $x$  is an element of  $A$  (or  $x$  belongs to  $A$ ) is denoted by  $x \in A$ . The statement that  $x$  is not an element of  $A$  (or  $x$  does not belong to  $A$ ) is denoted by  $x \notin A$ .

**Designation of a set :** There are two standard notations for designating a particular set (i) List form and (ii) Property form.

## Applied Mathematics - IV

(a) **List Form**  
Whenever possible we specify the set by listing the elements of the set in braces. Thus, a set whose elements are  $a, b, c, d$  is denoted by  $\{a, b, c, d\}$ . The set of week days can be denoted as  $D = \{\text{SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY}\}$ .

It may be noted that the order in which elements of the set are written is not important. With this convention, the sets  $\{a, b, c, d\}, \{b, c, d, a\}, \{a, c, b, d\}$  are the same. Further if an element occurs more than once in a set, it is treated once only. The set  $\{x, x\}$  does not have two elements, the set  $\{a, a, a\}$  does not have three elements. Both the sets have one element each.

(b) **Property Form**

The method of listing all the elements of a set is obviously inconvenient if there are large number of elements. In many circumstances it is even unworkable. If there are infinite elements in the set obviously we cannot list all of them. Under these circumstances we denote the set by stating a property which is possessed by all the elements of the set. We usually use the letter  $x$  to represent an arbitrary element. If the property is  $P(x)$  then the set of elements  $x$  which possess the property  $P(x)$  is denoted by  $\{x | P(x)\}$ , it is read as the set of  $x$  such that  $x$  satisfies the property  $P(x)$ . Thus, the set of all irrational numbers can be denoted as  $B = \{x | x \text{ is real and irrational}\}$ . We read this as the set of all  $x$  such that  $x$  is real and irrational.

A set containing only one element is called a **singleton set** or a **unit set**. Thus,  $A = \{a\}$  or  $B = \{x | x \text{ is the positive root of } x^2 - x - 6 = 0\}$  or  $C = \{\text{The present principal of a college}\}$  are singleton sets.

The following are the common notations for denoting the various sets of real numbers:

$$Z = \text{Set of all integers} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

$$Z^+ = N = \text{Set of all positive integers} = \{1, 2, 3, 4, \dots\}$$

= Set of natural numbers.

$$Z^- = \text{Set of negative integers} = \{\dots, -4, -3, -2, -1\}$$

$$W = \text{Set of whole numbers} = \{0, 1, 2, 3, 4, \dots\}$$

$$Q = \text{Set of rational numbers} = \left\{ \frac{p}{q} \mid p, q \in Z, q \neq 0 \right\}$$

$$R = \text{Set of real numbers}$$

$$R^+ = \text{Set of positive real numbers} = \{x \mid x \in R, x > 0\}$$

$$R^- = \text{Set of negative real numbers} = \{x \mid x \in R, x < 0\}$$

$$C = \text{Set of complex numbers}$$

Finite intervals are denoted as sets as follows :

$$\text{Closed interval } [a, b] = \{x \mid x \in R, a \leq x \leq b\}$$

$$\text{Closed-open interval } [a, b) = \{x \mid x \in R, a \leq x < b\}$$

$$\text{Open-closed interval } (a, b] = \{x \mid x \in R, a < x \leq b\}$$

$$\text{Open interval } (a, b) = \{x \mid x \in R, a < x < b\}$$

Infinite intervals are denoted as follows :-

$$[a, \infty) = \{x \mid x \in R, x \geq a\}$$

$$(-\infty, a] = \{x \mid x \in R, x \leq a\}$$

## Applied Mathematics - IV

## (1-3)

## Prerequisite

## 3. Finite and Infinite Set

(M.U. 2007)  
A set which has finite elements is called a **finite set**, e.g. the set  $\{a_1, a_2, a_3, \dots, a_n\}$  is a finite set. A set which is not finite is called **infinite set** e.g. the sets described above are **infinite sets**.

## 4. Null Set

It is convenient to introduce the set which contains no elements. Such a set is empty or void and hence it is also called the null set, the empty set or the void set. The null set (derived from the Latin word nullus = not any) is denoted by the symbol  $\Phi$  (pronounced as phi) or  $\{\}$ . It should be noted that  $\Phi$  is not nothing; an empty box is very much different from no box at all.

**Definition :** The set having no elements is called the null set. It should be noted that  $\Phi$  is not identical to  $\{\Phi\}$ ; because  $\Phi$  is a set with no elements while  $\{\Phi\}$  is a set with  $\Phi$  as its element. Thus,  $\Phi \neq \{\Phi\}$ . Also for the same reason  $\Phi \neq \{0\}$ .

Examples of the null set can be given by stating any condition such that no object satisfies the condition.

- (i) The set of women presidents of India till 2000 is the null set,
- (ii)  $\{x \mid x \text{ is an odd number and divisible by 2}\}$  is the null set,
- (iii)  $\{x \mid x \neq x\}$  is the null set.

## 5. Universal Set

While talking about any set we usually need a 'bigger' set or a 'reference' set. Such a set is called a **universal set**. The universal set is denoted by  $U$  or  $S$ . It serves the purpose of providing a frame of reference or the universe for our discussion. The universal set naturally depends upon what ideas we are considering. If we are considering sets of students of a college, then the set of all the students of the college is sufficient as a universal set. If we are studying sets of real numbers, then the universal set  $U$  will be the set of all real numbers.

## 6. Venn-Euler Diagram

To have a geometric picture, we represent the universal set  $U$  by a rectangular area in a plane and the members of  $U$  by the points of the rectangular area. Sets then can be pictured by areas within this rectangle. The areas used to denote the sets may be enclosed by any simple curve (i.e., not intersecting itself) although circles are preferred by many. Such a diagram is known as Venn-Euler diagram or Venn-diagram, named after the English logician John Venn (1834-1923) who first used them.

## John Venn (1834 - 1923)

John Venn was born in a charitable family in England. He got his degree in mathematics in 1856 from Cambridge. In 1883 he got his D.Sc. from Cambridge and was elected a fellow of Royal Society of London. He was greatly influenced by Boole's work in Symbolic Logic. He wrote a book "Symbolic Logic" in which he clarified inconsistencies and ambiguities in Boole's ideas and notations. He used geometric diagrams to represent logical arguments. The technique was first suggested by Leibnitz and was developed by Euler. His two more famous books are "The Logic Of Chance" and "The Principles Of Empirical Logic".



**Leonhard Euler (1707 - 1783)**

One of the great mathematicians of Switzerland. His father wanted him to become a pastor (a priest). But Bernoulli persuaded his father to allow his son to pursue mathematics. He studied under his fellow countryman, mathematician Bernoulli and had published his first paper when he was 18. The word function first suggested by Leibnitz was generalised further by Bernoulli and Euler. Euler is supposed to be the most prolific mathematical writer in history. He has written a number of text books which are known for clarity, detail and completeness. Although he had lost his eye-sight for the last 17 years of his life, he did not allow his work to be hampered because all the formulae from trigonometry and analysis (and many poems including the entire Latin epic-Aeneid) were on the tip of his tongue.

**7. Subsets**

Let  $A$  be the set of the students of F.E. class of your college and  $B$  be the set of all students of your college. We see that all the elements of  $A$  are in  $B$ . We describe such situations as  $A$  is a subset of  $B$ .

**Definition :** Given two sets  $A$  and  $B$  if every element of  $A$  is an element of  $B$ , then  $A$  is called a **subset of  $B$** . We denote this as  $A \subseteq B$ . It is read as  $A$  is a subset of  $B$  or  $A$  is included in  $B$  or  $A$  is contained in  $B$ . If  $A$  is not a subset of  $B$ , it is denoted as  $A \not\subseteq B$ .  $A \subseteq B$  means if  $x \in A$  then  $x \in B$ .

We may also say that  $B$  is a **superset of  $A$**  or  $B$  includes  $A$  or  $B$  contains  $A$ . This we denote as  $B \supseteq A$ . Thus, the notations  $A \subseteq B$  and  $B \supseteq A$  mean one and the same thing. By the by, can we say,  $A \subseteq A$  i.e., every set is a subset of itself? [See Fig. 1.1 (Yes)]

**Example 1 :** If  $A$  is the set of black balls in a box and  $B$  is the set of all balls in the box then  $A \subseteq B$ .

**Example 2 :** If  $A = \{x \mid x$  is a positive integer divisible by 6 $\}$  and  $B = \{x \mid x$  is a positive integer divisible by 3 $\}$ , then since

$$A = \{6, 12, 18, 24, \dots\}$$

$$\text{and } B = \{3, 6, 9, 12, 15, 18, 21, 24, 27, \dots\}, \quad A \subseteq B.$$

**Proper subset :** If  $A$  is a subset of  $B$  and  $A$  is not equal to  $B$ , (See § 8 below) we say that  $A$  is a **proper subset of  $B$** . This relation is denoted by  $A \subset B$ .

If the sets  $N, Z, Q, R, C$  are as defined on page 1-2, then it is clear that  $N \subset Z \subset Q \subset R \subset C$ .

**8. Equality**

By equality of sets we mean that the sets have the same or identical elements.

**Definition :** If every element of  $A$  is an element of  $B$  and if every element of  $B$  is an element of  $A$ , then the set  $A$  is equal to the set  $B$ . This is denoted by  $A = B$ .

In other words using the notation of set inclusion,

**If  $A \subseteq B$  and if  $B \subseteq A$ , then  $A = B$  and conversely**

**Example 1 :** If  $A = \{3, 4\}$  and  $B = \{x \mid x^2 - 7x + 12 = 0\}$ , then  $A = B$ .

It is clear that the roots of the equation  $x^2 - 7x + 12 = 0$  are 3 and 4. Therefore,  $B = \{3, 4\}$  if written in the list form. Since each element 3, 4 of  $A$  is an element of  $B$  and each element 3, 4 of  $B$  is in  $A$ ,  $A = B$ .

**Example 2 :** If  $A = \{x \mid x$  is a letter in 'spot' $\}$ ,  $B = \{x \mid x$  is a letter in 'tops' $\}$ , then  $A = B$ .

The elements of the set  $A$  are s, p, o, t and those of  $B$  are t, o, p, s. Since, every element of  $A$  is in  $B$  and every element of  $B$  is in  $A$ .  $\therefore A = B$ . Note that because of this reason order of elements in a set is immaterial. Thus,  $\{a, b, c\} = \{c, a, b\} = \{b, a, c\}$ .

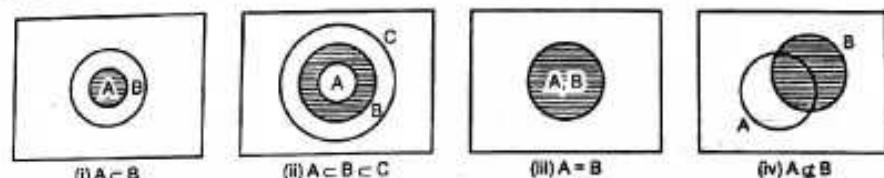


Fig. 1.1

Using Venn diagrams set inclusion and equality can be represented as shown above. If  $A, B$  and  $C$  are sets, then Fig. (i) represents the situation that  $A$  is subset of  $B$ , and Fig. (ii) represents the situation that  $A$  is a subset of  $B$  and  $B$  is a subset of  $C$ , Fig. (iii) represents the situation  $A = B$ , Fig. (iv) represents the situation that  $A \not\subseteq B$ .

**9. Operations On Sets**

Just as we have operations of addition, subtraction, multiplication and division on real numbers, we can operate on given sets and produce new sets. The operations are (i) Complementation, (ii) Union, (iii) Intersection.

**10. Complement of A Set**

Consider the set  $U$  of all students of your college and the set  $A$  of all students of F.E. class, and the set  $B$  of all students of all other classes. We see that the elements of  $B$  are in  $U$  but not in  $A$ . Such a set is called the complement of the given set.

**Definition :** Let  $A$  be a subset of the universal set  $U$ . The set of all elements of  $U$  which do not belong to  $A$  is called the complement of  $A$ . It is denoted by  $A'$  or  $\bar{A}$  or  $A^c$ . In symbols,

$$\bar{A} = \{x \mid x \in U \text{ and } x \notin A\}$$

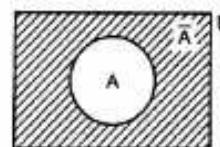


Fig. 1.2 (a)

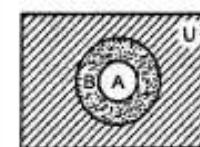


Fig. 1.2 (b)

In the Fig. 1.2 (a), the shaded area represents the complement of  $A$ .

### Applied Mathematics - IV

(1-6)

**Example 1 :** If  $U$  is the set of all students who appeared for F.E. examination and  $A$  is the set of students who passed, then  $\bar{A}$  is the set of all students who failed at the F.E. examination.

**Example 2 :** If  $U = \{1, 2, 3, 4, 5, 6, 7\}$  and  $A = \{1, 3, 5\}$ , then  $\bar{A} = \{2, 4, 6, 7\}$ .

The following properties of the operation of forming complements are obvious:

- (i)  $\bar{\bar{A}} = A$
- (ii)  $\bar{U} = \emptyset$
- (iii)  $\bar{(\bar{A})} = A$
- (iv) If  $A \subseteq B$  then  $\bar{B} \subseteq \bar{A}$

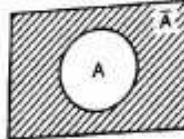
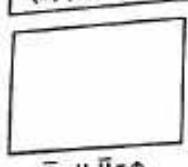


Fig. 1.3

### Prerequisite

### Applied Mathematics - IV

(1-7)

### Prerequisite

### Applied Mathematics - IV

(1-7)

### Prerequisite

### Applied Mathematics - IV

(1-7)

### Prerequisite

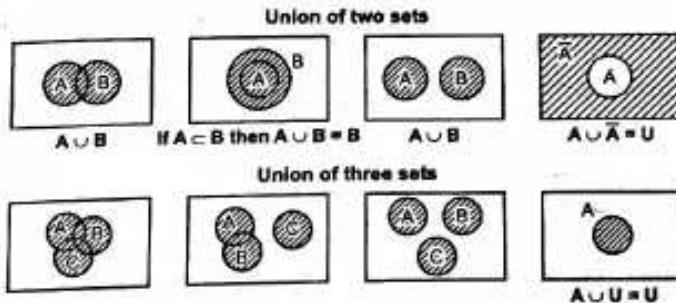


Fig. 1.4

### Note ...

Note that the usual law of 'cancellation' does not hold for union of two sets. For example, if  $A = \{a, b\}$ ,  $B = \{a, c\}$  and  $C = \{b, c\}$ , then  $A \cup B = A \cup C = \{a, b, c\}$  and still  $B \neq C$ .

## 12. Intersection of Sets

The next operation on sets is that of forming intersection. Consider the example of the previous article,  $A$  is the set of persons who speak Marathi and  $B$  is the set of persons who speak English. Then the set of persons who speak both Marathi and English is the set of persons common to both the sets  $A$  and  $B$ . This set is called the **Intersection** of  $A$  and  $B$ .

**Definition :** The **intersection** of two sets  $A$  and  $B$  is defined as the set of elements which are both in  $A$  and in  $B$ . It is denoted by  $A \cap B$  and read as  $A$  intersection  $B$  or  $A$  cap  $B$ . In symbols,

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

In the Figs. 1.6 given below,  $A \cap B$  is denoted by shaded area. It is clear that  $A \cap B$  is obtained by taking the common part i.e., the common elements of  $A$  and  $B$ .

**Example 1 :** If  $A = \{1, 2, 5, 7\}$ ,  $B = \{1, 3, 4, 5, 6, 8\}$ , then  $A \cap B = \{1, 5\}$ .

**Example 2 :** If  $A = \{a, b, c, d\}$  and  $B = \{b, d, g, h\}$ , then  $A \cap B = \{b, d\}$ .

### Notes ...

Note that the usual law of 'cancellation' does not hold for the intersection of sets. For example, if  $A = \{a, b\}$ ,  $B = \{a, c\}$  and  $C = \{a, d\}$  then  $A \cap B = A \cap C = \{a\}$  and still  $B \neq C$ .

## 13. Disjoint Sets

**Definition :** If  $A$  and  $B$  are two sets such that  $A \cap B = \emptyset$  i.e. their intersection is empty then  $A$  and  $B$  are called **disjoint sets**.

**Example 1 :** The sets  $A = \{1, 2, 3\}$  and  $B = \{4, 5, 6\}$  are disjoint sets.

**Example 2 :** The sets  $A = \{a, b, c\}$ ,  $B = \{d, e, f\}$  are disjoint sets.

**Example 3 :** The set  $A = \{1, 3, 5, 7, \dots\}$ ,  $B = \{2, 4, 6, 8, \dots\}$  are disjoint.

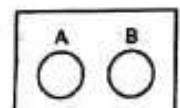


Fig. 1.5 : Disjoint sets.

## 11. Union of Sets

Let  $U$  be the set of all persons in Maharashtra,  $A$  be the set of persons who speak Marathi and  $B$  be the set of persons who speak English. Then the set of persons who speak either Marathi or English is clearly the set of all persons in the two sets taken together. Some persons may speak English and Marathi but we know that they are to be taken into account only once. This set is called the **union**.

**Definition :** The **union** of two sets  $A$  and  $B$  is defined as the set of all elements which are either in  $A$  or in  $B$  (including those which are in both). It is denoted by  $A \cup B$  and read as  $A$  union  $B$  or  $A$  cup  $B$ . In symbols,

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

It is clear that  $A \cup B$  is formed by lumping together the elements of  $A$  and of  $B$  and treating them as forming a single set.

**Example 1 :** If  $A$  is the set of persons who drink tea and  $B$  is the set of those persons who drink coffee then  $A \cup B$  is the set of persons who drink either tea or coffee including those who drink both.

**Example 2 :** If  $A = \{1, 2, 3, 4\}$  and  $B = \{3, 4, 5, 6\}$ , then  $A \cup B = \{1, 2, 3, 4, 5, 6\}$ .

**Example 3 :** If  $A = \{a, b, d, f\}$ ,  $B = \{b, c, d, e\}$ , then  $A \cup B = \{a, b, c, d, e, f\}$ .

The following properties of the operation of forming union are obvious

- (i)  $A \cup B = B \cup A$
- (ii)  $A \cup (B \cup C) = (A \cup B) \cup C$
- (iii)  $A \cup A = A$
- (iv)  $A \cup \emptyset = A$
- (v)  $A \cup U = U$
- (vi) If  $A \subset B$ , then  $A \cup B = B$
- (vii)  $A \cup \bar{A} = U$
- (viii)  $A \subseteq (A \cup B)$  and  $B \subseteq (A \cup B)$

If  $A$  and  $B$  are any two sets with universal set  $U$  then there are three possibilities. (i) one set is a subset of the other, (ii) they intersect, (iii) they do not intersect i.e. they are disjoint.

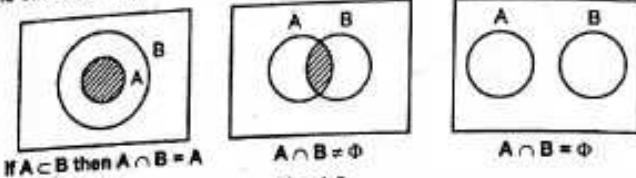


Fig. 1.6

If  $A, B, C$  are three sets then there are various possibilities. We consider some of them.  
(i)  $A$  and  $B$  intersect but  $A, C$  and  $B, C$  are disjoint, (ii)  $A, B$  intersect;  $B, C$  intersect but  $A, C$  are disjoint, (iii)  $A, B, C$  are all disjoint, (iv)  $A, B, C$  all intersect i.e.  $A \cap B \cap C \neq \emptyset$ . [ See Fig. 1.7 (c) below.]



Fig. 1.7 (a) : Intersection of one set.

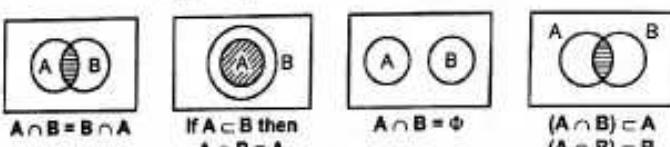


Fig. 1.7 (b) : Intersection of two sets.

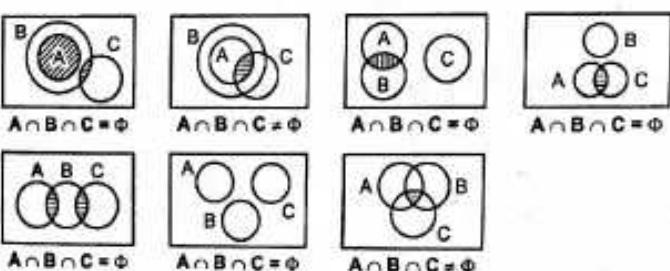


Fig. 1.7 (c) : Intersection of three sets.

Observe that if  $A, B, C$  are three sets, then they create  $2^3 = 8$  regions. These regions can be described as follows. If  $x$  is an element of the universal set  $U$  then (i)  $x \in A$  only, (ii)  $x \in B$  only, (iii)  $x \in C$  only, (iv)  $x \in A$  and  $x \in B$  but  $x \notin C$ , (v)  $x \in B$ ,  $x \in C$  but  $x \notin A$ , (vi)  $x \in C$ ,  $x \in A$  but  $x \notin B$ , (vii)  $x \in A, x \in B$  and also  $x \in C$ , (viii)  $x \notin A, x \notin B, x \notin C$ .

(We have not shown all the cases in the above figures.)

Since for an element of  $U$  there are two possibilities, either  $x$  belongs to the set  $A$  or  $B$  or  $C$  or  $x$  does not belong to these sets  $A$  or  $B$  or  $C$ . Since there are three sets there are  $2^3$  possibilities.

**Example 4 :** If  $A = \{x | x \text{ is real and } x^2 - 5x + 6 = 0\}$  and  $B = \{x | x \text{ is real and } x^2 - 7x + 10 = 0\}$  i.e.,  $A = \{2, 3\}$  and  $B = \{2, 5\}$  then  $A \cap B = \{2\}$ .

The following properties of the operation of forming intersection are obvious :

- |                                    |  |
|------------------------------------|--|
| (i) $A \cap B = B \cap A$          | (ii) $A \cap (B \cap C) = (A \cap B) \cap C$             |
| (iii) $A \cap A = A$               | (iv) $A \cap \emptyset = \emptyset$                      |
| (v) $A \cap U = A$                 | (vi) If $A \subset B$ then $A \cap B = A$                |
| (vii) $A \cap \bar{A} = \emptyset$ | (viii) $(A \cap B) \subset A$ and $(A \cap B) \subset B$ |

#### 14. Difference of Two Sets ( $A - B$ )

If  $A$  and  $B$  are two sets then the set of elements in  $A$  which are not in  $B$  is called the difference and is denoted by  $A - B$ . Some authors denote the difference by  $A \setminus B$  or  $A - B$ .

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

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

The Venn-diagrams of  $A - B$  and  $B - A$  are shown below.

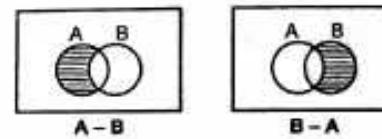


Fig. 1.8

Three particular cases of  $A - B$  are shown below.

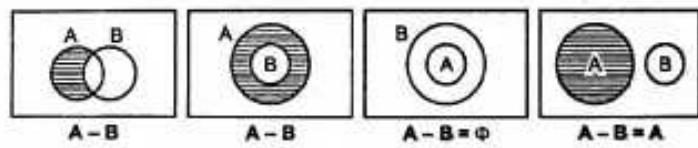


Fig. 1.9

The difference of two sets is also sometimes called the relative complement. It is easy to see that

$$A - B = A \cap \bar{B} \quad \text{and} \quad B - A = B \cap \bar{A}$$

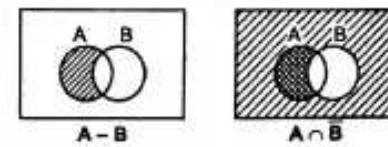


Fig. 1.10

- Example 1 :** If  $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$ ,  $A = \{1, 2, 3, 6, 7\}$ ,  $B = \{2, 3, 4, 8\}$ ,  
then  $A - B = \{1, 6, 7\}$  and  $B - A = \{4, 8\}$ .
- Example 2 :** If  $U = \{a, b, c, d, e, f, g, h\}$ ,  $A = \{a, b, c, e, f\}$ ,  $B = \{b, c, d, g, h\}$ ,  
then  $A - B = \{a, e, f\}$  and  $B - A = \{d, g, h\}$ .

### 15. Symmetric Difference ( $A \oplus B$ )

**Definition :** If  $A$  and  $B$  are two sets then the symmetric difference of  $A$  and  $B$  is defined as the set of elements which belong to either  $A$  or to  $B$  but not to both. It is denoted by  $A \Delta B$  or  $A \oplus B$  and is also called the Boolean sum of  $A$  and  $B$ . Thus,

$$A \Delta B = A \oplus B = \{x \mid x \in A \text{ or } x \in B\} \quad (1)$$

The symmetric difference between  $A$  and  $B$  is also defined by

$$A \oplus B = \{x \mid x \in A - B \text{ or } x \in B - A\} \quad (1A)$$

This definition leads to the following definition,

$$A \oplus B = (A - B) \cup (B - A) \quad (1B)$$

- Example 1 :** If  $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$  and  $A = \{1, 2, 4, 5\}$ ,  $B = \{2, 3, 4, 6\}$ ,  
then  $A \oplus B = \{1, 3, 5, 6\}$ .

- Example 2 :** If  $U = \{a, b, c, d, e, f, g, h\}$  and  $A = \{a, c, e, f\}$ ,  $B = \{c, e, g, h\}$ ,  
then  $A \oplus B = \{a, f, g, h\}$ .

It is easy to see that  $A \oplus B = (A \cup B) - (A \cap B)$

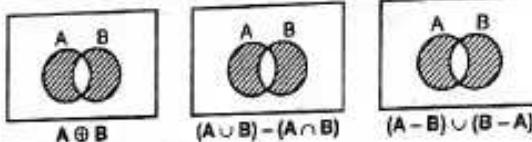


Fig. 1.11

Also we can show that

$$A \oplus B = (A - B) \cup (B - A) \quad (3)$$

Three particular cases of symmetric difference are shown below.



Fig. 1.12

### 16. Distribution

We have defined above the two fundamental operations on sets viz. union and intersection. We shall now see how they are related to each other. They are known as distributive laws. These laws are :

and

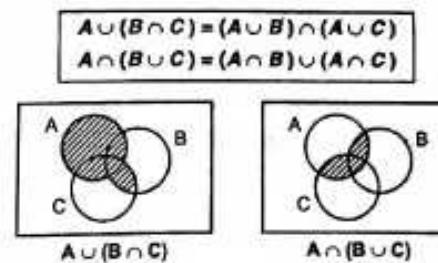


Fig. 1.13

It may be seen that the above laws are analogous to the law of multiplication over addition viz.  $a \times (b + c) = a \times b + a \times c$ .

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

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

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

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

$$\therefore A \cup (B \cap C) = \{1, 3, 4, 5\} = (A \cup B) \cap (A \cup C)$$

Now,  $B \cup C = \{1, 2, 3, 5, 6, 7\}$ ,  $A \cap B = \{3\}$ ,  $A \cap C = \{1\}$

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

### 17. De Morgan's Laws

Lastly we state how the operation of forming complements is related to the formation of unions and intersections. These laws are known as **De Morgan's laws**.

If  $A$  and  $B$  are any two sets, then

$$(A \cup B)' = \bar{A} \cap \bar{B} \text{ and } (A \cap B)' = \bar{A} \cup \bar{B}$$

The first equation states that the complement of the union is equal to the intersection of the complements and the second equation states that the complement of the intersection is equal to the union of the complements.

#### Augustus De Morgan (1806 - 1871)

Augustus De Morgan was born in Madurai, Tamil Nadu. His father was a colonel in the Indian army. His family returned to England when he was 7 months old. When in schools he mastered Latin, Greek and Hebrew and developed strong interest in mathematics.

He was a fellow of the Astronomical Society and a founder of London Mathematical Society. De Morgan greatly influenced the development of mathematics in the 19th century. He was a prolific writer and wrote over 1000 articles in more than 15 journals, in addition to a number of books known for clarity, logical presentation and minute details. He made original contributions to analysis and logic. He coined the term mathematical induction and gave first precise definition of limit in his book "The Differential And Integral Calculus".



### Prerequisite

(1-12)

### Applied Mathematics - IV

**Example :** If  $U = \{a, b, c, d, e, f, g, h\}$ ,  $A = \{a, b, c, d\}$  and  $B = \{c, d, e, f\}$ , verify the De Morgan's laws.

Sol. : We have  $A \cup B = \{a, b, c, d, e, f\}$

$$\therefore \overline{(A \cup B)} = \{g, h\}$$

$$\text{But } \overline{A} = \{a, f, g, h\} \text{ and } \overline{B} = \{a, b, g, h\}$$

$$\therefore \overline{A} \cap \overline{B} = \{g, h\}$$

$$\therefore \overline{(A \cup B)} = \overline{A} \cap \overline{B} = \{g, h\}$$

$$\text{Further, } A \cap B = \{c, d\}$$

$$\therefore \overline{(A \cap B)} = \{a, b, e, f, g, h\}$$

$$\text{But } \overline{A} \cup \overline{B} = \{a, b, e, f, g, h\}$$

$$\therefore \overline{A \cap B} = \overline{A} \cup \overline{B}$$

### 18. Class of Sets

We know that a set is a collection of objects called elements. But in some situations we may need to talk about the subsets of a given set as elements. Such a collection of sets is called a class of sets or a family of sets. Suppose we are given  $A = \{a, b, c\}$ . From this we can have a set whose elements are subsets of  $A$ . e.g.,  $S = \{\{a\}, \{b\}, \{a, b\}\}$ . Such a set  $S$  is called a class of sets.

**Example :** Let  $S = \{a, b, c, d\}$ . Find the class of subsets of  $S$  which contain (1) exactly two elements, (2) exactly three elements, (3)  $c$  and two other elements.

Sol. : We have

$$A = \{\{a\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b\}, \{b, c\}, \{b, d\}, \{c\}, \{c, d\}\}$$

$$B = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, b, c\}\}$$

$$C = \{\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}\}$$

### 19. Power Set

**Definition :** If  $S$  is a given set then the set of all subsets of  $S$  is called power set of  $S$  and is denoted by  $P(S)$ . Clearly  $\emptyset$  and  $S$  are the elements of  $P(S)$ .

**Example 1 :** If  $S = \{\emptyset\}$ , then  $P(S) = \{\emptyset, \{\emptyset\}\}$

**Example 2 :** If  $S = \{a, b\}$ , then  $P(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ .

**Example 3 :** If  $S = \{a, b, c\}$  then  $P(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ .

[ If  $S$  has  $N$  elements then  $P(S) = 2^N$  elements and hence some times the power set is also denoted by  $2^N$ . See that in Ex. 1 above  $S$  has only 1 element and  $P(S)$  has  $2^1 = 2$  elements. In Ex. 2,  $S$  has 2 elements and  $P(S)$  has  $2^2 = 4$  elements. In Ex. 3,  $S$  has 3 elements and hence  $P(S)$  has  $2^3 = 8$  elements. ]

**Example 4 :** If  $A = \{\alpha, \beta, \gamma, \delta\}$ , find the power set of  $A$ .

Sol. :  $P(A) = \{\emptyset, \{\alpha\}, \{\beta\}, \{\gamma\}, \{\delta\}, \{\alpha, \beta\}, \{\alpha, \gamma\}, \{\alpha, \delta\}, \{\beta, \gamma\}, \{\beta, \delta\}, \{\gamma, \delta\}, \{\alpha, \beta, \gamma\}, \{\alpha, \beta, \delta\}, \{\alpha, \gamma, \delta\}, \{\beta, \gamma, \delta\}, \{\alpha, \beta, \gamma, \delta\}\}$

$P(A)$  has  $2^4 = 16$  elements.

### Prerequisite

### Applied Mathematics - IV

(1-13)

### Prerequisite

(M.U. 2001, 02, 11)

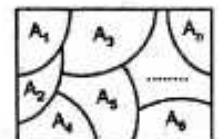


Fig. 1.14

### 20. Partition of Sets

If  $S$  is a non-empty set, by partition of  $S$ , we mean the division of  $S$  into disjoint subsets such that their union is  $S$ . As shown in the Fig. 1.14, if  $S$  is the given set then  $A_1, A_2, A_3, \dots, A_n$  form the partition of  $S$ .

**Definition :** A collection  $\{A_i\}$  of non-empty subsets of  $S$  is called a partition of  $S$  if (i) each element of  $S$  belongs to one subset  $A_i$  i.e.,  $\cup A_i = S$  and (ii) the subsets  $A_i$  are mutually disjoint i.e.,  $A_i \cap A_j = \emptyset$ .

The subsets in a partition are called cells.

**Example 1 :** Let  $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$  and consider the following collections of subsets of  $S$ ,

$$(i) A_1 = \{\{1, 2, 3\}, \{3, 4, 5\}, \{6, 7, 8\}\}$$

$$(ii) A_2 = \{\{1, 2\}, \{3, 4, 5\}, \{6, 7\}\}$$

$$(iii) A_3 = \{\{1, 2, 3\}, \{4, 5\}, \{6, 7\}, \{8\}\}$$

Which of them is a partition of  $S$  and why? Also draw diagrams.

Sol. : The collection  $A_1, A_2, A_3$  are shown in Fig. 1.15.

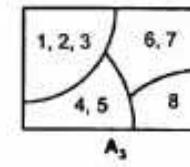
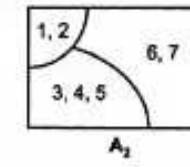
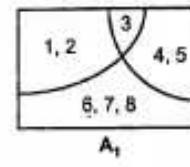


Fig. 1.15

$A_1$  is not a partition because subsets  $\{1, 2, 3\}$  and  $\{3, 4, 5\}$  are not disjoint. Their intersection is  $\{3\}$ .

$A_2$  is not a partition because their union is not  $S$ . The element 8 does not belong to any subset.

$A_3$  is a partition because each element of  $S$  belongs to one of the subsets i.e., the union of the subsets is  $S$  and no element belongs to two (or more) subsets i.e., all subsets are mutually disjoint.

**Example 2 :** Let  $S = \{a, b, c, d, e, f, g, h\}$  and consider the following subsets of  $S$

$$A = \{a, b, c, d\}, \quad B = \{a, c, e, g, h\},$$

$$C = \{a, c, e, g\}, \quad D = \{b, d\}, \quad E = \{f, h\},$$

Determine whether each of the following is a partition of  $S$  or not.

$$(i) \{A, B\}, (ii) \{A, E\}, (iii) \{C, D, E\}. \quad \text{Give reason.}$$

Sol. : (i) Consider  $\{A, B\}$

$$(1) A \cup B = \{a, b, c, d, e, g, h\}$$

$$\therefore f \notin (A \cup B) \quad \therefore A \cup B \neq S$$

$$(2) A \cap B = \{a, c\} \neq \emptyset \quad \therefore \{A, B\} \text{ is not a partition.}$$

[ Fig. 1.15 (a) ]

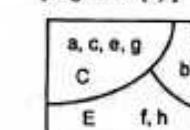
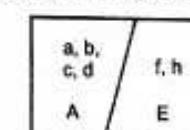
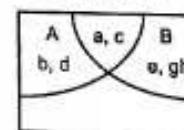


Fig. 1.15 (a)

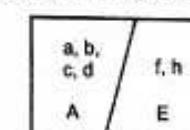


Fig. 1.15 (b)



Fig. 1.15 (c)

- (ii) Consider  $\{A, E\}$   
 (1)  $A \cup E = \{a, b, c, d, e, f, h\}$ ;  $e$  and  $f$  do not belong to  $A \cup B$ .  $\therefore A \cup B \neq S$   
 (2)  $A \cap E = \emptyset$   
 $\therefore \{A, E\}$  is not a partition. [Fig. 1.15 (b) on previous page]
- (iii) Consider  $\{C, D, E\}$   
 (1)  $C \cup D \cup E = \{a, b, c, d, e, f, g, h\} = S$   
 (2)  $C \cap D \cap E = \emptyset$   
 $\therefore \{C, D, E\}$  is a partition. [Fig. 1.15 (c) on previous page]

**21. Ordered Set**

A set as we know is a collection of objects with no reference to the order in which the elements of the set are written. For this reason the sets  $\{a, b, c\}$ ,  $\{b, c, a\}$ ,  $\{c, a, b\}$  are equal. If we assign a position to each element of a set then the set is called an ordered set.

Definition : A set of elements such that each element is assigned a position is called an ordered set. If  $a_1, a_2, \dots, a_n$  are the elements of an ordered set in this order, it is denoted by  $(a_1, a_2, \dots, a_n)$ . An ordered set with  $n$  elements is called an  $n$ -tuple.

Two  $n$ -tuples are equal if and only if their corresponding elements are equal. The ordered set  $(a_1, a_2, \dots, a_n)$  and  $(b_1, b_2, \dots, b_n)$  are equal if and only if  $a_i = b_i$  for every  $i$ .

For example, in the number system a number is an ordered set of digits. The number '2435' is an ordered set of the digits 2, 3, 4 and 5. Similarly, a word is an ordered set of letters. The word 'theory' is an ordered set of the letters t, h, e, o, r, y.

(M.U. 2011)

**22. Cartesian Product**

The Cartesian product of two sets  $A$  and  $B$  denoted by  $A \times B$  is the set of all ordered pairs  $(a, b)$  where  $a \in A$  and  $b \in B$ . Thus,

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Example 1 : Write the cartesian product  $A \times B$  where  $A = \{a, b, c\}$  and  $B = \{1, 2, 3\}$ .

Sol. : By definition the cartesian product  $A \times B$  is the set  $(a, b)$  where the first element  $a \in A$  and the second element  $b \in B$ . Each element of  $A$  is to be paired with each element of  $B$ .

$$\therefore A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}$$

A cartesian product can be represented pictorially by taking the set  $A$  on the horizontal axis and the set  $B$  on the vertical as usual. [Fig. 1.33(a)]

Similarly, we get

$$B \times A = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c)\}$$

Pictorial representation of this product is as shown in Fig. 1.33 (b).

Note that since  $(a, 1)$  and  $(1, a)$  are ordered pairs, they are not equal. Hence, in this case the sets  $A \times B$  and  $B \times A$  are not equal.

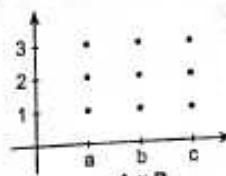


Fig. 1.17 (a)

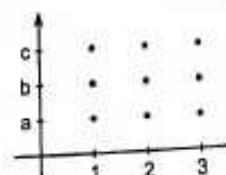


Fig. 1.17 (b)

Example 2 : If  $A$  and  $B$  are the sets as given in Ex. 1, write  $A \times A$ ,  $B \times B$ .

Sol. : Clearly, we have

$$A \times A = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$$

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

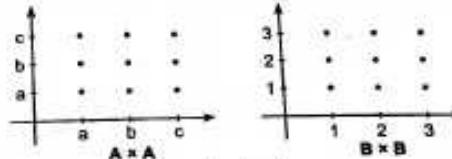


Fig. 1.18

**PERMUTATION AND COMBINATION****1. Introduction**

In this chapter we shall first learn two new concepts viz. permutation and combination. We shall solve some interesting examples based on these concepts. Lastly in this chapter we shall learn some easy progressions viz. arithmetic and geometric progressions.

Consider the following problems :

- (i) Suppose, there are five English novels and four Marathi novels. In how many different ways can a boy choose a novel either English or Marathi ?
- (ii) Population of a city is to be classified according to sex (male and female) and religion (Hindu, Muslim and Christian). How many different classes will be formed ?
- (iii) How many different numbers can be formed by taking four digits at a time out of five digits 1, 2, 3, 4, 5 ?
- (iv) In how many different ways a committee of six students be formed out of ten ?

The above questions can be answered by actually counting all the possible cases. But if the number of things involved is large the method will be tedious. In this chapter we shall find some general rules that can be conveniently used to answer questions of the above type.

**2. Basic Rules**

We give below certain basic rules which are more or less obvious.

Rule 1 : If a certain operation A can be performed in  $m$  different ways and if another operation B can be performed in  $n$  different ways, then the total number of ways in which either the operation A or the operation B can be performed in  $m + n$ .

The rule is obvious. Referring to the example (i) article 1, we see that the boy can choose either an English or a Marathi novel in  $5 + 4 = 9$  different ways.

Now, suppose there are four different roads connecting a city A to another city B and three different roads connecting B to a third city C. (Refer Fig. 1.19) In how many ways can a person go from A to B and then to C, thus completing the journey ? He can choose any one road from A to B

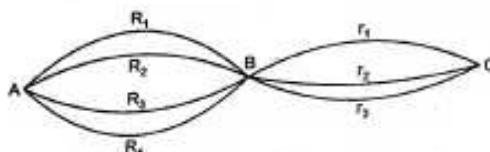


Fig. 1.19

and then he has three alternatives for going from B to C. Thus, for each of the four choices of the roads from A to B he has three alternative roads from B to C. Hence, the total number of ways in which he can complete the journey is  $4 \times 3 = 12$ . If  $R_1, R_2, R_3, R_4$  are the roads from A to B and  $r_1, r_2, r_3$  are the roads from B to C then twelve ways of his journey are :

$$\begin{array}{llll} R_1 r_1, & R_1 r_2, & R_1 r_3, & : \\ R_2 r_1, & R_2 r_2, & R_2 r_3, & : \\ R_3 r_1, & R_3 r_2, & R_3 r_3, & : \\ R_4 r_1, & R_4 r_2, & R_4 r_3, & \end{array}$$

In general we can state the following rule :

**Rule 2 :** If an operation can be performed in any one of  $m$  different ways and if after performing this in one of these ways, a second operation can be performed in  $n$  different ways, then the total number of ways in which the two operations can be performed together in this order is  $m \times n$ .

Let  $a_1, a_2, a_3, \dots, a_m$  be  $m$  different ways of performing the first operation and  $b_1, b_2, b_3, \dots, b_n$  be  $n$  different ways of performing the second operation.

If the first operation is performed in any one way, say,  $a_1$  then the second operation can be done in any one of the  $n$  ways  $b_1, b_2, b_3, \dots, b_n$ . Thus, the two operations can be performed together in this order in  $n$  ways.

$$a_1 b_1, a_1 b_2, a_1 b_3, \dots, a_1 b_n$$

Similarly for  $a_2, a_3, \dots, a_m$  we have the following ways

$$a_2 b_1, a_2 b_2, a_2 b_3, \dots, a_2 b_n$$

$$a_3 b_1, a_3 b_2, a_3 b_3, \dots, a_3 b_n$$

$$\dots$$

$$a_m b_1, a_m b_2, a_m b_3, \dots, a_m b_n$$

Thus, the total number of different ways is

$$n + n + n + \dots, m \text{ times} = mn$$

Referring to the example (ii) of article 1, we see that the population is classified in  $2 \times 3 = 6$  classes. If the population is further classified according to 4 age groups, say, 0-25, 25-50, 50-75, 75 and above 75 years, then there will be  $2 \times 3 \times 4 = 24$  classes.

**Corollary of the above rule :** If each of the  $n$  operations can be performed in  $m$  different ways i.e., if  $m_1 = m_2 = m_3 = \dots = m_n = m$  then the total number of operations in which all  $n$  operations are performed in the order is

$$m \times m \times m \dots, n \text{ times} = m^n$$

Suppose we want to place 4 different books in 3 different boxes. With each operation of placing a book there are three different ways. It can be placed in any of the three boxes. Hence, the total number of ways in which 4 books can be placed in three boxes is  $3 \times 3 \times 3 \times 3 = 81$ .

**Example 1 :** If a set A has  $n$  (distinct) elements then how many subsets can be formed from A?

**Sol. :** The first element can be dealt with in two ways, either selecting it for the set-inclusion or by not selecting. In the same way there are 2 ways for the second element, for the third element, ..., for  $n$  elements.

$$\therefore \text{No. of subsets} = 2 \times 2 \times 2 \dots, n \text{ times} = 2^n$$

For example if  $A = \{a, b, c\}$ , then the following  $2^3 = 8$  subsets are possible,

$$\{\emptyset\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}$$

**Example 2 :** A coin is tossed  $n$  times and the results are recorded. How many sequences of H and T are possible ?

**Sol. :** As above  $2^n$ .

Give the explanation. For example, if the coin is tossed thrice, we have the following 8 sequences.

$$\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}$$

**Example 3 :** A label identifier, for a computer system, consists of one letter followed by 4 digits. If the repetitions are allowed, how many distinct label identifiers are possible ?

**Sol. :** There are 26 letters from A to Z. Hence, the identifier begins with in 26 different ways. It is followed by first digit in 10 ways, second digit is 10 ways, and so on,

$$\begin{aligned} \therefore \text{No. of label identifier} &= 26 \times 10 \times 10 \times 10 \times 10 \\ &= 260000 \end{aligned}$$

### 3. Permutations

Suppose we have to form numbers from three digits 2, 6, 9 taking all the three digits at a time. Suppose further no digit is to be repeated. We will get six numbers.

(1) 269, (2) 296, (3) 629, (4) 692, (5) 926, (6) 962. All the six numbers consist of the same three digits. But they are all different because the order in which the digits appear is significant.

The above result can be obtained by using Rule 2. The hundreds place can be filled in 3 ways by any of the three digits. There are two digits left which can fill tens place. The units place can be filled in only one way. Hence, by Rule 2 the total number of ways =  $3 \times 2 \times 1 = 6$ . Such an ordered arrangement is called a permutation.

**Definition :** An arrangement of some or all of a given number of things in order is called permutation.

The total number of permutations of  $n$  different things taken  $r$  at a time is denoted by  ${}^n P_r$  or  $P(n, r)$ . Thus,  ${}^5 P_2$  means the number of permutations of 5 things taken 2 at a time.  ${}^7 P_3$  means the number of permutations of 7 things taken 3 at a time.

**To find the number of permutations of  $n$  different things taken  $r$  at a time.**

Suppose there are  $r$  chairs in a row and  $n$  persons are to take these chairs. In how many ways they can take these chairs ?

Chair	1	2	3	...	$r-1$	$r$
No. of ways	$n$	$n-1$	$n-2$	...	$n-r+2$	$n-r+1$

## Applied Mathematics - IV

(1-18)

### Prerequisite

The first chair can be filled by any one of the  $n$  persons in  $n$  different ways. Having filled the first chair by any one of these ways, the second chair can be filled by any one of the remaining  $(n-1)$  persons in  $(n-1)$  ways. Hence, the number of ways in which the first two chairs can be filled is  $n(n-1)$ .

After having filled the first two chairs in any one of the  $n(n-1)$  ways, the third chair can be filled by any one of the remaining  $(n-2)$  persons in  $(n-2)$  ways. Hence, the first three chairs can be filled in any one of the  $n(n-1)(n-2)$  ways.

Proceeding in this manner we see that the  $r$ -th chair can be filled by any one of the remaining  $n-(r-1)$  persons in  $n-(r-1)$  ways. Hence, the number of ways in which  $r$  chairs can be filled is  $n(n-1)(n-2) \dots (n-(r-1))$ . This we denote by  ${}^n P_r$ .

$${}^n P_r = n(n-1)(n-2) \dots (n-(r-1)) \quad \dots \dots \dots (1)$$

### 4. Factorial Notation (Meaning of $n!$ )

In the above formula for  ${}^n P_r$ , we see that we need to write the product of consecutive integers. To express the product of consecutive integers factorial notation is very convenient.

The product  $1 \cdot 2 \cdot 3 \cdot 4 \dots n$  is denoted by  $n!$  or  $|n|$  (read as  $n$  factorial or factorial  $n$ ).

$$\text{Thus, } 10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 ; 5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5.$$

$$\text{Also, } 11 \cdot 12 \cdot 13 \dots 40 = \frac{(1 \cdot 2 \cdot 3 \dots 10)(11 \cdot 12 \cdot 13 \dots 40)}{1 \cdot 2 \cdot 3 \dots 10} = 40!$$

It may be noted that  $n! = n(n-1)!$  and  $(n+1)n! = (n+1)!$ . The formula for  ${}^n P_r$  can be written more conveniently in factorial notation as,

$$\begin{aligned} {}^n P_r &= n(n-1)(n-2) \dots (n-r+1) \\ &= \frac{n(n-1)(n-2) \dots (n-r+1) \times (n-r)(n-r-1) \dots 3 \cdot 2 \cdot 1}{(n-r)(n-r-1) \dots 3 \cdot 2 \cdot 1} \\ &\therefore {}^n P_r = \frac{n!}{(n-r)!} \quad \dots \dots \dots (2) \end{aligned}$$

**Corollary :** The number of permutations of  $n$  different things taken all at a time is  ${}^n P_n = n!$ . The number  ${}^n P_n$  can be obtained by putting  $r=n$  in the formula (1).

$$\begin{aligned} \therefore {}^n P_n &= n(n-1)(n-2) \dots (n-n+1) \\ &= n(n-1)(n-2) \dots 3 \cdot 2 \cdot 1 = n! \end{aligned}$$

**Definition of  $0!$  :** From the definition of  $n!$ , it appears that  $0!$  is meaningless. However, if we

put  $r=n$  in (2) above we get  ${}^n P_n = \frac{n!}{0!}$ . But we know that from (1)  ${}^n P_n = n!$ . In order to make the two results agree we define  $0! = 1$ .

$${}^n P_n = n! \text{ and } 0! = 1$$

### 5. Permutations of Things not all Different

To find the number of permutations of  $n$  things taken all at a time when some of them are similar, we consider a particular example.

## Applied Mathematics - IV

(1-19)

### Prerequisite

**Example :** Find the number of permutations of the letters of the word "institutions" taken all at a time.

We have 12 letters of which 3 are  $t$ 's, 3 are  $i$ 's, 2 are  $n$ 's, 2 are  $s$ 's and the remaining two are different. If all the 12 letters had been different, the number of permutations would have been  $12!$ .

Let  $x$  denote the number of permutations required in the above example. Let us take any such arrangement of the letters of the given word, say 'institutinsino'. If we replace the three  $t$ 's by the different letters  $t_1, t_2, t_3$  and keep all other letters in the same positions and permute  $t_1, t_2, t_3$  only in all possible ways we will get  $3!$  arrangements from this arrangement. If this change is made in each of the  $x$  arrangements we will get  $x \times 3!$  permutations.

Similarly, if in each of the  $x \times 3!$  permutations, the three  $i$ 's are replaced by  $i_1, i_2, i_3$  we will get  $x \times 3! 3!$  permutations.

Continuing this procedure by replacing  $n$ 's and  $s$ 's by  $n_1, n_2, s_1, s_2$  we will get  $x \times 3! 3! 2! 2!$  permutations in all.

But now all the letters are different and hence, this number must be equal to  $12!$ .

$$\therefore x \times 3! 3! 2! 2! = 12! \quad \therefore x = \frac{12!}{(3!)^2 (2!)^2}$$

Thus, we get the theorem :

**Theorem :** Given  $n$  things of which  $p$  are similar and of one type,  $q$  are similar and of another type,  $r$  are similar and of third type, the number of permutations of these  $n$  things taken all at a time is

$$\frac{n!}{p! q! r!}$$

The proof of the above theorem goes parallel to the solution of the above example.

### The number of permutations with restrictions (Conditional Permutations)

1. The number of permutations of  $n$  things taken  $r$  at a time when  $p$  particular things are always to be excluded is

$${}^{n-p} P_r$$

Since,  $p$  particular things are always to be excluded we have to select  $r$  things from  $n-p$  things only. This can be done in  ${}^{n-p} P_r$  ways. Suppose there are 10 persons and 6 chairs in a row. If two particular persons of the 10 refuse to sit then there are only 8 persons and 6 chairs. They can take the chairs in  ${}^8 C_6$  ways.

2. The number of permutations of  $n$  things taken  $r$  at a time when  $p$  (less than  $r$ ) particular things always occur together in a given order is

$$(r-p+1) {}^{n-p} P_{r-p}$$

We can consider the  $p$  particular things which occur together in a particular order as a single object. Keeping this out of consideration for a while, we have  $n-p$  things to permute and we have to take  $r-p$  things at a time. This can be done in  ${}^{n-p} P_{r-p}$  ways.

When  $r-p$  things are taken at a time there are  $r-p-1$  spaces between them and 2 spaces at the two ends i.e. in all  $r-p+1$  spaces. The single object can take any of these spaces. Hence, the total number of arrangements is

$$(r-p+1) \cdot {}^{n-p} P_{r-p}$$

Suppose there are 10 persons for a photograph and only 8 chairs. Suppose out of these 10 persons 3 are ladies and they are always to get chairs and together. We can keep out or our consideration the three ladies and their three chairs. We have to permute  $10 - 3 = 7$  persons taking 8 - 3 = 5 at a time. This can be done in  ${}^7P_5$  ways. These 5 persons create 6 spaces 4 between them and 2 at the ends. The three chairs for the three ladies can be placed at any of these spaces. Hence, the total number of permutations is

$$6 \cdot {}^7P_5$$

3. The number of permutations of  $n$  things taken  $r$  at a time when  $p$  (less than  $r$ ) particular things always occur in any order is

$${}^rP_p \cdot {}^{n-p}P_{r-p}$$

Since,  $p$  particular things are always to be included in any order, the  $r$  places can be filled by these  $p$  things in  ${}^rP_p$  ways. Now, out of  $r$  spaces  $p$  have been filled up and  $r - p$  are vacant. There are  $n - p$  things to take these spaces. These  $n - p$  things can fill  $r - p$  spaces in  ${}^{n-p}P_{r-p}$  ways. The total number of permutations therefore is

$${}^rP_p \cdot {}^{n-p}P_{r-p}$$

Suppose as before there are 10 persons and 8 chairs. Suppose further that out of 10 persons 3 are ladies to be included always. These 8 chairs can be occupied by 3 ladies in  ${}^8P_3$  ways. There are now 5 vacant chairs and 7 persons to occupy them. They can occupy these chairs in  ${}^7P_5$  ways. Therefore, the number of permutations is

$${}^8P_3 \cdot {}^7P_5$$

**Example 1 :** For each set A, find the number of permutations of A taken  $r$  members at a time.

- (i)  $A = \{1, 2, 3, 4, 5, 6, 7\}$ ,  $r = 3$ .
- (ii)  $A = \{a, b, c, d, e, f\}$ ,  $r = 2$ .

**Sol. :** (i) There are 7 things and we have take 3 at a time.

$$\therefore \text{No. of permutations} = {}^7P_3 = 7 \cdot 6 \cdot 5 = 210.$$

(ii) There are 6 things and we have to take 2 at a time.

$$\therefore \text{No. of permutations} = {}^6P_2 = 6 \cdot 5 = 30.$$

**Example 2 :** Find the sum of 4 digit numbers that can be formed with the four digits 2, 3, 4, 5 if repetitions are not allowed.

**Sol. :** Four things can be chosen from four in  ${}^4P_4 = 4 \cdot 3 \cdot 2 \cdot 1 = 24$  ways. The given four digits will occur at four places viz. ones, tens, hundreds, thousands equal number of times i.e.  $24 / 4 = 6$ .

The sum of digits =  $2 + 3 + 4 + 5 = 14$ .  $\therefore 14 \times 6 = 84$ .

Thus, the sum of digits in ones place = 84. Similar is the case in tens, hundreds, thousands place.

$$\therefore \text{Sum} = 1000 \times 84 + 100 \times 84 + 10 \times 84 + 84 = 93324.$$

## 6. Combinations

So far we have been dealing with arrangements in which the order in which things were selected played an important role. But this is not the case always. Suppose a committee of two students is to

be selected out of 4. It is obvious that the order in which the students are selected is immaterial. A committee of A and B is the same as the committee of B and A. If A, B, C, D are four students then a committee of two can be formed in the following six ways.

$$AB, AC, AD, BC, BD, CD.$$

Such a selection is called a combination.

**Definition :** A group or a set of some or all of a given number of things without considering the order of things is called combination.

The total number of combinations of  $n$  things taken  $r$  at a time is denoted by  ${}^nC_r$  or  ${}_nC_r$  or  $\binom{n}{r}$  or  $C(n, r)$ . Thus,  ${}^5C_2$  means the number of combinations of 5 things taken 2 at a time,  ${}^6C_3$  means the number of combinations of 6 things taken 3 at a time.

**To find the number of combinations of  $n$  things taken  $r$  at a time.**

Let us denote the number of combinations of  $n$  things taken  $r$  at a time by  ${}^nC_r$  and consider any one of these combinations. In this particular combination there are  $r$  things. Supposing they are all different we can arrange them in  ${}^rP_r$  ways i.e.  $r!$  ways. Hence, the number of permutations is  $r!$ .

Every such combination of  $r$  things will give rise to  $r!$  permutations. Hence, the total number of permutations of  $n$  things taken  $r$  at a time is  ${}^nC_r \times r!$ .

But we already know that the number of permutations of  $n$  things taken  $r$  at a time is

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

Thus, equating the two values of permutations of  $n$  things taken  $r$  at a time, we get

$$\begin{aligned} {}^nC_r \times r! &= {}^nP_r \\ \therefore {}^nC_r \times r! &= \frac{n!}{(n-r)!} \\ \therefore {}^nC_r &= \frac{n!}{r!(n-r)!} \end{aligned} \quad (1)$$

The above formula can also be written as

$$\begin{aligned} {}^nC_r &= \frac{n(n-1)(n-2)\dots(n-r+1)}{r!(n-r)!} \\ \therefore {}^nC_r &= \frac{n(n-1)(n-2)\dots(n-r+1)}{r!} \end{aligned} \quad (2)$$

**Corollary :**  ${}^nC_n = {}^nC_0 = 1$

(i) Putting  $r = n$  in (1) we get,

$${}^nC_n = \frac{n!}{0!(n-0)!} = \frac{n!}{0!} = 1 \quad [\because 0! = 1]$$

(ii) Putting  $r = 0$  in (1) and remembering  $0! = 1$ ,

$${}^nC_0 = \frac{n!}{0!(n-0)!} = \frac{n!}{0!} = 1.$$

The meanings of  ${}^nC_n$  and  ${}^nC_0$  may also be explained like this.  
 (i)  ${}^nC_n$  means the number of selecting all  $n$  things at a time out of  $n$  given things and this can be done in only one way by selecting all of them.  
 (ii)  ${}^nC_0$  means the number of selecting zero things out of  $n$  given things and this can be done in only one way by selecting none of them.

**Complementary combinations :** When out of say, 10 things we select a group of 3 we leave behind a group of  $10 - 3 = 7$  things. Such combinations are called complementary. We have the following relation between complementary combinations.

$${}^nC_r = {}^nC_{n-r}$$

**Proof :** We have,  ${}^nC_r = \frac{n!}{r!(n-r)!}$

Changing  $r$  to  $n-r$ , we get,

$${}^nC_{n-r} = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!r!} \text{ which is the same } {}^nC_r$$

$$\therefore {}^nC_r = {}^nC_{n-r}$$

**Alternatively :**  ${}^nC_r$  denotes the number of selections of  $n$  things taken  $r$  at a time. When we select a group of  $r$  things out of  $n$  we leave a group of  $(n-r)$  things behind. This is true for each of our selections. Whenever we select a group of  $r$  things we create another group of  $(n-r)$  things. Hence, the number of these two types of groups must be equal.

$$\text{i.e., } {}^nC_r = {}^nC_{n-r}$$

**Note ...**

1. The formula  ${}^nC_r = {}^nC_{n-r}$  helps us to simplify numerical calculations. Thus,

$${}^{18}C_{15} = \frac{18 \cdot 17 \cdot 16 \dots \text{to } 15 \text{ terms}}{1 \cdot 2 \cdot 3 \dots 14 \cdot 15} \text{ which is tedious to write. But by the above formula,}$$

$${}^{18}C_{15} = {}^{18}C_3 = \frac{18 \cdot 17 \cdot 16}{1 \cdot 2 \cdot 3} \text{ which can be easily calculated.}$$

2. If  ${}^nC_x = {}^nC_y$  then either the two combinations are made up of the same number of things i.e.,  $x = y$  or they are complementary i.e.,  $x = n - y$  or  $x + y = n$ .

## 7. Combinations with Restrictions (Conditional Combinations)

In certain problems on combinations we are given a condition that certain things are always to be included in the group or that certain things are always to be excluded from the group.

1. The number of combinations of  $n$  different things taken  $r$  at a time when  $p$  particular things are always to be included is  ${}^{n-p}C_{r-p}$ .

$p$  things are always to be included means we have only to select  $r-p$  things out of  $n-p$ . This can be done in  ${}^{n-p}C_{r-p}$  ways. Suppose we have to form a committee of 5 members out of the 15 members of Gymkhana Council and the committee is to include the general secretary and the cricket secretary always. We therefore have only to select 3 members from 13 members of the council and this can be done in  ${}^{13}C_3$  ways.

2. The number of combinations of  $n$  different things taken  $r$  at a time, when  $p$  particular things are always to be excluded is  ${}^{n-p}C_r$ .

Since, every combination is to exclude  $p$  particular things we are to select  $r$  things out of the remaining  $n-p$  things. Thus, in the above example if the general secretary and cricket secretary are to be excluded from the committee we have to select 5 members from 13 members and this can be done in  ${}^{13}C_5$  ways.

3. The number of combinations of  $n$  things taken  $r$  at a time, when  $p$  particular things are always to be included and  $q$  particular things are always to be excluded is  ${}^{n-p-q}C_{r-p-q}$ .

$p$  things are always to be included means we have freedom to select  $r-p$  things out of  $n-p$  things. Since,  $q$  things are always to be excluded means we have to keep those things out of our consideration i.e. we have to select  $r-p$  things out of  $n-p-q$  things and this can be done in  ${}^{n-p-q}C_{r-p-q}$  ways. If in the above example out of 15 members of Gymkhana Council, two members are always to be included and if say three particular members are always to be excluded then a committee of 5 members can be formed in  ${}^{15-2-3}C_{5-2}$  i.e.  ${}^{10}C_3$  ways.

4. The number of combinations of  $n$  different things taken some or all at a time is  $2^n - 1$ .

Each of the  $n$  things can be dealt with in two ways, either it is selected in the group or it is not selected. Hence, by the fundamental theorem the number of such combinations =  $2 \times 2 \times 2 \dots n$  times =  $2^n$ .

But this includes the case of rejecting all of them.

Hence, the total number of combinations of  $n$  things taken some or all at a time =  $2^n - 1$ .

5. The number of combinations of  $n$  things taken some or all at a time when  $n_1$  are alike and of one kind,  $n_2$  are alike and of another kind and so on i.e.  $n = n_1 + n_2 + \dots + n_k$  is  $(n_1 + 1)(n_2 + 1) \dots (n_k + 1) - 1$ .

Consider, first the group of  $n_1$  things. We can select 0, 1, 2, ...,  $n_1$  of them i.e. the selection of some or all of them can be done in  $(n_1 + 1)$  ways. Similarly,  $n_2$  things of the second kind can be selected some or all at a time in  $(n_2 + 1)$  ways. Proceeding in this manner and using the fundamental principle. The number of ways some or all things out of  $n$  can be selected is  $(n_1 + 1)(n_2 + 1) \dots (n_k + 1)$ .

But this includes the case of rejecting all of them. Hence, the required number of ways in which some or all of things out of  $n$  can be selected is  $(n_1 + 1)(n_2 + 1) \dots (n_k + 1) - 1$ .

**Example 1 :** In how many ways a committee of three faculty members and two students can be formed from 7 faculty members and 8 students?

**Sol. :** Three faculty members out of 7 can be selected in  ${}^7C_3$  ways.

Two students out of 8 can be selected in  ${}^8C_2$  ways.

$$\therefore \text{Total number of ways} = {}^7C_3 \times {}^8C_2$$

**Example 2 :** Number of diagonals in a polygon is 44. Find the number of sides of the polygon.

**Sol. :** If there are  $n$  points in a plane, no three of which are collinear, they can be connected in  ${}^nC_2$  ways. Thus, from  $n$  points we get  ${}^nC_2$  segments. But  $n$  of them form the sides of the polygon. Hence, the number of diagonals in this polygon =  ${}^nC_2 - n$ . But there are 44 diagonals.

$$\therefore {}^nC_2 - n = 44 \quad \therefore \frac{n(n-1)}{2} - n = 44$$

$$\begin{aligned} n^2 - n - 2n &= 88 \\ (n-11)(n+8) &= 0 \end{aligned}$$

Since  $n = -8$  is absurd the number of sides of the polygon = 11.

**Example 3 :** Of ten electric bulbs, three are defective but it is not known which are defective. In how many ways can three bulbs be selected? How many of these selections will include at least one defective bulb?

**Sol. :** Three bulbs out of 10 can be selected in  ${}^{10}C_3$  ways.

There are seven non-defective bulbs. Three bulbs out of these seven can be selected in  ${}^7C_3$  ways.

$\therefore$  No. of ways of selecting at least one defective

$${}^{10}C_3 - {}^7C_3 = 120 - 35 = 85.$$

**Example 4 :** A box contains 7 red, 6 white and 4 blue balls. How many selections of three balls can be made so that (i) none is red, (ii) one is of each colour?

**Sol. :** There are in all 17 balls. If no red ball is to be selected, we have to select 3 balls from the remaining 10 (6 white and 4 blue). This can be done in  ${}^{10}C_3$  ways = 120.

If we have to select one ball of each colour the number of selections

$$= {}^7C_1 \times {}^6C_1 \times {}^4C_1 = 7 \times 6 \times 4 = 168$$

**Example 5 :** How many different 8 card-hands with 5 red cards and 3 black cards can be dealt from a pack of 52 cards?

**Sol. :** There are 26 red cards and 26 black cards.

Out of 26 red cards 5 cards can be had in  ${}^{26}C_5$  ways.

Out of 26 black cards, 3 black cards can be had in  ${}^{26}C_3$  ways.

$$\therefore \text{Total number of ways} = {}^{26}C_5 \times {}^{26}C_3 \text{ ways.}$$

## PROBABILITY

### 1. Introduction

The words *probably*, *likely*, *possibly* are common in our everyday conversation. We say, "I shall probably get first class". "It is likely to rain today". "It is possible that the price of sugar will rise". Each one of these statements indicates the chance of an event. We human beings are interested to know as much as possible about the events that are going to happen in future. The science of probability tries to measure the probability or likelihood of such events.

#### (a) A-priori or Classical or Mathematical Definition of Probability

**Definition :** If an experiment results in any one of  $n$  exhaustive, mutually exclusive and equally likely events and if  $m$  of them are favourable to an event  $A$ , then the probability of  $A$  denoted by  $P(A)$  is equal to the ratio  $m/n$ .

Thus,

$$P(A) = \frac{m}{n}.$$

This definition is sometimes called *A-priori* (based on reasoning or not based on experience) or *Classical or Mathematical* definition because it is not based on experiment but on reasoning and intuition.

#### (b) A-posteriori or Empirical or Statistical Definition of Probability

If a trial is repeated under identical conditions, then the limit of the ratio of the number of times the event occurs, to the number of trials, as the number of trials becomes infinitely large, is called the probability of that event.

Thus, if a trial is repeated  $n$  times and if  $A$  occurs  $m$  times then the limit of the ratio  $m/n$  as  $n$  tends to infinity is called the probability of  $A$  and is denoted by  $P(A)$ .

$$\therefore P(A) = \lim_{n \rightarrow \infty} \left( \frac{m}{n} \right)$$

(It is assumed that the limit is finite and unique). This definition is called *A-posteriori* (based on experience) or *Empirical* or *Statistical* definition.

#### (c) Axiomatic Definition of Probability

Let  $E$  be a random experiment and  $S$  be the sample space. We define the probability  $P(A)$  of event  $A$  of  $S$  satisfying the following axioms :

1.  $P(A) \geq 0$  (Axiom 1)
2.  $P(S) = 1$  (Axiom 2)
3.  $P(A \cup B) = P(A) + P(B)$  (Axiom 3)

If  $A$  and  $B$  are any two exclusive events (i.e. they are disjoint sets).

**Explanation :** The first axiom states that the probability of any event is greater than zero, which means the probability of any event cannot be negative.

The second axiom states that the sum of the probabilities of all events is equal to one. This together with the first axiom states that the probability of an event must be less than or equal to one

i.e.,

$$P(A) \leq 1$$

The third axiom states that if two events are mutually exclusive then the probability that either of them will occur is equal to the sum of their probabilities.

For our study the classical definition is sufficient. We give that definition in terms of sets again for ready reference.

**Definition :** If a sample space  $S$  has  $n$  points which are equally likely and mutually exclusive and an event  $A$  of  $S$  has  $m$  points then the ratio  $m/n$  is called probability of  $A$  and is denoted by  $P(A)$ . [Fig. 1.20 (a)]

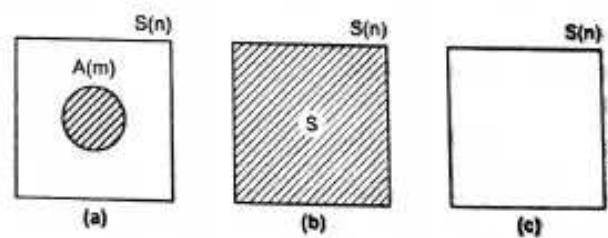


Fig. 1.20

Thus,

$$P(A) = \frac{m}{n} = \frac{\text{number of points in } A}{\text{number of points in } S}$$

**Note ...**

We shall be concerned with only such random experiments in which all sample points are equally likely. And to find the probability of an event in such a random experiment we need to know the number of points in sample space  $S$  and the number of points in the event  $A$ .

We shall now prove some theorems on probability of events using these axioms. It should be noted that while proving these theorems we can use only the axioms and the theorems proved earlier. Also we note that the left hand sides of the theorems give symbolic expressions of the verbal statements and the right hand sides give the formulae for evaluation of these probabilities.

We need the following two results known as Laws of Distribution.

$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \end{aligned}$$

**2. Theorems on Probability of Events**

**Theorem 1 : Probability of an impossible event is zero i.e.  $P(\Phi) = 0$ .**

An event which has no sample points is called an impossible event and is denoted by  $\Phi$ .

We have  $S \cup \Phi = S \quad \therefore P(S \cup \Phi) = P(S)$

But  $S$  and  $\Phi$  are exclusive events.

$$\therefore P(S) + P(\Phi) = P(S) \quad [\text{By Axiom 3}]$$

$$\therefore P(\Phi) = 0.$$

Thus, we have two important results,

$$P(S) = 1 \quad [\text{By Axiom 2}] \quad \text{and} \quad P(\Phi) = 0$$

**Complementary Events :** The events  $A$  and  $\bar{A}$  where  $\bar{A}$  is the complement of  $A$  in  $S$  are called complementary events.

$$\text{Theorem 2 : } P(\bar{A}) = 1 - P(A)$$

**Proof :** Since  $A \cup \bar{A} = S$ ,  $P(A \cup \bar{A}) = P(S)$ .

But  $P(S) = 1$  and  $A, \bar{A}$  are exclusive.

By Axiom 2,

$$P(S) = P(A \cup \bar{A}) = P(A) + P(\bar{A})$$

$$\therefore P(A) + P(\bar{A}) = 1$$

$$\therefore P(\bar{A}) = 1 - P(A)$$

**Note ...**

Since  $A$  and  $\bar{A}$  are exclusive, we have  $A \cup \bar{A} = S$  and  $A \cap \bar{A} = \Phi$ .

**Corollary :** Probability of an event is always less than or equal to one.

$$\text{i.e., } P(A) \leq 1$$

**Proof :**  $P(A) = 1 - P(\bar{A})$ . But  $P(\bar{A}) \geq 0$  by axiom 1.

$$\therefore P(A) \leq 1.$$



Fig. 1.21

**Remark ...**

**Not Both and Both Not  $A$  and  $B$  :** Note that the events  $A$  and  $B$  'that not both will happen' and 'that both will not happen' have significantly different meanings. The first is symbolised as  $\bar{A} \cap \bar{B}$  and the second is symbolised as  $\bar{A} \cap \bar{B}$ .

**De Morgan's Law's :** Since an event is a subset of sample space De Morgan's Laws are applicable to events. Thus, we have

$$P(\bar{A} \cup \bar{B}) = P(\bar{A} \cap \bar{B})$$

$$P(\bar{A} \cap \bar{B}) = P(\bar{A} \cup \bar{B})$$

**Example 1 :** What is the chance that a leap year selected at random will contain 53 Sundays?

(M.U. 1996, 2003, 04, 05)

**Sol. :** A leap year has 52 complete weeks and 2 more days. These days can be Monday and Tuesday, Tuesday and Wednesday, Wednesday and Thursday, Thursday and Friday, Friday and Saturday, Saturday and Sunday, Sunday and Monday. Let the required event be denoted by  $A$ .

There are 7 outcomes and 2 are in  $A$ .

$$\therefore n = 7 \quad \text{and} \quad m = 2 \quad \therefore P(A) = \frac{m}{n} = \frac{2}{7}.$$

**Example 2 :** In the play of two dice, a person loses if the sum obtained is 2 or 4 or 12. He wins if the sum is 5 or 11. Find the ratio of his probability of losing to the probability of winning in the first throw.

**Sol. :** When two dice are thrown simultaneously there are 36 cases as shown below,

(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6),

(2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (2, 6),

(3, 1), (3, 2), (3, 3), (3, 4), (3, 5), (3, 6),

(4, 1), (4, 2), (4, 3), (4, 4), (4, 5), (4, 6),

(5, 1), (5, 2), (5, 3), (5, 4), (5, 5), (5, 6),

(6, 1), (6, 2), (6, 3), (6, 4), (6, 5), (6, 6).

The sum 2 is obtained in only one way - (1, 1). The sum 4 is obtained in 3 ways - (1, 3), (2, 2), (3, 1). The sum 12 is obtained in only one way - (6, 6).

$$\therefore m = 1 + 3 + 1 = 5, \quad n = 36 \quad \therefore P(\text{losing}) = \frac{m}{n} = \frac{5}{36}.$$

The sum 5 is obtained in 4 ways - (1, 4), (2, 3), (3, 2), (4, 1). The sum 11 is obtained in 2 ways - (5, 6), (6, 5).

$$\therefore m = 4 + 2 = 6, \quad n = 36 \quad \therefore P(\text{winning}) = \frac{m}{n} = \frac{6}{36}.$$

$$\text{Ratio of probability of losing to probability of winning} = \frac{P(\text{losing})}{P(\text{winning})} = \frac{5/36}{6/36} = \frac{5}{6}.$$

**Example 3 :** Seven persons including A and B stand in a line for a photograph. Find the probability that there are exactly two persons between A and B.

Sol.: Seven persons can stand in a row in  ${}^7C_7$  ways = 7! ways.  $\therefore n = 7!$   
If there are two persons between A and B, there are the following 4 cases

A ★ ★ B ★ ★  
★ A ★ ★ B ★ ★  
★ ★ A ★ ★ B ★  
★ ★ ★ A ★ ★ B

But in these 4 ways A and B can interchange the positions. Hence, there are 2 ways. The remaining 5 persons can interchange the positions in  ${}^5C_5$  ways = 5! ways.

$\therefore$  The number of favourable cases  $m = 4 \times 2 \times 5!$

$$\therefore P(A) = \frac{m}{n} = \frac{4 \times 2 \times 5!}{7!} = \frac{4 \times 2}{7 \times 6} = \frac{4}{21}.$$

### 3. Laws of Probability

There are two laws. The probability of A or B i.e.  $P(A \cup B)$  is given by the law of addition and the probability of A and B i.e.  $P(A \cap B)$  is given by the law of multiplication.

Theorem 3 : For any two events A and B the probability that exactly B will occur is given by

$$P(B \cap \bar{A}) = P(B) - P(A \cap B)$$

and that exactly A will occur is given by

$$P(A \cap \bar{B}) = P(A) - P(A \cap B)$$

Proof : To prove this result we first express the event B as the union of two exclusive events  $A \cap B$  and  $\bar{A} \cap B$ .

$$\therefore B = (A \cap B) \cup (\bar{A} \cap B)$$

Since the events on the r.h.s. are exclusive

$$P(B) = P(A \cap B) + P(\bar{A} \cap B) \quad [ \text{By Axiom 3} ]$$

$$\therefore P(B \cap \bar{A}) = P(B) - P(A \cap B)$$

Similarly, we can prove that

$$P(A \cap \bar{B}) = P(A) - P(A \cap B)$$

Theorem 4 : Addition Theorem (Two Events)

Probability that at least one of the events A and B will occur is given by

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

Proof : We first express the event  $A \cup B$  as the union of two exclusive events  $A$  and  $\bar{A} \cap B$ .

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

$$\therefore P(A \cup B) = P[A \cup (\bar{A} \cap B)]$$

But the events on the r.h.s. are mutually exclusive.

$$\begin{aligned} \therefore P(A \cup B) &= P(A) + P(\bar{A} \cap B) \\ &= P(A) + P(B) - P(A \cap B) \end{aligned} \quad [ \text{By Axiom 3} ] \quad [ \text{By Theorem 2} ]$$

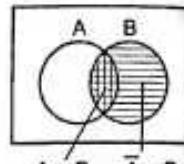


Fig. 1.22

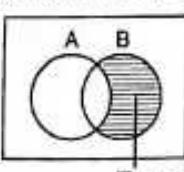


Fig. 1.23

Corollary 1 : If A and B are two mutually exclusive events then the probability that either A or B will happen is the sum of the probabilities of A and B.

$$\text{i.e., } P(A \cup B) = P(A) + P(B)$$

Proof : Since events are exclusive  $A \cap B = \emptyset$ .

$$\therefore P(A \cap B) = P(\emptyset) = 0$$

[ By Theorem 1 ]

Hence, from the above theorem,

$$P(A \cup B) = P(A) + P(B)$$

Corollary 2 : If A, B, C, ..., K are mutually exclusive events such that their union is the whole of sample space then

$$P(A) + P(B) + P(C) + \dots + P(K) = 1$$

Proof : Since  $A \cup B \cup C \cup \dots \cup K = S$

$$\therefore P(A \cup B \cup C \cup \dots \cup K) = P(S)$$

Since, events are mutually exclusive, we get, from above,

$$P(A) + P(B) + P(C) + \dots + P(K) = P(S)$$

$$\text{But } P(S) = 1$$

[ By Axiom 2 ]

$$\therefore P(A) + P(B) + P(C) + \dots + P(K) = 1$$

Note ...

The group of all possible events A, B, C, ..., K of the sample space S such that

$$P(A) + P(B) + P(C) + \dots + P(K) = 1$$

is called exhaustive. e.g. in the toss of a coin H, T; in the toss of a dice 1, 2, 3, 4, 5, 6 are exhaustive events.

Corollary 3 :  $P(A \cap B) \geq P(A) + P(B) - 1$

Proof : Since  $P(A \cup B) \leq 1$ .

[ By Cor. page 1-26 ]

$$P(A) + P(B) - P(A \cap B) \leq 1.$$

$$\therefore P(A \cap B) \geq P(A) + P(B) - 1.$$

Theorem 5 : Addition Theorem (Three Events)

If A, B, C are any three events then the probability that at least one of them will occur is given by

$$P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(B \cap C) - P(C \cap A) + P(A \cap B \cap C).$$

Proof : The theorem can be proved using the theorem 4.

### 4. Conditional Probability

Consider general case of conditional probability (See Fig. 1.26, page 1-31). Let  $n$  = the number of points in  $S$ ,  $m_1$  = number of points in  $A$ ,  $m_2$  = number of points in  $B$ ,  $m_{12}$  = number of points in  $A$  and  $B$  both.

$$\text{Then, } P(A) = \frac{m_1}{n}, \quad P(B) = \frac{m_2}{n} \quad \text{and} \quad P(A \cap B) = \frac{m_{12}}{n}.$$

Now, suppose in a trial we know the result partially i.e. we know that A has occurred. What is the probability now that B has occurred along with A ?

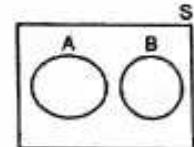


Fig. 1.24

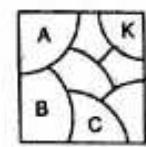


Fig. 1.25

Since we know that  $A$  has occurred the outcome of the trial is one of those points in  $A$ . i.e., one of  $m_1$  (and not  $n$ ). And of these,  $m_{12}$  are in  $B$ . Hence, the probability that  $B$  will occur, when  $A$  has already occurred is  $(m_{12} / m_1)$ . This is called conditional probability of  $B$  under the condition that  $A$  has occurred. It is denoted by  $P(B/A)$ .

$$\text{Thus, } P(B/A) = \frac{m_{12}}{m_1}$$

**Definition :** Let  $A$  and  $B$  be any two events in a sample space  $S$ . The probability that  $B$  will occur, given that  $A$  has already occurred is called the **conditional probability of  $B$**  and is denoted by  $P(B/A)$ .

Similarly the probability that  $A$  will occur given that  $B$  has already occurred is called the **conditional probability of  $A$**  and is denoted by  $P(A/B)$ .

**Example :** Suppose there are 100 students in a class and the results of an examination of the class are given in the following table.

	Passed	Failed	Total
Boys	28	32	60
Girls	26	14	40
Total	54	46	100

Let us define two events  $A$ ,  $B$  as follows :

$A$  = a student has passed,  $B$  = a student is a male student.

Suppose a student is selected at random and is known to be a male student. What is the probability that this student has passed? In symbols, we want to find  $P(A/B)$ .

Since the student is a male student, the sample space of  $B$  has 60 points. Of these 28 have passed i.e.,  $A$  has now 28 points. Hence,

$$\therefore P(A/B) = \frac{28}{60} = \frac{7}{15}$$

But, from the table we see that 28 is the number of points in  $A \cap B$  and 60 is the number of points in  $B$ .

$$P(A/B) = \frac{\text{No. of points in } A \cap B}{\text{No. of points in } B} \quad \dots \dots \dots (1)$$

$$\text{or } P(A/B) = \frac{\text{No. of points in } A \text{ out of } B}{\text{No. of points in } B} \quad \dots \dots \dots (2)$$

Similarly, we can find that

$$P(B/A) = \frac{\text{No. of points in } B \cap A}{\text{No. of points in } A} \quad \dots \dots \dots (3)$$

$$\text{or } P(B/A) = \frac{\text{No. of points in } B \text{ out of } A}{\text{No. of points in } A} \quad \dots \dots \dots (4)$$

Further, we see that, (1) can be written as

$$P(A/B) = \frac{(\text{No. of points in } A \cap B) / \text{No. of points in } S}{(\text{No. of points in } B) / \text{No. of points in } S}$$

$$\therefore P(A/B) = \frac{P(A \cap B)}{P(B)} \quad \text{Similarly, from (3) we can get } P(B/A) = \frac{P(A \cap B)}{P(A)}$$

From these we get

$$P(A \cap B) = P(A/B) \times P(B) \quad \text{and} \quad P(A \cap B) = P(B/A) \times P(A)$$

which is called the law of multiplication of probability.

**Theorem 7 : Multiplication Theorem**

If  $A$  and  $B$  are two events and neither is null then the probability that both of them will occur is given by

$$P(A \cap B) = P(A) \times P(B/A) \quad \text{or} \quad P(A \cap B) = P(B) \times P(A/B)$$

where  $P(A/B)$  and  $P(B/A)$  denote the conditional probabilities which are greater than zero.

**Proof :** Let the number of points in  $A$  be  $m_1$  and those in  $B$  be  $m_2$ . Let the number of points in  $(A \cap B)$  be  $m_{12}$  and let  $n$  be the total number of points in  $S$ .

$$P(A) = \frac{m_1}{n}, \quad P(B) = \frac{m_2}{n}$$

To find the probability of  $B$  when  $A$  has happened, we have to consider the sample space of  $A$  which has  $m_1$  points. In this sample space only  $B$  can occur (along with  $A$ ) which has  $m_{12}$  points.

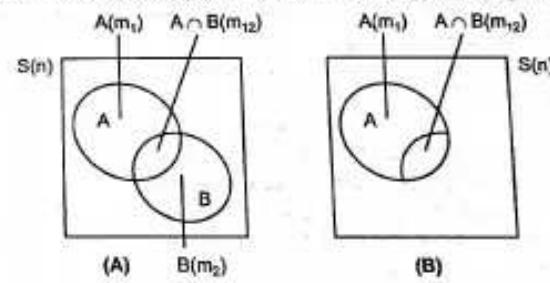


Fig. 1.26

$$\therefore P(B/A) = \frac{\text{No. of points in } A \cap B}{\text{No. of points in } A} = \frac{m_{12}}{m_1}$$

$$\text{Now, } P(A \cap B) = \frac{m_{12}}{n} = \frac{m_1}{n} \times \frac{m_{12}}{m_1} \quad \therefore P(A \cap B) = P(A) \times P(B/A)$$

Similarly, we can prove that  $P(A \cap B) = P(B) \times P(A/B)$ .

## 5. Independent Events

Two events are said to be **independent** of each other if the occurrence or non-occurrence of one does not affect the occurrence of the other in any way. For example, if a coin is tossed twice the result of the second throw is in no way affected by the result of the first. If the occurrence of one event affects the occurrence of the other the events are called **dependent**. Suppose a box contains only one white ball and some black balls. Suppose two balls are drawn one after the other without replacement. Suppose  $A$  is the event getting a black ball in the first draw and  $B$  is the event getting the white ball in the second draw. Then the occurrence of  $B$  depends upon  $A$ .  $B$  can occur only if  $A$  has occurred. If  $A$  has not occurred  $B$  cannot occur.

If  $A, B$  are independent events then the conditional probability of  $A$  when  $B$  has happened is same as  $P(A)$  and also the conditional probability of  $B$  when  $A$  has happened is same as  $P(B)$ . This fact is used to define independence of two events.

- (a) **Definition**  
Two events  $A, B$  are said to be independent ( $P(A) \neq 0, P(B) \neq 0$ ) if

$$P(A/B) = P(A) \quad \text{and} \quad P(B/A) = P(B)$$

#### Multiplication Law (For Independent Events)

For two events  $A$  and  $B$  which are independent the probability that both  $A$  and  $B$  will occur is given by :

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

Proof : We know that  $P(A \cap B) = P(A) \times P(B/A)$

But since the events are independent,  $P(B/A) = P(B)$

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

Note ...

Sometimes this law is taken as the definition of independent events.

#### (b) Independence and Exclusiveness

Independence and exclusiveness of two events  $A$  and  $B$  are two entirely different concepts. For exclusiveness the condition is

$$P(A \cap B) = 0$$

and for independence the condition is  $P(A \cap B) = P(A) \times P(B)$ .

If  $A$  and  $B$  are exclusive events they cannot be independent.

If  $A$  and  $B$  are exclusive,  $P(A \cap B) = 0$ . But since  $P(A) \neq 0$  and  $P(B) \neq 0$  we cannot have  $P(A \cap B)$  and  $P(A) \times P(B)$  equal. Hence,  $A, B$  are not independent.

If  $A$  and  $B$  are independent, they cannot be exclusive.

If  $A$  and  $B$  are independent  $P(A \cap B) = P(A) \times P(B)$ . But since  $P(A) \neq 0$  and  $P(B) \neq 0$  we cannot get  $P(A \cap B) = 0$ . Hence,  $A, B$  are not exclusive.

**Example 1 :** If  $P(A) = 0.3, P(B) = 0.5$ , find  $P(A \cup B)$  when (i)  $A, B$  are exclusive (ii)  $A, B$  are independent.

**Sol. :** (i) If  $A, B$  are exclusive  $P(A \cap B) = 0$

$$\begin{aligned} P(A \cup B) &= P(A) + P(B) - P(A \cap B) \\ &= 0.3 + 0.5 - 0 = 0.8 \end{aligned}$$

(ii) If  $A, B$  are independent  $P(A \cap B) = P(A) \times P(B)$

$$\begin{aligned} P(A \cup B) &= P(A) + P(B) - P(A) \times P(B) \\ &= 0.3 + 0.5 - 0.3 \times 0.5 = 0.65 \end{aligned}$$

(Note that  $P(A \cup B)$  has two different values under the two conditions.)

## Prime Numbers

### 1. Introduction

In this and the next chapter, we are going to be acquainted with some concepts in number theory. Number theory is a branch of mathematics that deals with the properties of integers, especially the properties of positive integers. Number theory was once considered as 'purest' part of mathematics, but now it has found ever increasing applications in Cryptography and Computer Science.

We shall accept the following laws of addition and multiplication of integers :

If  $a, b, c$  are integers, we have,

$$(i) \text{ Associative Law : } (a + b) + c = a + (b + c)$$

$$(ab)c = a(bc)$$

$$(ii) \text{ Commutative Law : } a + b = b + a$$

$$ab = ba$$

$$(iii) \text{ Distributive Law : } a(b+c) = ab+ac$$

We have two integers 0 and 1 with some special properties :

(iv) **Additive Identity 0 and multiplicative Identity 1** : They are defined by the following properties :

$$a + 0 = 0 + a = a \quad \text{and} \quad a \cdot 1 = 1 \cdot a = a$$

(v) **Additive Inverse** : For every integer  $a$ , we have an integer  $-a$ , such that

$$a + (-a) = (-a) + a = 0.$$

We also assume the following property for integers.

**The Well Ordering Property** : Every non-empty set of non-negative integers has smallest integer.

For example, the set of positive integers has 1 as the smallest integer. The set of positive even numbers has 2 as the smallest integer. The set of all integers, positive and negative has no such smallest integer.

### 2. Divisibility

When we divide an integer by another integer, the quotient may or may not be an integer.

For example,  $\frac{35}{5} = 7$ . But  $\frac{18}{4} = 4$  remainder 2.

From this observation, we define divisibility as follows :

**Definition** : If  $a$  and  $b$  are any two integers with  $a \neq 0$ , such that  $b = ka$  where  $k$  is an integer, then we say that  $a$  divides  $b$  or  $b$  is divisible by  $a$  or  $b$  is a multiple of  $a$ .

- When  $a$  divides  $b$ , we write  $a \mid b$ . When  $a$  does not divide  $b$ , we write  $a \nmid b$ . For example,
- 56 is divisible by 7, in notation  $7 \mid 56$ , because  $56 = 8 \times 7$ .
  - 15 divides 135, in notation  $15 \mid 135$ , because  $135 = 9 \times 15$ .
  - 224 is a multiple of 16, in notation  $16 \mid 224$ , because  $224 = 14 \times 16$ .
  - $-8$  is a divisor of 72, in notation  $-8 \mid 72$ , because  $72 = (-9)(-8)$ .
  - 66 is divisible by  $-11$ , in notation  $-11 \mid 66$ , because  $66 = (-6)(-11)$ .

**Note ...**

- It is clear that if  $b = ka$ , then  $b = (-k)(-a)$ , therefore,  $a \mid b$  if and only if  $(-a) \mid b$ .
- Since  $0 = a \cdot 0$ ,  $a \mid 0$  for every  $a \neq 0$ .

**Theorem 1 :** The divisibility has the following properties :

If  $a, b, c$  are integers, then

- $a \mid b, b \mid c$  implies  $a \mid c$
- $c \mid a, c \mid b$  implies  $c \mid ma + nb$  for any integers  $m$  and  $n$
- $a \mid 0$ , if  $a \neq 0$

**Proof :** 1. By the definition of divisibility,  $a \mid b$  means there is an integer  $k$ , such that  $b = ka$ . Similarly,  $b \mid c$  means, there is an integer  $k'$ , such that  $c = k'b$ . Therefore, together they mean  $c = k'ka = k''a$  (say). Hence,  $a \mid c$ .

2. Since  $c \mid a$  and  $c \mid b$ , we have integers  $k$  and  $k'$ , such that  $a = kc$  and  $b = k'c$ . Therefore, for any integers  $m$  and  $n$ , we have

$$\begin{aligned} ma + nb &= m(kc) + n(k'c) \\ &= (mk)c + (nk')c \\ &= (mk + nk')c \\ &= k''c \text{ (say)} \end{aligned}$$

This means,  $c \mid ma + nb$ .

3. Since division by 0 is 'illegal', we assume  $a \neq 0$ . Choose  $k = 0$ , we have  $0 = 0 \cdot a = ka$ . Hence,  $a \mid 0$ .

**Illustrations :**

- $7 \mid 56$  and  $56 \mid 168$ . Hence,  $7 \mid 168$ .

We can verify that  $56 = 8 \times 7$ ,  $168 = 3 \times 56$  and  $168 = 3 \times 8 \times 7 = 24 \times 7$ .

- Since  $5 \mid 25$  and  $5 \mid 50$ , we have  $5 \mid 4 \times 25 + 7 \times 50 = 450$ .

**3. Division Algorithm**

**Theorem :** Let  $a$  and  $b$  be integers with  $b > 0$ . Then, there exist unique integers  $q$  and  $r$ , such that  $a = qb + r$ ,  $0 \leq r < b$ .

**Proof :** Consider the set  $S = \{a - xb \mid x \text{ is an integer}, a - xb \geq 0\}$

Clearly,  $S$  is a set of non-negative integers. We further claim that,  $S$  is non-empty. Since  $b > 0$ , we have  $b \geq 1$  and therefore,  $|a| \geq |a|$ , for any integer  $a$ . Hence, we have

$$a - (-|a|)b = a + |a|b \geq a + |a| \geq 0.$$

Therefore, if we choose  $-|a| = x$ , then  $a - xb \geq 0$  and  $S$  contains  $a - xb$ .

Since  $S$  is a non-empty set of non-negative integers,  $S$  contains, by the well-ordering principle, the smallest non-negative integer, say,  $r$ . Therefore, by the nature of elements in  $S$ , there exists an integer  $q$ , such that

$$r = a - qb; \quad 0 \leq r$$

Our claim is  $r < b$ .

Suppose our claim is not true. Then  $r \geq b$ ; i.e.,  $r - b \geq 0$ . Then

$$a - (q+1)b = (a - qb) - b = r - b \geq 0$$

Therefore,  $a - (q+1)b$  lies in  $S$ .

But then we have  $a - (q+1)b = r - b < r$ , as  $b$  is a positive integer. This contradicts the smallestness of  $r$  in  $S$ . Hence, our claim is wrong and thus,

$$0 \leq r < b$$

The proof of the theorem is complete, if we show the uniqueness of  $q$  and  $r$ , satisfying conditions (i) and (ii).

Let, if possible, there be integers  $q'$  and  $r'$ , such that

$$r' = a - q'b; \quad 0 \leq r' < b$$

From (i) and (iii), we get

$$(r - r') = (q - q')b.$$

Taking absolute values, we have

$$|r - r'| = |q - q'|b = |q - q'|b$$

On the other hand inequalities in (ii) and (iii) yield  $-b < r - r' \leq 0$  and  $0 \leq r' < b$ , and therefore,  $-b < r' - r < b$  or  $|r' - r| < b$ .

Therefore, from (iv), we have

$$|q - q'|b = |r' - r| < b.$$

This leads to  $|q - q'| < 1$ . Since,  $|q - q'|$  cannot be negative, the only possibility remaining is  $|q - q'| = 0$  i.e.,  $q = q'$ .

This together with (iv) yields  $|r - r'| = 0$  or  $r = r'$ . Hence, the uniqueness of  $q$  and  $r$  in (i).

**Definition :** If for an integer  $a$  and  $b$ ,  $a = qb + r$ ;  $0 \leq r < b$ , then,  $q$  is called the quotient and  $r$  is called the remainder of the division of  $a$  by  $b$ .

**Remark ...**

- Let  $a > 1$  be any given integer, choosing  $b = 2$ , we observe that  $r$  can take only two values 0 and 1. Therefore,  $a = 2n$  or  $a = 2n + 1$  for some fixed  $n$ . Choosing  $b = 3$ , we find  $r$  takes only 3 values 0, 1, 2. Therefore,  $a = 3n$  or  $a = 3n + 1$  or  $a = 3n + 2$  for some fixed  $n$ . Similarly, we have

$$a = 4n, \quad a = 4n + 1, \quad a = 4n + 2 \text{ or } a = 4n + 3.$$

$$a = 5n, \quad a = 5n + 1, \quad a = 5n + 2, \quad a = 5n + 3 \text{ or } a = 5n + 4.$$

This property has great applications in modular arithmetic.

- The division algorithm can be extended to integers  $b$ , even when  $b < 0$ .

Any integer  $a$  and  $b \neq 0$  can be written in the form

$$a = qb + r, \quad 0 \leq r < |b|$$

For example, if  $a = 31$ ,  $b = -5$ , then  $31 = (-6) \times (-5) + 1$ ;  $0 < 1 < |-5|$ .

Similarly, we have  $90 = (-11) \times (-8) + 2$ ;  $0 < 2 < |-8|$ .

**Example 1 :** Given  $a$  and  $b$ , express them in the form  $a = qb + r$ ;  $0 \leq r < b$ .

- (i)  $0, 22$ , (ii)  $-13, 5$ , (iii)  $-44, -5$ , (iv)  $-195518, 22$ , (v)  $100, 999$
- Sol. : (i)  $0 = 0 \times 22 + 0$ ,  $0 < 22$ .
- (ii)  $-13 = -3 \times 5 + 2$ ,  $0 < 2 < 5$
- (iii)  $-44 = 9 \times -5 + 1$ ,  $0 < 1 < |-5|$
- (iv)  $-195518 = -8888 \times 22 + 18$ ,  $0 < 18 < 22$
- (v)  $100 = 0 \times 999 + 100$ ,  $0 < 100 < 999$

**Example 2 :** Prove that the product of 3 consecutive integers is divisible by 3.

**Sol. :** Consider three consecutive integers  $a, a+1, a+2$ .

By division algorithm,  $a = 3k + r$ ,  $0 \leq r < 3$

Thus,  $a$  is one of the following 3 forms :

- (i)  $a = 3k$ , (ii)  $a = 3k+1$ , (iii)  $a = 3k+2$ .

In the first case, clearly  $3 \mid a$ . In the second case,  $a+2 = 3k+3 = 3(k+1)$ . Hence,  $3 \mid a+2$ .

In the third case  $a+1 = 3k+3 = 3(k+1)$ . Hence,  $3 \mid a+1$ .

Therefore, 3 divides either  $a$  or  $a+1$  or  $a+2$ . Hence, their product.

### EXERCISE - I

- Find the quotient and the remainder when  $b$  does not divide  $a$ , where  $a$  and  $b$  are given below.
  - (i)  $a = -100, b = 17$ , (ii)  $a = 43, b = -7$ , (iii)  $a = 289, b = 18$
  - (iv)  $a = -25, b = -187$ , (v)  $a = 25, b = 76$ .

[Ans. : (i)  $q = -6, r = 2$ , (ii)  $q = -6, r = 1$ , (iii)  $q = 16, r = 1$ , (iv)  $q = 1, r = 162$ , (v)  $q = 0, r = 25$ .]
- Prove that product of five consecutive integers is divisible by 5.
- Prove that the product of three consecutive integers is divisible by 6. Deduce that  $a^3 - a$  is divisible by 3 and 6, for any integer  $a$ .
- Prove that product of 5 consecutive integers is divisible by 60.
- Show that square of every odd integer  $n > 7$  is of the form  $8k+1$ .  
(Hint :  $(2n+1)^2 = 4n(n+1) + 1$ , one of  $n$  and  $n+1$  is always even.)
- For integers  $a, b, c$ , prove the following :
  - (i)  $a \mid 0, 1 \mid a, a \mid a$
  - (ii)  $a \mid 1$  if and only if  $a = \pm 1$ .
  - (iii) If  $a \mid b$  and  $c \mid d$ , then  $ac \mid bd$ .
  - (iv) If  $a \mid b$  and  $b \mid c$ , then  $a \mid c$ .
  - (v) If  $a \mid b$  and  $b \mid a$ , then  $a = \pm b$ .
  - (vi) If  $a \mid b$  and  $b \neq 0$ , then  $|a| < |b|$ .
  - (vii) If  $a \mid b$  and  $a \mid c$ , then  $a \mid bx + cy$  for any integers  $x$  and  $y$ .

### 4. Prime Numbers

It is obvious that the positive integer 1 has only one positive divisor, namely 1 itself. Every other positive integer has at least two positive divisors, namely 1 and the integer itself. For example, 2 has divisors 1 and 2; 3 has divisors 1 and 3; 4 has divisors 1, 2 and 4; 6 has divisors, 1, 2, 3 and 6.

The positive integers with exactly two positive divisors are of great importance. They are the building blocks of numbers. Therefore, they are called prime numbers.

**Definition :** A positive integer greater than 1, which is divisible by no other positive integers other than 1 and itself is called prime.

The positive integers 2, 3, 5, 7, 11, 13, 17, 19 are examples of prime numbers. The largest known prime till December 2017 is  $2^{74207281} - 1$ . It has 2,338,618 digits. It was found in January 2016. If written in usual way it will occupy few pages of a news paper. It can be proved that if  $p_1, p_2, \dots, p_n$  are distinct primes, then  $p_1 p_2 \dots p_n + 1$  is also a prime other than  $p_1 p_2 \dots p_n$ . Hence, there are infinitely many primes.

**Definition :** A positive integer other than 1 which is not prime is called composite.

For example,  $6 = 2 \times 3, 10 = 2 \times 5, 15 = 3 \times 5, 55 = 5 \times 11, 105 = 3 \times 5 \times 7$ , etc. are composite.

#### Note ...

The number 1 is neither prime nor composite. It is the only number with this property. Every other number is either prime or composite.

**Question :** Now, a question arises; given a (positive) integer, how can we determine, whether it is prime or composite? If it is composite how can we find its divisors?

Of course, a very simple method is to divide the given integer by each of the numbers preceding it. If none of the preceding numbers (except 1) is a divisor, the given number is a prime. For example, to check whether 20 is prime or composite, we divide 20 by each of the numbers 1, 2, 3, ..., 19 preceding it. We find that 2 divides 20, 4 divides 20 and hence 20 is not a prime.

To check, whether 13 is prime or composite, we divide 13 by each of the number 1, 2, 3, 4, ..., 13. We find that 13 is not divisible by any other preceding numbers except 1 and 13 itself. Hence, 13 is prime. Although the method is very simple, clearly, it cannot be regarded as useful in practice as it will take a lot of time and a lot of work if the number in hand is very large.

**Theorem 1 :** Every positive integer greater than 1, has a prime divisor.

**Proof :** Suppose the theorem is not true. Then there must be a positive integer greater than 1, which has no prime divisor. Let  $n$  be the smallest such. Since  $n$  has no prime divisor and  $n$  divides  $n$ ,  $n$  must be composite. Let  $n = ab$ , where  $a$  and  $b$  are integer,  $1 < a < n$  and  $1 < b < n$ . Since,  $a$  is smaller than  $n$  and  $n$  is the smallest positive integer with no prime divisor,  $a$  must have a prime divisor say  $p$ , i.e.,  $p \mid a$ . But if  $p \mid a$ , then  $p \mid ab$  i.e.,  $p \mid n$ .

This is contradiction. Hence, the theorem is true.

The following theorem reduces our efforts to search for prime factors.

**Theorem 2 :** Every composite integer  $n > 0$  has a prime factor not exceeding  $\sqrt{n}$ .

**Proof :** Let  $n$  be a composite integer and  $n = ab$ , where  $a$  and  $b$  are integers. Without the loss of generality, we can assume that  $a \leq b$ . Clearly,  $1 < a \leq b < n$ .

We claim that  $a \leq \sqrt{n}$ .

Suppose our claim is not true. Then we have  $a > \sqrt{n}$ . Therefore,  $\sqrt{n} < a$ . But then  $\sqrt{n} < b$ . Therefore,  $\sqrt{n} \cdot \sqrt{n} < ab = n$ . Thus, we have absurd result that  $n < n$ .

Hence, our claim  $a \leq \sqrt{n}$  is true.

Now, by Theorem 1 above, every integer greater than 1 has a prime divisor. In particular  $a$  has a prime divisor. Since the prime divisor is less than or equal to  $a$ , it is less than or equal to  $\sqrt{n}$ .

**Example 1 :** (i) Consider 40. We find  $\sqrt{40} = 6.3245$ . Prime numbers less than or equal to  $\sqrt{40}$  are, therefore, 2, 3, 5. We verify that 2 and 5 are prime divisors of 40 and hence 40 is a composite number.

(ii) Consider 509. We calculate  $\sqrt{509} = 22.56$ . The prime numbers less than or equal to  $\sqrt{509}$  are 2, 3, 5, 7, 11, 13, 17, 19. We check that none of them is a divisor of 509. Therefore, 509 is a prime number.

(iii) Consider 2093. We have  $\sqrt{2093} = 45.75$ . The prime numbers less than or equal to  $\sqrt{2093}$  are, therefore, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, and 43. By actual verification, we find  $7 | 2093$  and obtain  $2093 = 299 \times 7$ .

(iv) Consider 299. We calculate  $\sqrt{299} = 17.29$ . The prime numbers less than 17.29 are 2, 3, 5, 7, 11, 13, 17. We try each of these primes and find the  $13 | 299$ . In fact  $299 = 23 \times 13$ . Note that 23 is also a prime.

(v) Combining (iii) and (iv), we obtain  $2093 = 7 \times 13 \times 23$ .

#### Note ...

In all the above examples, we have actually found  $\sqrt{n}$ . This is quite unnecessary. If  $\sqrt{n}$  is not easily known, we may find integers  $a$ , such that  $a < \sqrt{n} < a+1$  easily and try primes less than or equal to  $a$ .

**Example 2 :** Check if 1037 is a prime number. If not, find its prime factors.

Sol. : Clearly  $30^2 = 900 < 1037 < 31^2$ . Therefore, we consider the primes less than 30. They are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. By trial, we found that  $17 \times 61 = 1037$ .

**Example 3 :** Find whether 2737 is a prime or composite. If it is a composite number find its divisors.

Sol. : We first note that  $\sqrt{2737} = 52.32$ .

Hence, we examine whether 2737 is divisible by a prime less than 52 i.e., by 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47. Clearly, 2737 is not divisible by 2, 3, 5. But it is divisible by 7.

$$2737 = 7 \times 391$$

Now, we find  $\sqrt{391}$ . We see that  $\sqrt{391} = 19.77$ .

Hence, we examine whether 391 is divisible by a prime less than 19.77 i.e., 2, 3, 5, 7, 11, 13, 17, 19. Clearly, 391 is not divisible by 2, 3, 5, 7, 11, 13. But it is divisible by 17 and

$$391 = 17 \times 23$$

Hence, the given number 2737 is a composite number and

$$2737 = 7 \times 17 \times 23$$

**Example 4 :** Check whether 7293 is a prime or composite. If it is not a prime find its divisors.

Sol. : We first note that  $\sqrt{7293} = 85.3990$ .

Hence, we examine whether 7293 is divisible by a prime less than 85 i.e., by 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83.

Clearly, 7293 is not divisible by 2. But it is divisible by 3 and

$$7293 = 3 \times 2431 \quad (1)$$

We now find  $\sqrt{2431}$ .  $\sqrt{2431} = 49.305$

Hence, we examine whether 2431 is divisible by a prime less than 49 i.e., by 2, 3, 5, 7, 11, 13, 17, ..., 47.

Clearly, 2431 is not divisible by 2, 3, 5, 7. But it is divisible by 11 and

$$2431 = 11 \times 221 \quad (2)$$

We now find  $\sqrt{221}$ .

$$\sqrt{221} = 14.8660$$

Hence, we examine whether 221 is divisible by a prime less than 14 i.e., by 2, 3, 5, 7, 11, 13.

Clearly, 221 is not divisible by 2, 3, 5, 7, 11. But it is divisible by 13 and

$$221 = 13 \times 17 \quad (3)$$

Hence, from (1), (2) and (3), we get

$$7293 = 3 \times 11 \times 13 \times 17$$

#### 5. Sieve of Eratosthenes

We have seen above that a composite number  $a$  will always have a prime divisor  $p$  such that  $p \leq \sqrt{a}$ . This means if  $a$  is not composite number then it is not divisible by any prime number  $p \leq \sqrt{a}$ . Then  $a$  itself is a prime.

#### Eratosthenes (c. 276 BC — c.194 BC)

Eratosthenes was a Greek scholar celebrated to this day for his significant contributions to mathematics, astronomy, and geography. He is perhaps best known for measuring the circumference of the Earth, and for devising the "Sieve of Eratosthenes," a quick method for identifying prime numbers.

He calculated the circumference of the Earth, by comparing altitudes of the mid-day sun at two places a known North-South distance apart. His calculation was remarkably accurate. He was also the first to calculate the tilt of the Earth's axis (again with remarkable accuracy). Additionally, he may have accurately calculated the distance from the Earth to the Sun and invented the leap day. He created the first map of the world, incorporating parallels and meridians based on the available geographic knowledge of his era.

He wrote on many topics — geography, mathematics, philosophy, chronology, literary criticism, grammar, poetry, and even old comedies. Unfortunately, there are only fragments left of his works after the Destruction of the Library of Alexandria.



For example, consider 641. We first see that  $\sqrt{641} = 25.3180$ . Now, the primes less than 25 are 2, 3, 5, 7, 11, 13, 17, 19, 23.

We see that 641 is not divisible by any of these primes and hence itself is a prime.

Eratosthenes used this fact as a basis of clever technique called **Sieve of Eratosthenes** (Sieve = a utensil having many small meshed or perforated openings, used to strain solids from liquids, sifter, strainer.)

The method of Eratosthenes is very simple. Suppose, we want to find all primes less than 100. We take the square root of  $\sqrt{100} = 10$ . The primes less than 10 are 2, 3, 7.

We now write all the integers from 1 to 100 in their natural order. Then we cross all the integers from this list which is divisible by 2 but not 2 itself. Then we cross all the integers divisible by 3, but not 3 itself. Then we cross all the integers divisible by 5 but not 5 itself and then by 7 but not 7 itself. After crossing the integers, all the integers that are found uncrossed are the primes less than or equal to 100.

(For clear understanding, the numbers divisible by 2 are crossed horizontally like —, the numbers divisible by 3 are crossed by slash like /, the number divisible by 5 are crossed by backslashes like \, and the number divisible by 7 are noted by a circle like O. (The number 2, 3, 5, 7 themselves are not crossed.))

1	2	3	—	5	—	7	—	8	—
11	—	13	—	15	—	17	—	19	—
21	—	23	—	25	—	27	—	29	—
31	—	33	—	35	—	37	—	39	—
41	—	43	—	45	—	47	—	49	—
51	—	53	—	55	—	57	—	59	—
61	—	63	—	65	—	67	—	69	—
71	—	73	—	75	—	77	—	79	—
81	—	83	—	85	—	87	—	89	—
91	—	93	—	95	—	97	—	99	—

The number that have not been crossed in any way are the primes. We see that following are the primes less than 100.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 97.

**Example :** Find all the primes less than 150.

**Sol. :** We first note that  $\sqrt{150} = 12.247$ .

We have already obtained the primes less than 100. We shall now only find the primes between 101 and 150 by Sieve of Eratosthenes.

We first divide each of the above number by 2 and cross them by —. Now, we divide the remaining number by 3 and cross them by /. Now, we divide the remaining number by 5 and cross them by \. Then we divide the remaining numbers by 7 and encircle them by O. Lastly we divide the remaining numbers by 11 and denote by square □.

101	102	103	104	105	106	107	108	109	110
111	—	113	—	115	—	117	—	119	—
121	—	123	—	125	—	127	—	129	—
131	—	133	—	135	—	137	—	139	—
141	—	143	—	145	—	147	—	149	—

Thus, the primes between 101 and 150 are

101, 103, 107, 109, 113, 127, 131, 137, 139 and 149.

## 6. The Prime Number Theorem

Having learnt to find the number of primes less than a given positive integers, the question arises; how many primes are there or for that matter how many primes are there less than a given positive integer. Answer to the first question is "there are infinity of prime numbers". A brilliant proof of this fact produced by Euclid is sketched on the page 2-5. The answer to the second question is given by one of the most famous theorem of all mathematics, "the prime number theorem". To understand this theorem, we need to introduce a new function  $\pi$  defined on the set of all positive integers.

**Definition :** If  $x$  is a positive real number then "the number of primes not exceeding  $x$ " is denoted by the symbol  $\pi(x)$ .

For example,  $\pi(10)$  means the number of primes not exceeding 10. Since the primes less than 10 are 2, 3, 5, 7 (not considering 1 as a prime). We see that  $\pi(10) = 4$ . Similarly, from the above table, we see that the primes less than 20 are 2, 3, 5, 7, 11, 13, 17, 19. Hence,  $\pi(20) = 8$ . Also we see from the above table that  $\pi(100) = 25$ .

### The Prime Number Theorem

The prime number theorem states that

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{(x/\log x)} = 1$$

In other words, the ratio  $\frac{\pi(x)}{(x/\log x)}$  approaches 1 as  $x$  becomes large and large i.e., if  $x$  is very very large  $\pi(x)$ , the number of primes less  $x$ , is nearly equal to  $x/\log x$ .

The prime number theorem was conjectured by Gauss and Legendre in 1793 but was proved in 1886 by a French mathematician J. Hadamard and a Belgian mathematician C. J. de la Vallée-Poussin almost simultaneously but independently. We will accept the theorem without proof as the proofs are highly complicated.

We give below a table of values of  $\pi(x)$  and  $x/\log x$  for some values of  $x$ .

$x$	$\pi(x) = \text{the number of primes less than } x$	$\log_e x$	$\frac{x}{\log_e x}$	$\frac{\pi(x)}{x/\log x}$
10	4	2.3026	4.34	0.921
100	25	4.6052	21.71	1.151
1000	168	6.9077	144.76	1.161
10000	1229	9.2103	1085.7409	1.132
.....	.....	.....	.....	.....

We see from this table that as  $x$  becomes larger and larger  $\frac{\pi(x)}{x/\log x}$  i.e., the number of primes preceding  $x$  divided by  $x/\log x$  because closer and closer to one.

**EXERCISE - II**

1. Check the following integers for their primeness. If they are not prime find their prime factors  
 (i) 2093. (ii) 509. (iii) 349. (iv) 209.  
 [Ans. : (i)  $7 \times 13 \times 23$ , (ii) Prime, (iii) Prime, (iv)  $11 \times 19$ ]
2. Prove that any prime of the form  $5n + 1$  is of the form  $10m + 1$ .  
 More generally, let  $p \neq 2$  be a prime integer. If  $pn + 1$  is a prime, show that it is of the form  $2pm + 1$ .
3. Find all the primes between 150 and 200 using the Sieve of Eratosthenes.

**CHAPTER****3****Euclidean Algorithm****1. Introduction**

In this chapter, we are going to learn Euclidean algorithm, a very efficient algorithm which obtains the greatest common divisor of a pair of integers. We will use it to find integral solutions of the equations of the type  $ax + by = c$ , the famous Diophantine equations, when solutions exist.

**Euclid (300?-275? B.C.)**

He taught at Alexandria and founded the Alexandrian School of Mathematics. Euclid is called "the father of geometry". When the king of Alexandria (Egypt) Ptolemy I asked Euclid if there is an easy way to learn geometry, he replied "there is no royal road to geometry". Euclid wrote thirteen books on algebra and geometry mostly compiling the works of earlier mathematicians but had made also significant contributions of his own. Algebra and geometry that is taught at school level all over the world is based on his books. It is said that his books are read and studied only next to the Bible. More than 2000 editions of his book are published in various languages since the first print in 1482. Unfortunately very little is known about this great mathematician.

**2. Greatest Common Divisor**

Given two integers, our objective is to find the greatest integer that divides both. Since every positive integer divides 0, there is no greatest integer that divides 0. So when we talk of the greatest integer that divides both  $a$  and  $b$ , we assume that atleast one of  $a$  and  $b$  is not zero. For theoretical clarity it is necessary to note that the set of common divisors of  $a, b$  is non-empty as  $\pm 1$  and  $\pm b$  are always common divisors.

**Definition 1 :** Let  $a$  and  $b$  be two integers, such that atleast one of them is non-zero. The largest integer that divides both  $a$  and  $b$  is called the **greatest common divisor of  $a, b$**  and is denoted as  $(a, b)$ .

The following results are immediate consequences of the definition.

- 1.  $(a, 1) = (1, a) = 1$
- 2.  $(a, 0) = (0, a) = |a|$
- 3.  $(a, b) = (b, a) = (-a, b) = (a, -b) = (-a, -b) = (|a|, |b|)$

**Illustrations :**

- (i) The common divisors of 30 and 78 are  $\pm 1, \pm 2, \pm 3, \pm 6$ . Therefore,  $(30, 78) = 6$ .

(ii) The common divisor of 48 and 168 are  $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm 24$ . Hence,  $(48, 168) = 24$ .  
 (iii) Readers should verify that  $(85, 34) = 17$ ,  $(78, 0) = 78$ ,  $(51, 100) = 1$ ,  $(-81, 15) = 3$ ,  $(-84, -24) = 12$ ,  $(-41, 5) = 1$ .

The concept of the greatest common divisor can be extended inductively. But we do not need it presently.

Pair of integers having no common divisor except the usual  $\pm 1$  have special significance. We designate them.

**Definition 2:** Let  $a$  and  $b$  be integers. If their greatest common divisor  $(a, b) = 1$ , we call them relatively prime. Thus,  $a$  and  $b$  are relatively prime if 1 is the only positive divisor.

**Example :** Since  $(35, 66) = 1$ , 35 and 66 are relatively prime.

The following results are immediate consequences of the definition :

1. If  $a$  and  $b$  are distinct prime, they are relatively prime.
2. If  $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$  and  $b = q_1^{l_1} q_2^{l_2} \dots q_m^{l_m}$  are prime factorizations of  $a$  and  $b$  and  $p_1, p_2, \dots, p_n$  are totally different from  $q_1, q_2, \dots, q_m$ , then  $a$  and  $b$  are relatively prime.
3. Integers  $a$  and  $b$  may be composite numbers, but they can, still, be relatively prime. Note that 35 and 66 are not prime numbers, but still they are relatively prime.

The following properties of  $(a, b)$  are useful :

**Theorem 1 :** Let  $a, b, c$  be integers and  $(a, b) = d$ . Then the following holds :

- |                                 |  |                              |
|---------------------------------|--|------------------------------|
| (i) $(ad, bd) = 1$              | (ii) $(a + cb, b) = (a, b)$                | (iii) $(a, ac + b) = (a, b)$ |
| In particular if $a = qb + r$ , |  |                              |
| (iv) $(a, b) = (b, r)$          | (v) $(a, ka) =  a $ for all integers $k$ . |                              |

**Proof :**

- (i) Let  $e > 0$  be a common divisor of  $a/d$  and  $b/d$ . Then by the definition of divisor, we have  $a/d = ke$  and  $b/d = he$ , for some integers  $k$  and  $h$ . Therefore,  $a = k(ed)$  and  $b = h(ed)$ . Thus,  $ed$  is a common divisor of  $a$  and  $b$ . But  $d$  is the greatest common divisor of  $a, b$  as  $d \leq ed$ . Therefore,  $d = ed$ , i.e.,  $e = 1$ . Thus, 1 is the only positive divisor of  $a/d$  and  $b/d$ .

Therefore,  $(a/d, b/d) = 1$ .

- (ii) Let  $e$  be a common divisor of  $a$  and  $b$ . Then  $e | a$  and  $e | b$  and therefore,  $e | ma + nb$  for all integers  $m$  and  $n$  (by Theorem 1, § 2, page 2-2 of chapter 2).

We choose  $m = 1$  and  $n = c$ , so that  $e$  is a common divisor of both  $a + cb$  and  $b$ . Thus, every divisor of  $a$  and  $b$  is also a divisor of  $a + cb$  and  $b$ .

Conversely, let  $f$  be a common divisor of  $a + cb$  and  $b$ . Then  $f | m(a + cb) + nb$ . Choose  $m = 1$  and  $n = -c$ , we get  $f | (a + cb) - cb = a$ .

Thus, every common divisor of the pair  $a, b$  is a common divisor of the pair  $a + cb$  and  $b$  and vice versa.

Hence, the result (ii).

- (iii) Interchanging the roles of  $a$  and  $b$  in (ii), we get (iii).  
 (iv) When  $a = qb + r$ , then  $(a, b) = (qb + r, b) = (r, b)$  by the result (ii) above.  
 (v) When  $a = qb + 0$   $(a, b) = (b, 0) = |b|$  [By (iv)]

Thus,  $(qb, b) = |b|$ . Writing  $a$  for  $b$  and  $k$  for  $q$ , we get (v).

**Illustrations :** (1)  $(30, 78) = 6$ , therefore,  $(30/6, 78/6) = (5, 13) = 1$  [By (i)]

(2)  $(32, 3) = (2 + 10 \times 3, 3) = (2, 3) = 1$ . [By (ii)]

(3)  $(48, 168) = (48, 4 \times 48 - 24) = (48, -24) = (-2 \times -24, -24) = 24$  [By (ii) and (v)]

**Theorem 2 :** Let  $a$  and  $b$  be integers, at least one of them is not zero. The greatest common divisor  $(a, b)$  of  $a$  and  $b$ , is the least positive integer which is a linear combination of  $a$  and  $b$ .

**Meaning of the theorem :** Given  $a$  and  $b$  both integers, at least one of them is not 0. Consider the set of all expressions of the type  $ax + by$  for different values of integers  $x$  and  $y$ , so that  $ax + by$  is positive. Then the smallest integer in this set is  $(a, b)$ .

**Proof :** First we note that such a set is non-empty : If  $a$  is non-zero and positive choose  $x = 1$ ,  $y = 0$ , so that  $ax + by$  is positive. If  $a$  is negative choose  $x = -1$ ,  $y = 0$ , so that  $ax + by$  is positive.

Since, the set of positive linear combinations is non-empty, it has the smallest integer, say,  $d$  in it.

Let  $d = ma + nb$  for some integers  $m$  and  $n$ . .... (i)

We claim that  $d | a$  and  $d | b$ .

Applying division algorithm to  $a$  and  $d$ , we get

$$a = qd + r; \quad 0 \leq r < d \quad \text{..... (ii)}$$

From (i) and (ii), we get

$$r = a - qd = a - q(ma + nb) = (1 - qm)a + (-qn)b$$

Clearly, then  $r$  is a linear combination of  $a$  and  $b$ , while  $0 \leq r < d$ . But  $d$  is, by choice, the smallest linear combination. Therefore,  $r$  must be 0. But, then from (ii),  $a = qd$  and consequently  $d | a$ . Similarly, interchanging the roles of  $a$  and  $b$ , we prove  $d | b$ .

To prove  $d = (a, b)$ , we show that  $d$  is the greatest integer dividing  $a$  and  $b$ . So, let  $c$  be any other integer,  $c | a$  and  $c | b$ . Since,  $c | ma + nb$  for all  $m, n$ ,  $c | d$ . Therefore,  $c \leq d$ . Hence, the theorem.

**Corollary 1 :** Given integers  $a, b$ , there exist integers  $m$  and  $n$ .

$$ma + nb = (a, b)$$

**Corollary 2 :** If  $a, b, c$  are integers, then

(1) If  $a | c, b | c$ ,  $(a, b) = 1$ , then  $ab | c$ .

(2) If  $a | bc$ ,  $(a, b) = 1$ , then  $a | c$ . This is known as Euclid's Lemma.

**Proof :** (1)  $a | c$  implies there is an integer  $s$ , such that  $c = sa$ . Similarly, there is an integer  $t$ , such that  $c = tb$ . Since,  $(a, b) = 1$ , we have integers  $x$  and  $y$ , such that,  $ax + by = 1$ .

Therefore,  $cax + aby = c$  [By multiplying by  $c$ ]

Therefore,  $(tb)ax + (sa)by = c$  [By substituting  $c = tb$  and  $c = sa$  in that order]

Hence,  $ab(tx + sy) = c$

Therefore,  $ab | c$ .

(2) Since  $a | bc$ , we have  $bc = sa$  for some integer  $s$ . Since  $(a, b) = 1$ ,  $ax + by = 1$  for some integers  $x$  and  $y$ .

Multiplying the last equation by  $c$ , we have  $acx + bcy = c$ .

Therefore,  $acx + bcy = c$  [Since  $bc = sa$ ]

This gives  $a(cx + sy) = c$ .  
Therefore,  $a \mid c$ .

The following theorem gives a characterization of the greatest common divisor.

**Theorem 3:** Let  $a$  and  $b$  be two integers such that not both are zero. Then  $d$  is the greatest common divisor of  $a$  and  $b$  if and only if (i)  $d \mid a$  and  $d \mid b$ , (ii) If  $c \mid a$  and  $c \mid b$ , then  $c \mid d$ .

**Proof:** Let  $d = (a, b)$ . Then by definition of the common divisor,  $d \mid a$  and  $d \mid b$ . By Theorem 2, above  $d = ax + by$  for some integers  $x$  and  $y$ . Now, if  $c \mid a$  and  $c \mid b$ , then clearly  $c \mid ax + by$ , i.e.,  $c \mid d$ .

For converse, suppose the conditions (i) and (ii) hold. By the condition (i),  $d$  is a divisor of  $a$  and  $b$ . The condition (ii) shows that if  $c$  is a divisor of  $a$  and  $b$ , then  $c \mid d$  and therefore,  $c \leq d$ . Thus,  $d$  is the greatest among the common divisors of  $a$  and  $b$ , i.e.,  $d = (a, b)$ .

**Example:** If  $(a, b) = 1$ , then  $(a - b, a + b)$  is either equal to 1 or equal to 2, for any integers  $a$  and  $b$ .

**Sol.:** Let  $(a, b) = 1$ . Then by Theorem 2, Corollary 1 (page 3-3), there exist integers  $m$  and  $n$  such that

$$ma + nb = 1 \quad \dots \text{(I)}$$

By Theorem 1 (ii) and (iii), we get

$$(a - b, a + b) = ((a - b) + (a + b), a + b) = (2a, a + b) \quad \dots \text{(II)}$$

$$\text{and } (a - b, a + b) = (a - b, -(a - b) + (a + b)) = (a - b, 2b) \quad \dots \text{(III)}$$

Let  $(a - b, a + b) = d$ . Then by Theorem 3, (II) and (III)

$$d = (2a, a + b) \text{ implies } d \mid 2a$$

$$\text{and } d = (a - b, 2b) \text{ implies } d \mid 2b$$

Therefore,  $d \mid 2ma + 2nb$ . But, by (I)  $2ma + 2nb = 2$ .

Hence,  $d \mid 2$ . i.e.,  $d = 1$  or  $d = 2$ .

### 3. Additional Properties of Primes

Before proceeding further, we recall the following properties of prime numbers.

Let  $a, a_1, a_2, \dots, a_n, b$  be integers  $p, p_1, p_2, \dots, p_k$  and  $q, q_1, q_2, \dots, q_{k'}$  be prime numbers. Then the following results hold :

1. If  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .
2. If  $p \mid a_1 a_2 \dots a_n$ , then  $p \mid a_k$  for some  $k$ , where  $1 \leq k \leq n$ .
3. If  $p \mid q_1 q_2 \dots q_{k'}$ , then  $p = q_k$  for some  $k$ , where  $1 \leq k \leq k'$ .
4. Every positive integer  $n > 1$  is a product of primes, i.e., of the type  $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$  where  $k_1, k_2, \dots, k_m$  are positive integers.

**Example:** Prove that every prime  $3n + 1$  is of the form  $6m + 1$ .

**Sol.:** Let  $3n + 1$  be prime. Clearly  $n \neq 0$ . For, then  $3n + 1 = 1$ , which is not prime. Similarly,  $n \neq 1$ . For, then  $3n + 1 = 4$ , which is not prime.

Therefore,  $3n + 1 > 2$  and hence is an odd prime. Let, therefore,  $3n + 1 = 2k + 1$  for some integer  $n$ . But then  $3n = 2k$  and therefore,  $2 \mid 3n$ . By Corollary 2 (2), Theorem 2 (page 3-3), we must have  $2 \mid n$ . Therefore,  $n = 2m$  for some integer  $m$ ; that is  $3n + 1 = 3(2m) + 1 = 6m + 1$ .

Alternatively : Every integer is either odd or even. Can  $n$  be odd? If  $n = 2m + 1$ , then  $3n + 1 = 3(2m + 1) + 1 = 6m + 4 = 2(3m + 2)$ , which is not prime.

Hence,  $n$  is even and rest follows.

### EXERCISE - I

1. Find the greatest common divisors :

$$(a) (27, -35); (b) (12, 30); (c) (225, 120); (d) (100, 102); (e) (272, 1479)$$

[ Ans. : (a) 1, (b) 6, (c) 15, (d) 2, (e) 17.]

2. Prove the following, if  $a$  and  $b$  are given to be relatively prime.

$$\begin{array}{ll} (\text{i}) (a, a + b) = 1 & (\text{ii}) (a, na + b) = 1, \text{ for all } n = 0, 1, 2, \dots \\ (\text{iii}) (a, a + 2a + b) = 1 & (\text{iv}) (a, a + 2a + \dots + na + b) = 1, \text{ for } n = 0, 1, 2, \dots \\ (\text{v}) (a + b + 2b + \dots + nb, b) = 1 & (\text{Hint : Use Theorem 1 (iii), Induction}) \end{array}$$

3. Prove that :

$$\begin{array}{ll} (\text{i}) (2, 2 + 4 + 6 + \dots + 2n + 3) = 1, & \text{for } n = 0, 1, 2, \dots \\ (\text{ii}) (2 + 3 + 6 + \dots + 3n, 3) = 1, & \text{for } n = 0, 1, 2, \dots \\ (\text{iii}) (4 + 5 + 5^2 + \dots + 5^n, 5) = 1, & \text{for } n = 0, 1, 2, \dots \\ (\text{iv}) (6, 7 + 6 + 6^2 + \dots + 6^n) = 1, & \text{for } n = 0, 1, 2, \dots \end{array}$$

4. Prove that if  $(a, b) = 1$ , then the following hold :

$$(a) (a, b^2) = 1 \quad (b) (a^2, 1) = 1 \quad (c) (a^2, b^2) = 1$$

5. Prove that, if  $(a, b) = 1$ , then  $(a^2 + b^2, a + b)$  is either 1 or 2.

6. Show that if  $a, b, c$  are integers, such that,  $(a, b) = 1 = (a, c)$ , then  $(a, bc) = 1$ .

### 4. The Euclidean Algorithm

Now, we are in a position to develop a general algorithm to calculate the greatest common divisor of any two positive integers, and therefore of any two integers [ Recall  $(a, b) = (-a, b) = (a, -b) = (-a, -b) = (|a|, |b|)$  ]. The process is called the Euclidean Algorithm named after the great Euclid. The algorithm is simple to follow. It is repeated use of the result  $(a, ac + b) = (a, b)$  or  $(a + cb, b) = (a, b)$  (Proved in Theorem 1, § 2 and the division algorithm given in Theorem, § 3, page 2-2 of Chapter 2). Before stating it in a general form it may be useful to see how it works.

**Example 1:** Compute (i) (102, 222), (ii) (666, 1414), (iii) (20785, 44305).

**Sol.:** (i) By division algorithm, we have that

$$222 = 2 \times 102 + 18.$$

$$\therefore (102, 222) = (102, 2 \times 102 + 18) = (102, 18) \quad [\text{Using } (a, ac + b) = (a, b)]$$

Again by division algorithm,

$$102 = 5 \times 18 + 12$$

$$\therefore (102, 18) = (18, 5 \times 18 + 12) = (18, 12)$$

Again by division algorithm,

$$18 = 1 \times 12 + 6$$

$$\therefore (18, 12) = (12, 1 \times 12 + 6) = (12, 6)$$

### Applied Mathematics - IV

(3-6)

Euclidean Algorithm

Again by division algorithm,

$$12 = 2 \times 6 + 0$$

$$(12, 6) = (2 \times 6 + 0, 6) = (0, 6) = 6$$

(ii) Now, we apply the division algorithm and the results  $(a+cb, b) = (a, b) = (a, ac+b)$ , without mentioning them explicitly.

$$(666, 1414) = (666, 2 \times 666 + 82) = (666, 82)$$

$$(666, 82) = (8 \times 82 + 10, 82) = (10, 82)$$

$$(10, 82) = (10, 8 \times 10 + 2) = (10, 2)$$

$$(10, 2) = (5 \times 2, 2) = (2, 2)$$

$$(2, 2) = (1 \times 2 + 0, 2) = (0, 2) = 2.$$

**Theorem 1 (Euclidean Algorithm)** : Let  $a$  and  $b$  be non-negative integers with  $b \neq 0$ . If by division algorithm, we obtain

$$r_j = q_{j+1} r_{j+1} + r_{j+2}; \quad 0 < r_{j+2} < r_{j+1}$$

where,  $r_0 = a$ ,  $r_1 = b$  and  $j = 0, 1, 2, \dots, n-2$  and  $r_{n-1} = q_n r_n + 0$ ,

then  $(a, b) = r_n$ .

**Proof :** Without the loss of generality, we assume that  $a \geq b$ . Let  $r_0 = a$ ,  $r_1 = b$  and with successive application of division algorithm, we have the following :

$$r_0 = q_1 r_1 + r_2 \quad 0 < r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3 \quad 0 < r_3 < r_2$$

$$\dots$$

$$r_{n-3} = q_{n-2} r_{n-2} + r_{n-1} \quad 0 < r_{n-1} < r_{n-2}$$

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_n r_n + 0$$

The process ends at some finite step  $n$  because,  $a$  is a finite integer,  $r_1, r_2, \dots, r_n$  are integers and  $a = r_0 > r_1 > r_2 > \dots > r_n > 0$  is a strictly decreasing sequence of positive integers. Again,

$$(r_j, r_{j+1}) = (q_{j+1} r_{j+1} + r_{j+2}, r_{j+1}) = (r_{j+2}, r_{j+1}) \\ = (r_{j+1}, r_{j+2}); \quad \text{for } j = 0, 1, \dots, n-2$$

Therefore,  $(a, b) = (r_0, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n)$

Moreover  $(r_{n-1}, r_n) = (q_n r_n + 0, r_n) = (0, r_n) = r_n$

Hence,  $(a, b) = r_n$  — the last non-zero remainder in the sequence  $r_0, r_1, r_2, \dots$  of the remainders.

**Example 2 :** Using Euclidean algorithm find  $(20785, 44350)$ .

Sol. : Since  $(20785, 44350) = (44350, 20785)$ , we apply the algorithm on the latter.

$$44350 = 2 \times 20785 + 2780$$

$$20785 = 7 \times 2780 + 1325$$

$$2780 = 2 \times 1325 + 130$$

$$1325 = 10 \times 130 + 25$$

$$130 = 5 \times 25 + 5$$

$$25 = 5 \times 5 + 0$$

The last non-zero remainder is 5. Therefore,  $(20785, 44350) = 5$ .

### Applied Mathematics - IV

(3-7)

Euclidean Algorithm

Notes ....

1. In the above problem, we started with larger of the two numbers. It is convenient but not necessary. Had we started with the smaller number our first two steps would have been as follows.

$$20780 = 0 \times 44350 + 20780$$

$$44350 = 2 \times 20780 + 2780$$

The remaining steps would have been the same.

2. While applying the formula  $r_j = q_{j+1} r_{j+1} + r_{j+2}$  we 'play safe' by choosing  $r_j \geq 0$ .

However, at some stage if remainder is very big, we can increase  $q_j$  so that residue is negative but numerically small. This reduces some calculation. But it may produce  $r_n$  negative. In such case care should be taken to see that  $(a, b) = |r_n|$  and not  $r_n$ , because  $(a, b) > 0$ , always.

**Example 3 :** Compute (i)  $(138, 24)$ , (ii)  $(718, 193)$ .

Sol. : (i)  $(138, 24)$

Keeping remainder positive, we have

$$138 = 5 \times 24 + 18$$

$$24 = 1 \times 18 + 6$$

$$18 = 3 \times 6 + 0$$

Hence,  $(138, 24) = 6$ .

Waving the restriction  $r_j \geq 0$ ,

$$138 = 6 \times 24 - 6$$

$$24 = (-4)(-6) + 0$$

Hence,  $(128, 24) = 6$  (not -6)

Here, one step is reduced.

(ii)  $(718, 193)$

$$718 = 3 \times 193 + 139$$

$$193 = 1 \times 139 + 54$$

$$139 = 2 \times 54 + 31$$

$$54 = 1 \times 31 + 23$$

$$31 = 1 \times 23 + 8$$

$$23 = 2 \times 8 + 7$$

$$8 = 1 \times 7 + 1$$

$$7 = 7 \times 1 + 0$$

Hence,  $(718, 193) = 1$

Waving the restriction that the remainder is positive, we have

$$718 = 4 \times 193 - 24$$

$$193 = (-8)(-24) + 1$$

$$24 = 24 \times 1$$

Thus,  $(718, 193) = 1$

Here, five steps are reduced. But this should be done if sufficient experience is gained.

**Example 4 :** Using Euclidean algorithm, prove that the following pairs of integers are relatively prime : (a) 143, 227, (b) 306, 659, (c) 674, 1565, (d) 987, 1597.

Sol. : (a)  $227 = 1 \times 143 + 84$

$$143 = 1 \times 84 + 59$$

$$84 = 1 \times 59 + 25$$

$$59 = 2 \times 25 + 9$$

$$25 = 2 \times 9 + 7$$

$$9 = 1 \times 7 + 2$$

$$7 = 3 \times 2 + \boxed{1}$$

$$2 = 2 \times 1 + 0.$$

Hence,  $(143, 227) = 1$ .

(b)  $659 = 2 \times 306 + 47$

$$306 = 6 \times 47 + 24$$

$$47 = 1 \times 24 + 23$$

$$24 = 1 \times 23 + \boxed{1}$$

$$23 = 23 \times 1 + 0.$$

Hence,  $(306, 659) = 1$ .

(c)  $1565 = 2 \times 674 + 217$

$$674 = 3 \times 217 + 23$$

$$217 = 9 \times 23 + 10$$

$$23 = 2 \times 10 + 3$$

$$10 = 3 \times 3 + \boxed{1}$$

$$3 = 3 \times 1 + 0.$$

Hence,  $(674, 1565) = 1$ .

(d)  $1597 = 987 + 610$

$$987 = 610 + 377$$

$$610 = 377 + 233$$

$$377 = 233 + 144$$

$$233 = 144 + 89$$

$$144 = 89 + 55$$

$$89 = 55 + 34$$

$$55 = 34 + 21$$

$$34 = 21 + 13$$

$$21 = 13 + 8$$

$$13 = 8 + 5$$

$$8 = 5 + 3$$

$$5 = 3 + 2$$

$$3 = 2 + \boxed{1}$$

$$2 = 2 \times 1 + 0.$$

Hence,  $(987, 1597) = 1$ .

As an important consequence of the Euclidean algorithm, we have the following theorem. This theorem connects our concept of greatest common divisor studied in our school.

**Theorem 2 :** If  $k > 0$ , then  $(ka, kb) = k(a, b)$ .

**Proof :** Recall the proof of Euclidean algorithm used to obtain  $(a, b)$ . There  $r_0 = a$ ,  $r_1 = b$  and

$$r_0 = q_1 r_1 + r_2 \quad 0 < r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3 \quad 0 < r_3 < r_2$$

$$\dots \dots \dots$$

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_n r_n$$

$$\text{Then, } r_n = (a, b).$$

Now, multiply each equation and inequality given above by  $k > 0$ . Then we have

$$k r_0 = q_1 (k r_1) + k r_2 \quad 0 < k r_2 < k r_1$$

$$k r_1 = q_2 (k r_2) + k r_3 \quad 0 < k r_3 < k r_2$$

$$\dots \dots \dots$$

$$k r_{n-2} = q_{n-1} (k r_{n-1}) + k r_n \quad 0 < k r_n < k r_{n-1}$$

$$k r_{n-1} = q_n (k r_n)$$

$$\text{Clearly, } k r_n = (k r_0, k r_1) = (ka, kb).$$

$$\text{But } r_n = (a, b).$$

$$\text{Therefore, } k(a, b) = (ka, kb).$$

**Corollary :** For any  $k \neq 0$ ,  $(ka, kb) = |k| (a, b)$ .

**Proof :** If  $k > 0$ , then clearly, as proved earlier

$$(ka, kb) = k(a, b).$$

$$\text{If } k < 0, \text{ then } (ka, kb) = (-ka, -kb) = -k(a, b).$$

Hence, the result.

**Illustration :** Find  $(924, 660)$ .

We take common factor of the pair of integers out.

$$\text{Then, } (924, 660) = 4(231, 165) = 4 \times 3(77, 55)$$

$$= 4 \times 3 \times 11(7, 5) = 4 \times 3 \times 11 \times 1$$

$$= 132 \quad [\text{Since } (7, 5) = 1]$$

## 5. Solving Diophantine Equations

Let  $a, b, c$  be integers and  $x$  and  $y$  be unknown integers.

The equations of the type  $ax + by = c$  are called Diophantine equations. Note that, Diophantus was interested only integral solutions of the equation. These equations have integral solutions if and only if the greatest common divisor  $(a, b)$  divides  $c$ . If  $x_0, y_0$  is one known solution, then other solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)t, \quad y = y_0 - \left(\frac{a}{d}\right)t \quad \text{where, } t \text{ is arbitrary and } d = (a, b).$$

The solution  $x_0, y_0$  can be found by using Euclidean algorithm.

## Euclidean Algorithm



**Diophantus (AD 201 & 2015 — AD 285 & 299)**

Diophantus, often known as the 'father of algebra', is best known for his *Arithmetica*, a work on the solution of algebraic equations and on the theory of numbers. However, essentially nothing is known of his life and there has been much debate regarding the date at which he lived.

He lived in Alexandria, Egypt, during the Roman era, probably from between AD 200 and 214 to 284 or 298. Diophantus has variously been described by historians as either Greek, non-Greek, Hellenized Egyptian, Hellenized Babylonian, Jewish, or Chaldean. Much of our knowledge of the life of Diophantus is derived from a 5th-century Greek anthology of number games and puzzles created by Metrodorus.

If  $a$  and  $b$  are integers, then  $(a, b)$  the greatest common divisor of  $a, b$  is the smallest positive value of the expressions  $ax + by$ , where  $x$  and  $y$  are integers. This can be done by using Euclidean algorithm. Using the algorithm in a reverse way, we can find integers  $x$  and  $y$ , such that  $(a, b) = ax + by$ .

In other words, the algorithm can be used to find one solution of the equation  $ax + by = (a, b)$ . The method can be stated in one sentence :

Replace the last remainder by available expression in  $a$  and  $b$ , and continue the process till  $(a, b)$  is expressed completely as a linear combination of  $a$  and  $b$ .

**Type I :  $ax + by = (a, b)$**

**Example 1 :** Find the integers  $x, y$ , such that  $333x + 707y = 1$ .

**Sol. :** Step 1 : We first obtain  $(333, 707)$  using Euclidean algorithm

$$\begin{aligned} 1. \quad 707 &= 2 \times 333 + 41 \\ 2. \quad 333 &= 8 \times 41 + 5 \\ 3. \quad 41 &= 8 \times 5 + 1 \\ 4. \quad 5 &= 5 \times 1 \end{aligned}$$

Step 2 : Now, we write  $707 = b$  and  $333 = a$ . ( $a < b$ ) and start replacing these quantities for expressing the remainders one by one in terms of  $a$  and  $b$ , starting from 41 and ending with the last non-zero remainder i.e., 1. Thus,

$$\begin{aligned} 41 &= b - 2a && \text{[ By 1 ]} && (i) \\ 5 &= 333 - 8 \times 41 = a - 8(b - 2a) = 17a - 8b && \text{[ By 2 and (i) ]} && (ii) \\ 1 &= 41 - 8 \times 5 = (b - 2a) - 8(17a - 8b) && \text{[ By (i) and (ii) ]} && \\ &= -138a + 65b. \end{aligned}$$

Therefore,  $x = -138, y = 65$  is a solution.

Other solutions are  $x = -138 + 707t, y = 65 - 333t$ ,  $t$  is any integer.

However, the process of obtaining the solution can be performed mechanically, if we put the above data into two columns. In the first column (say left column), find  $(a, b)$  by Euclidean algorithm and in the second column (say right column) go on expressing the latest remainder in terms of  $a$  and  $b$ . We illustrate the method in the following example. In the right column, remainder will be on the left side of the equations.

**Example 2 :** Find all solutions of the equation  $1769x + 2378y = 29$  for integral values of  $x$  and  $y$ .

**Sol. :** In the first column, we find  $(1769, 2378)$ . In the second column we find the values of  $x$  and  $y$  in the process of expressing  $(a, b)$ , where  $a = 1769, b = 2378$ , as a linear combination of  $a$  and  $b$ .

1. $b = 2378 = 1 \times 1769 + 609$	(i) $609 = b - a$	[ By 1 ]
2. $a = 1769 = 2 \times 609 + 551$	(ii) $551 = a - 2(b - a)$ $= 3a - 2b$	[ By 2 and (i) ]
3. $609 = 1 \times 551 + 58$	(iii) $58 = (b - a) - (3a - 2b)$ $= 3b - 4a$	[ By 3, (i) and (ii) ]
4. $551 = 9 \times 58 + 29$ $58 = 2 \times 29$	(iv) $29 = (3a - 2b) - 9(3b - 4a)$ $= 39a - 29b$	[ By 4, (ii) and (iii) ]

From the first column, we obtain  $(a, b) = 29$ .

From the second column, we obtain  $(39) a - (29) b = (a, b)$ .

Therefore,  $x = 39, y = -29$  is a solution to the equation  $1769x + 2378y = 29$ .

Other solutions are  $x = 39 + (2378 / 29) t$  and  $y = -29 - (1769 / 29) t$

i.e.,  $x = 39 + 82t$  and  $y = -29 - 61t$ , where  $t$  is any integer.

**Type II :  $ax + by = k(a, b)$**

In this type  $c \neq (a, b)$ . However, we notice this fact only when  $(a, b)$  is calculated. Therefore, the method of solving Type II is essentially the same as that of Type I. We first solve  $ax + by = (a, b)$ . Then multiply both sides by  $k$  to get

$$a(kx) + b(ky) = k(a, b)$$

i.e.,  $aX + bY = k(a, b)$

where, we obtain the solution  $X = kx$  and  $Y = ky$  where  $k, x, y$  are already known.

**Example 1 :** Solve the equation  $51x + 111y = 6$  for integral values of  $x$  and  $y$ .

**Sol. :** In the first column below, we calculate  $(51, 111)$ . In the second column we find integers  $x$  and  $y$ , such that  $51x + 111y = (51, 111)$ . Let  $a = 51, b = 111$ . Then,

1. $b = 111 = 2 \times 51 + 9$	(i) $9 = b - 2a$	[ By 1 ]
2. $a = 51 = 6 \times 9 - 3$	(ii) $-3 = a - 6(b - 2a)$	[ By 1 and (i) ]
	$9 = (-3) \times (-3)$	$= 13a - 6b$

Hence,  $(a, b) = 3$ .

Therefore,  $(-13) a + (6) b = 3$ .

From the first column, we obtain  $(a, b) = 3$ .

From the second column, we obtain  $(-13) a + (6) b = 3$ .

Therefore,  $x = -13, y = 6$  is a solution of the equation  $ax + by = 3$  i.e.,  $51x + 111y = 3$ .

But we are interested in the solution of  $51X + 111Y = 6$ .

Therefore, we multiply the equation  $51x + 111y = 3$  by 2, to get  $51(2x) + 111(2y) = 6$ , which is the required equation, if we put  $2x = X$  and  $2y = Y$ .

Its solution is  $X = 2x = 2(-13) = -26, Y = 12$ .

To find general solution, observe that

$$x = -13 + (111/3)t = -13 + 37t \text{ and } y = 12 - (51/3)t = 12 - 17t$$

### Applied Mathematics - IV

(3-12)

### Euclidean Algorithm

is the solution of the  $51x + 111y = 3$ . The solution of the required equation is  
 $x = -26 + 74t, Y = 12 - 34t$ .

**Example 2 :** Find all integral solutions of  $24x + 138y = 18$ .  
**Sol.:** In the first column below, we calculate  $(24, 138)$ . In the second column, we find integers  $x$  and  $y$ , such that  $24x + 138y = (24, 138)$ . Let  $a = 24, b = 138$ . Then,

1. $b = 138 = 5 \times 24 + 18$	(i) $18 = b - 5a$ [ By 1 ]
2. $a = 24 = 1 \times 18 + 6$	(ii) $6 = a - (b - 5a)$ [ By 2 and (i) ] $= 6a - b$
$18 = 3 \times 6$	Therefore, we have (6) $a + (-1)b = 6$ .

From the first column, we observe that  $(a, b) = 6$ .

From the second column, we observe that (6)  $a + (-1)b = 6$ .

Thus,  $x = 6, y = -1$ , is a solution of  $ax + by = (a, b)$  i.e.,  $24x + 138y = 6$ .

The general solution of this equation is

$$x = 6 + \frac{138}{6}t = 6 + 23t \text{ and } y = -1 - \frac{24}{6}t = -1 - 4t$$

But we need solutions of  $24x + 138y = 18$ . Therefore, we multiply equation (i) by 3 to get

$$24(3x) + 138(3y) = 18$$

Substituting  $3x = X$  and  $3y = Y$ , we have

$$24X + 138Y = 18$$

which is the required equation. Therefore, its solution is

$$X = 3x = 18 + 69t \text{ and } Y = 3y = -3 - 12t \quad \text{where } t \text{ is any integer.}$$

**Example 3 :** A customer is to bring a dozen pieces of fruit, appeals and oranges for ₹ 132. An apple costs ₹ 3 more than an orange. Moreover, he is asked to bring more apples than oranges. How many pieces of each fruit he should bring?

**Sol.:** Let  $x$  be the number of apples and  $y$  be the number of oranges, he is going to purchase. Clearly, since he is going to purchase a dozen pieces of fruit

$$x + y = 12$$

Let oranges cost ₹  $z$  rupees a piece. Then apples cost ₹  $z + 3$  a piece. Since he has ₹ 132 to manage with ₹ 132, we have

$$(z + 3)x + zy = 132$$

Therefore,  $3x + z(x + y) = 132$

$$\text{or } 3x + 12z = 132 \quad [\text{By (i)}]$$

On simplification,  $x + 4z = 44$

Clearly,  $(1, 4) = 1$  divides 44, therefore solution exists. One obvious solution is  $x_0 = 0, z_0 = 11$ . The other solutions are  $x = 0 + 4t, z = 11 - t$ , where  $t$  is an integer to be determined by the given conditions.

Since, apples should be more than oranges and total number of pieces is 12, we have

$$6 < x \leq 12$$

$$6 < 4t \leq 12 \quad \text{i.e., } 3 < 2t \leq 6$$

### Applied Mathematics - IV

(3-13)

### Euclidean Algorithm

Clearly, the only admissible values for  $t$  are  $t = 2$  and 3. Thus, either he should purchase  $x = 4 \times 2 = 8$  apples or  $x = 4 \times 3 = 12$  apples. Oranges will be  $12 - x$ .

**Example 4 :** Indian mathematician Mahaviracharya of 850, had put the following puzzle :

There are 63 equal piles of plantain fruit put together and seven single fruits. They are divided evenly among 23 travelers. What is the number in each pile?

**Sol.:** Suppose there are  $x$  fruits in each pile, and each traveler gets  $y$  pieces of fruits. Then clearly

$$63x + 7 = 23y \quad \text{i.e., } -63x + 23y = 7$$

Let  $a = -63, b = 23$ , we use Euclidean algorithm to find  $(-63, 23)$  and a solution to the problem.

1. $a = -63 = -3 \times 23 + 6$	(i) $6 = a + 3b$ [ By 1 ]
2. $b = 23 = 4 \times 6 - 1$	(ii) $1 = 4(a + 3b) - b$ [ By 2 and (i) ] $= 4a + 11b$
	Therefore, $(-63, 23) = 1$ .

Hence,  $x = 4, y = 11$  is a solution of the equation  $-63x + 23y = 7$ .

More general solution is  $x = 4 + 23t, y = 11 + 63t$ .

The solution of the given problem  $-63X + 23Y = 7$  is  $X = 7x = 28 + 161t, Y = 77 + 441t$ .

The 'modest' situation is there are 28 fruits in each pile (and each traveller gets 77 fruits).

### EXERCISE - II

- Find the greatest common divisors of the following pairs of integers, using Euclidean algorithm.
  - (a) (112, 144) (b) (238, 1150) (c) (3063, 2893) (d) (194, 669)
  - (e) (3255, 1785) (f) (34, 55) (g) (232, 136) (h) (1598, 987)

[ Ans. : (a) 16, (b) 2, (c) 1, (d) 1, (e) 105, (f) 1, (g) 8, (h) 47.]
- Write the following greatest common divisors  $(a, b)$  as a sum of multiples of  $a$  and  $b$ .
  - (a) (136, 232) (b) (187, 221) (c) (1565, 674) (d) (1598, 987)

[ Ans. : (a)  $12 \times 136 - 7 \times 232$  (b)  $6 \times 187 - 5 \times 221$   
 (c)  $205 \times 1565 - 476 \times 674$  (d)  $13 \times 987 - 8 \times 1598$  ]
- Find the integral solutions of the equations :
  - (a)  $252x + 198y = 18$  (b)  $55x + 34y = 36$  (c)  $4x + y = 44$

[ Ans. : (a)  $x = 4 + 11t, y = -5 - 14t$ , (b)  $x = 26 + 68t, y = -41 - 110t$ ,  
 (c)  $x = 11 + t, y = -4t$ . ]
- Virat Kohli, in his score of 200 runs, had hit some sixes, some fours and rest singles. Had the number of his sixes and boundaries been interchanged, he would have scored 20 runs more. Find the number of the sixers and boundaries he hit in the score of 200.
 

[ Ans. : 15 sixers, 25 boundaries, 10 singles. ]
- Men, women and children together form a group of 20 persons. A man has to pay ₹ 3, a woman ₹ 2 and a child 50 paise to enter a hall. Together they pay ₹ 20 for the admission. How many men, women and children are in the group? [ Ans. : 1 man, 5 women, 14 children. ]



CHAPTER  
4

# Modular Arithmetic

## 1. Introduction

Modular arithmetic is a system of arithmetic of integers. In this system numbers get wrapped around upon reaching a certain value. The value is called the **modulus**. The arithmetic of modulus (the plural of modulus) is called **modular arithmetic**. German mathematician Carl Friedrich Gauss developed the present day modular arithmetic in 1801. At that time he was just 24.

### Karl Friedrich Gauss (1777 - 1855)



Karl Friedrich Gauss was a great German mathematician and scientist. He is called the "prince of mathematicians". He is ranked with Isaac Newton and Archimedes. It is said that Gauss at the age of three had pointed out an error in calculation made by his father while preparing a payroll. In his doctoral thesis he gave the first complete proof of the fundamental theorem of algebra that a polynomial of  $n$ th degree has  $n$  roots. He is considered to have laid the foundation of number theory. We are all familiar with Gaussian probability distribution (Normal Distribution). He gave first the geometric interpretation of complex numbers, developed the theory of conformal mapping. He did fundamental work in electromagnetism.

He knew many languages and read extensively. It is said that if Gauss had published all of his discoveries the state of mathematics would have advanced by 50 years.

In this chapter, we discuss some basic properties of congruences. Congruence is a very convenient tool to describe divisibility. They make the theory of divisibility similar to the theory of equations. More interestingly they pack the jinni of infinity of integers into finitely many bottles.

## 2. Congruence

**Definition :** Let  $a$  and  $b$  be integers and  $m$  a positive integer. The integer  $a$  is said to be congruent  $b$  modulo  $m$  if  $m \mid (a - b)$ . If  $m \nmid (a - b)$ , then we say  $a$  is incongruent to  $b$  modulo  $m$ . We write these facts in symbols, respectively, as  $a \equiv b \pmod{m}$  and  $a \not\equiv b \pmod{m}$ . Thus,

$$a \equiv b \pmod{m} \text{ if and only if } m \mid (a - b)$$

$$a \not\equiv b \pmod{m} \text{ if and only if } m \nmid (a - b)$$

Note ....

1. No generality is lost in assuming  $m > 0$ . For,  $m \mid (a - b)$  if and only if  $-m \mid (a - b)$ .
2.  $mk \equiv 0 \pmod{m}$  for any integer  $k$ .

Congruences are quite frequent in everyday life. Any phenomenon having integral cycle produces congruence. A clock works either modulo 12 or modulo 24; calendar works modulo 7 for days and modulo 12 for months.

**Example :** We know that  $27 - 15 = 12$  and therefore,  $12 \mid 27 - 15$ . Hence,  $27 \equiv 15 \pmod{12}$ . For similar reasons  $27 \equiv 15 \pmod{4}$ ,  $27 \equiv 15 \pmod{6}$ . Likewise one can observe that  $-41 \equiv 14 \pmod{11}$ ,  $52 \equiv -13 \pmod{5}$ .

**Theorem 1 :** Let  $a, b$  and  $m > 0$  be integers. Then

$$a \equiv b \pmod{m} \text{ if and only if } a \equiv km + b$$

for some integer  $k$ .

**Proof :** If  $a \equiv b \pmod{m}$ , then by definition  $m \mid (a - b)$ . But then, by the definition of divisibility, there exists an integer  $k$ , such that,  $a - b = km$ . Therefore,  $a \equiv km + b$ .

Conversely, if  $a \equiv km + b$  for some integer  $k$ , then  $a - b = km$ , i.e.,  $m \mid a - b$ . But this, by the definition of modulus, means  $a \equiv b \pmod{m}$ .

**Example 1 :** Clearly  $17 \equiv -1 \pmod{6}$  and  $17 \equiv 3 \times 6 - 1$ . Here,  $k = 3$ .

**Example 2 :** Prove that if  $a \equiv b \pmod{m}$  and  $n \mid m$ , then we have  $a \equiv b \pmod{n}$ . Hence, find all  $m$  such that (i)  $223 \equiv 103 \pmod{m}$ , (ii)  $1331 \equiv 0 \pmod{m}$ .

**Sol. :** If  $a \equiv b \pmod{m}$ , then by definition,  $m \mid (a - b)$ . But  $n \mid m$  and  $m \mid (a - b)$  imply  $n \mid (a - b)$ . [Theorem 1 (1), Chapter 2]. Therefore,  $a \equiv b \pmod{n}$ .

(i) Given  $223 \equiv 103 \pmod{m}$ , means  $m \mid (223 - 103) = 120$ . Therefore,  $m$  can be any divisor of 120. The divisors of 120 are 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120. Hence,  $m = 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120$ .

(ii) Given  $1331 \equiv 0 \pmod{m}$  means,  $m \mid 1331$ . Hence, we are to find all divisors of 1331. They are 1, 11, 121, 1331. Hence,  $m = 1, 11, 121, 1331$ .

**Theorem 2 :** Let  $a, b, c, m$  be any integers and  $m > 0$ . Then, the congruence modulo  $m$  satisfies the following properties :

- (i)  $a \equiv a \pmod{m}$  (This is called the Reflexive property)
- (ii) If  $a \equiv b \pmod{m}$ , then  $b \equiv a \pmod{m}$ . (This is called the Symmetric property)
- (iii) If  $a \equiv b \pmod{m}$ ,  $b \equiv c \pmod{m}$ , then  $a \equiv c \pmod{m}$ . This is called the Transitive property.

**Proof :** (i) Clearly, as  $a - a = 0$  and  $m \mid 0$ ,  $m \mid (a - a)$ . Hence,  $a \equiv a \pmod{m}$ .  
(ii) If  $a \equiv b \pmod{m}$ ,  $m \mid a - b$ . Therefore,  $a - b = km$  for some integer  $k$ . But then,  $b - a = (-k)m$ . Hence,  $m \mid b - a$ . Therefore,  $b \equiv a \pmod{m}$ .  
(iii) If  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ , then  $m \mid a - b$  and  $m \mid b - c$ . Therefore, by Theorem 1 (2), Chapter 2,  $m \mid (a - b) + (b - c) = a - c$ .

Therefore,  $a \equiv c \pmod{m}$ .

Using Theorem 2, we can divide the set of integers in disjoint sets, called **congruence classes modulo  $m$** . The congruence classes have the following properties.

- (i) Two classes are either identical or have no element in common.
- (ii) All integers in the same class are congruent modulo  $m$  to each other.

- (iii) Integers belonging to different classes are incongruent.  
 (iv) For every,  $m \geq 1$ , there are  $m$  congruent classes modulo  $m$ , each corresponding to  $0, 1, 2, \dots, m-1$ . Obviously if  $r$  and  $s$  are distinct integers lying between 0 and  $m-1$ , then they are incongruent modulo  $m$ .

For actual computation of a congruence class, we use Theorem 1, above. Given  $m > 0$ , select  $b = 0, 1, 2, m-1$ . Then  $a (= km + b)$  is congruent to  $b$  for all values  $k = \pm 1, \pm 2, \pm 3, \dots$ . If we denote the set of integers by  $\mathbb{Z}$ , let  $m = 2$ . Then there will be two congruence classes, one each for  $b = 0$  and  $b = 1$ . Choosing  $b = 0$ , it will consist of all  $a = 2k, k \in \mathbb{Z}$ . Hence, this class is  $\{2k | k \in \mathbb{Z}\}$ . We can denote it by  $2\mathbb{Z}$ , for it consists of all multiples of 2 of integers in  $\mathbb{Z}$ .

When  $n = 1$ , the congruence class will consist of all integers  $a = 2k + 1$ . Hence, this class is the set  $\{2k + 1 | k \in \mathbb{Z}\}$ , which may be denoted as  $2\mathbb{Z} + 1$ .

Thus,  $2\mathbb{Z} = \{ \dots, -6, -4, -2, 0, 2, 4, 6, 8, \dots \}$

and  $2\mathbb{Z} + 1 = \{ \dots, -5, -3, -1, 1, 3, 5, 7, \dots \}$

In other words,  $\dots = -4 = -2 = 0 = 2 = 4 = \dots \pmod{2}$

and  $\dots = -5 = -3 = 1 = 3 = 5 = \dots \pmod{2}$

When  $m = 3$ , then we will have 3 congruence classes each corresponding to  $b = 0, 1$  and  $2$ .

For  $b = 0$ , the class is  $\{3k | k \in \mathbb{Z}\}$

For  $b = 1$ , the class is  $\{3k + 1 | k \in \mathbb{Z}\}$

For  $b = 2$ , the class is  $\{3k + 2 | k \in \mathbb{Z}\}$

We may denote them as  $3\mathbb{Z}, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2$  respectively.

$3\mathbb{Z} = \{ \dots, -6, -3, 0, 3, 6, \dots \}$

$3\mathbb{Z} + 1 = \{ \dots, -5, -2, 1, 4, 7, \dots \}$

$3\mathbb{Z} + 2 = \{ \dots, -4, -1, 2, 5, 8, \dots \}$

In other words,  $\dots = -6 = -3 = 0 = 3 = 6 = 9 = \dots \pmod{3}$

$\dots = -5 = -2 = 1 = 4 = 7 = 10 = \dots \pmod{3}$

$\dots = -4 = -1 = 2 = 5 = 8 = 11 = \dots \pmod{3}$

More generally, if  $m > 0$  is any integer, then there are  $m$  classes.  $m\mathbb{Z}, m\mathbb{Z} + 1, m\mathbb{Z} + 2, \dots, m\mathbb{Z} + (m-1)$  any two integers in the same class are congruent and in different classes are incongruent. Note that integers  $0, 1, 2, \dots, m-1$  lie, respectively in  $m\mathbb{Z}, m\mathbb{Z} + 1, \dots, m\mathbb{Z} + (m-1)$ . Therefore, every integer is either congruent to 0 or 1, or 2, ..., or  $m-1$ . Hence, we define the following :

**Definition :** A set of integers such that every integer is congruent modulo  $m$  to exactly one integer in the set is called a **complete system of residues modulo  $m$** .

Note that if  $a \equiv b \pmod{m}$ , then  $a - b = km$  for some integer  $k$ , i.e.,  $a = km + b$ . This looks like  $a = qm + r$ ,  $0 \leq r < m$ . But  $b$ , here, need not be the remainder in the sense  $0 \leq b < m$ . For example  $223 \equiv 103 \pmod{30}$ , because  $30 \nmid 223 - 103$ . In fact,  $223 = 4 \times 30 + 103$ . Clearly,  $103 \not\equiv 0 \pmod{30}$ . Therefore, 103 is not the remainder after dividing 223 by 30. We, therefore, call 103 residue modulo 30.

**Definition :** If  $a \equiv b \pmod{m}$ , for any integers  $a, b, m$ , with  $m > 0$ , then  $b$  is called a **residue of  $a$  modulo  $m$** .

**Example 3 :** Find the least positive residue modulo 13, of (a) 1001, (b) -1000.

Sol. : (a)  $1001 = 77 \times 13 + 0 = 76 \times 13 + 13$

Hence, the least non-negative residue modulo 13 is 0; the least positive residue is 13.

(b)  $-1000 = (-77) \times 13 + 1$

Hence, the least positive residue of -1000 modulo 13 is 1.

**Example 4 :** The set  $\{0, 1\}$  is a complete system of residues modulo 2. The sets  $\{1, 2\}$  or  $\{-1, -2\}$  are also examples of complete system of modulo 2.

**Example 5 :** Prove that

the set  $\{0, 1, 2, \dots, m-1\}$  is a complete system of residues modulo  $m$ .

Sol. : Let  $a$  be any integer. Then by division algorithm, there exist unique integers  $k$  and  $r$ , such that  $a = km + r$ . Moreover,  $r$  is one of the integers  $0, 1, \dots, m-1$ . But by Theorem 1, above  $a \equiv km + r$  means  $a$  is congruent to  $r$  modulo  $m$ . Hence, the proof.

**Note ...**

1. Any complete system of residues modulo  $m$  has precisely  $m$  integers.
2. By picking exactly one integer from each congruence class modulo  $m$ , we get a complete system of residues modulo  $m$ .
3.  $0, 1, 2, \dots, m-1, m > 1$  is always a complete system of residues modulo  $m$ . They are the smallest non-negative integers to form a complete system of residues.
4. If  $a_1, a_2, \dots, a_m$  is a complete system of residues modulo  $m$ , and  $a_i \equiv b_i \pmod{m}$ ,  $i = 1, 2, \dots, m$ , then  $b_1, b_2, \dots, b_m$  is also a complete system of residues modulo  $m$ .

**Example 6 :** Let  $m$  be an odd positive integer. Then

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \dots, -1, 0, 1, \dots, \frac{m-3}{2}, \frac{m-1}{2}$$

is a complete system of residues modulo  $m$ .

Sol. : Since  $m$  is an odd positive number  $m = 2n + 1$  (say). Therefore, by Example 5 above it is clear that

$$0, 1, 2, \dots, n, n+1, \dots, 2n-1, 2n \quad \text{.....(I)}$$

is a complete system of residues modulo  $m$ .

Observe that  $(n+1) \equiv (-n) \pmod{(2n+1)}$ ,  $(n+2) \equiv -(n-1) \pmod{(2n+1)}$ ,  $\dots$ ,

$$(2n-1) \equiv (-2) \pmod{(2n+1)}$$
 and  $2n \equiv (-1) \pmod{(2n+1)}$ .

Replace  $n+1, n+2, \dots, (2n-1), 2n$  in (I) by  $-n, -(n-1), \dots, -2, -1$  respectively to get

$$0, 1, 2, \dots, n, -n, -(n-1), \dots, -2, -1 \quad \text{.....(II)}$$

Since (I) is a complete system of residues modulo  $2n+1$ , the new set (II) is also a complete system of residues modulo  $2n+1$ .

Resubstituting  $n = \frac{m-1}{2}$  in (II), we get

$$0, 1, 2, \dots, \frac{m-1}{2}, \frac{-(m-1)}{2}, \frac{-(m-3)}{2}, \dots, -2, -1$$

is a complete system of residues modulo  $m (= 2n+1)$ .

Hence, the result.

**Definition :** Let  $m > 1$  be an odd integer. The set of integers  $\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \dots, -1, 0, 1, \dots, \frac{m-3}{2}, \frac{m-1}{2}\right\}$  is called the set of absolute least residues modulo  $m$ . As seen in the above example, it is a complete system of residues modulo  $m$ .

**Theorem 3 :** Let  $a, b, c, m$  be integers,  $m > 0$  and  $a \equiv b \pmod{m}$ . Then the following holds:

- (i)  $(a+c) \equiv (b+c) \pmod{m}$
- (ii)  $(a-c) \equiv (b-c) \pmod{m}$
- (iii)  $ac \equiv bc \pmod{m}$

**Proof :** (i) Since  $a \equiv b \pmod{m}$ , we have  $m \mid a-b$ . But,  $(a+c)-(b+c) = a-b$ . Therefore, we get  $m \mid (a+c)-(b+c)$ . Hence,  $(a+c) \equiv (b+c) \pmod{m}$ .

(ii) Similarly,  $(a-c)-(b-c) = a-b$ , gives  $(a-c) \equiv (b-c) \pmod{m}$ .

(iii) Clearly,  $m \mid (a-b)$  implies  $m \mid c(a-b)$ . But since  $ac-bc = c(a-b)$ , we have  $m \mid (ac-bc)$ . Hence,  $ac \equiv bc \pmod{m}$ .

**Note ...**

We shall see however, that  $ac \equiv bc \pmod{m}$  need not imply  $a \equiv b \pmod{m}$ .

**Example 7 :** (i) Since  $22 \equiv 4 \pmod{6}$ , we have that

$$1000 + 22 \equiv 1000 + 4 \pmod{6}, \text{ i.e., } 1022 \equiv 1004 \pmod{6}.$$

Similarly,  $22 - 100 \equiv 4 - 100 \pmod{6}$ , i.e.,  $-78 \equiv -96 \pmod{6}$ .

Also,  $22 \times 3 \equiv 4 \times 3 \pmod{6}$ , i.e.,  $66 \equiv 12 \pmod{6}$ .

(ii) Clearly,  $22 = 11 \times 2$  and  $4 = 2 \times 2$ .

But we cannot cancel 2 from  $22 \equiv 4 \pmod{6}$ . For, we have  $11 \not\equiv 2 \pmod{6}$  as  $6 \nmid (11-2) = 9$ .

**Corollary :** If  $(a+c) \equiv (b+c) \pmod{m}$ , then  $a \equiv b \pmod{m}$ .

**Proof :** If  $(a+c) \equiv (b+c) \pmod{m}$ , then applying (ii) above

$$(a+c)-c \equiv ((b+c)-c) \pmod{m}$$

**Theorem 4 :** Let  $a, b, c, m$  be integers,  $m > 0$ .

If  $d = (c, m)$  and  $ac \equiv bc \pmod{m}$ , then  $a \equiv b \pmod{m/d}$ .

**Proof :** Since  $ac \equiv bc \pmod{m}$ , we have that  $m \mid (ac-bc)$ . Therefore,  $c(a-b) = ac-bc = km$  for some integer  $k$ . Since  $d = (c, m)$ , we divide the equation by  $d$  to get

$$(c/d)(a-b) = (m/d)k. \text{ Therefore, } m/d \mid (c/d)(a-b)$$

But  $(m/d, c/d) = 1$ , (Theorem 1 (i), Chapter 3).

Therefore, by Euclid's Lemma (Theorem 2, Corollary 2, Chapter 3), we find that  $m/d \mid (a-b)$ . Therefore,  $a \equiv b \pmod{m/d}$ .

**Corollary 1 :** If  $p$  is a prime number,  $p \nmid c$  and  $ac \equiv bc \pmod{p}$ , then  $a \equiv b \pmod{p}$ .

**Proof :** Since  $p$  is a prime and  $p \nmid c$ ,  $d = (c, p) = 1$ . Hence, the corollary.

**Example 8 :** (i) Consider  $22 \equiv 4 \pmod{6}$ .

Here,  $22 = 11 \times 2$ ,  $4 = 2 \times 2$ , and  $(2, 6) = 2$ .

Therefore, here  $c = 2$ ,  $d = 2$ . Hence, cancelling 2 and dividing 6 by 2, we get  $11 \equiv 2 \pmod{3}$ .

(ii) Consider  $210 \equiv 120 \pmod{18}$ .

Here,  $210 = 7 \times 30$ ,  $120 = 4 \times 30$ ,  $(30, 18) = 6$ . Hence,  $c = 30$ ,  $d = 6$ . Hence cancelling 30 and dividing 18 by 6, we get  $7 \equiv 4 \pmod{3}$ .

**Corollary 2 :** Let  $a, b, c, m$  be integers  $m > 0$ ,  $(c, m) = 1$  and  $ac \equiv bc \pmod{m}$ , then  $a \equiv b \pmod{m}$ .

**Example 9 :** We have  $44 \equiv 14 \pmod{15}$ , i.e.,  $2 \times 22 \equiv 2 \times 7 \pmod{15}$ . Since,  $(2, 15) = 1$ , we have

$$\frac{44}{2} \equiv \frac{14}{2} \pmod{15}, \text{ i.e., } 22 \equiv 7 \pmod{15}.$$

**Theorem 5 :** Let  $a, b, c, d, m$  be integers,  $m > 0$ ,  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then the following holds:

- (i)  $a+c \equiv b+d \pmod{m}$
- (ii)  $a-c \equiv b-d \pmod{m}$
- (iii)  $ac \equiv bd \pmod{m}$

**Proof :** Since  $a \equiv b \pmod{m}$ , we have  $m \mid a-b$ , and therefore,  $a-b = km$  for some integer  $k$ . Similarly, since  $c \equiv d \pmod{m}$ , we have  $c-d = hm$  for some integer  $h$ .

(i) Therefore,  $(a+c)-(b+d) = (a-b)+(c-d) = km+hm = (k+h)m$ .

Hence,  $m \mid (a+c)-(b+d)$ .

Therefore,  $a+c \equiv b+d \pmod{m}$ .

(ii) Similarly,  $(a-c)-(b-d) = (a-b)-(c-d) = km-hm = (k-h)m$ .

Therefore,  $m \mid (a-c)-(b-d)$ , implying  $a-c \equiv b-d \pmod{m}$ .

(iii) Clearly,  $ac-bd = ac-bc+bc-bd$

$$= (a-b)c+b(c-d)$$

$$= km\ c + b\ hm$$

$$= (kc+bh)m$$

Therefore,  $m \mid ac-bd$ , implying  $ac \equiv bd \pmod{m}$ .

**Example 10 :** Verify the above theorem for the following :

(i)  $31 \equiv 3 \pmod{7}$ ,  $18 \equiv 4 \pmod{7}$

(ii)  $27 \equiv 3 \pmod{6}$ ,  $19 \equiv 7 \pmod{6}$

**Sol. :** (i) (a)  $(31+18) \equiv (3+4) \pmod{7}$ , i.e.,  $49 \equiv 7 \pmod{7}$ .

Since  $7 \equiv 0 \pmod{7}$ , we can write  $49 \equiv 0 \pmod{7}$ , which is true as  $7 \mid 49$ .

(b)  $(31-18) \equiv (3-4) \pmod{7}$ , i.e.,  $13 \equiv -1 \pmod{7}$ .

This is true as  $7 \mid (13+1) = 14$ .

(c)  $31 \times 18 \equiv 3 \times 4 \pmod{7}$ , i.e.,  $558 \equiv 12 \pmod{7}$ .

This is true as  $7 \mid 558 - 12 = 546$ .

### Modular Arithmetic

(4-7)

#### Applied Mathematics - IV

- (II) (a)  $27 + 19 = (3 + 7) \pmod{6}$ , i.e.,  $46 = 10 \pmod{6}$ .  
 This is true, as  $6 \mid 46 - 10 = 36$ .
- (b)  $27 - 19 = (3 - 7) \pmod{6}$ , i.e.,  $8 = -4 \pmod{6}$ .  
 This is true, as  $6 \mid 8 + 4 = 12$ .
- (c)  $27 \times 19 = 3 \times 7 \pmod{6}$ , i.e.,  $513 = 21 \pmod{6}$ .  
 This is true, as  $6 \mid 513 - 21 = 492$ .

**Corollary :** If  $a \equiv b \pmod{m}$ , then  $a + mk \equiv b \pmod{m}$  for all integers  $k$ .

**Proof :**  $mk \equiv 0 \pmod{m}$ .

**Theorem 6 :** Let  $r_1, r_2, \dots, r_m$  be a complete system of residues modulo  $m$ , and  $a$  a positive integer, such that  $(a, m) = 1$ . Then

$$ar_1 + b, ar_2 + b, \dots, ar_m + b \quad \dots \quad (I)$$

is also a complete system of residues modulo  $m$ .

**Proof :** In order that (I) is a complete system of residues modulo  $m$ , these integers should satisfy two conditions.

(i) They should be  $m$  in number.

(ii) No two of them should be congruent.

The first condition obviously holds. So let us check the second condition.

Suppose the condition does not hold. Then there should be integers  $j$  and  $k$ ,  $j \neq k$ , and

$$ar_j + b \equiv ar_k + b \pmod{m}.$$

Subtracting  $b$  from both sides, we get

$$ar_j \equiv ar_k \pmod{m} \quad [\text{By Theorem 3}]$$

Since  $(a, m) = 1$ , by hypothesis, we can cancel  $a$  from both sides. (By Theorem 4, Corollary 2)

Therefore, we have

$$r_j \equiv r_k \pmod{m}, \quad j \neq k.$$

But this contradicts the hypothesis that  $r_1, r_2, \dots, r_m$  is a complete system of residues modulo  $m$ .

Hence, the condition (ii) holds and the proof is complete.

**Illustration :** We know  $0, 1, 2, \dots, 100$  form a complete system of residues modulo 101. Choosing  $a = 2$  and  $b = 1$ , we find that integers  $2 \times 0 + 1, 2 \times 1 + 1, \dots, 2 \times 100 + 1$ , i.e.,  $1, 3, 5, \dots, 201$ , is a complete system of residues modulo 101. Choose  $a = -1$  and  $b = 3$ , we find  $0 + 3, -1 + 3, -2 + 3, -3 + 3, -4 + 3, \dots, -100 + 3$ , i.e.,  $3, 2, 1, 0, -1, -2, \dots, -97$  form another complete system of residues modulo 101.

**Example 11 :** Give a complete system of residues modulo 13 consisting entirely of odd integers.

**Sol. :** Recall that  $0, 1, 2, \dots, 12$  is a complete system of residues modulo 13. We are through if we replace every even number from this set by an odd number congruent modulo 13.

Clearly, there are 7 even numbers in the set. They are  $n = 2k$ ,  $k = 0, 1, 2, \dots, 6$ . We know that  $13 + 2k \equiv 2k \pmod{13}$  and that  $13 + 2k$  is odd. Therefore, a complete system of residues modulo 13, consisting of odd numbers only will be  $1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25$ . (The last seven numbers are  $13 + 2k$ ,  $k = 0, 1, 2, \dots, 6$ )

### Modular Arithmetic

(4-8)

#### Applied Mathematics - IV

Modular Arithmetic

**Theorem 6 :** Let  $a, b, k, m$  be integers,  $k > 0, m > 0$

If  $a \equiv b \pmod{m}$ , then  $a^k \equiv b^k \pmod{m}$ .

**Proof :** Observe that  $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \dots + ab^{k-2} + b^{k-1})$ ; i.e.,  $a^k - b^k = (a - b)k$ , say.

But  $m \mid (a - b)$  implies  $m \mid (a - b)k = a^k - b^k$ .

Hence,  $a^k \equiv b^k \pmod{m}$ .

**Example 12 :** Since  $5 \equiv -3 \pmod{4}$ , we have,  $25 \equiv 9 \pmod{4}$ ,  $125 \equiv -27 \pmod{4}$ ,  $625 \equiv 81 \pmod{4}$ , etc.

**Example 13 :** Find the remainder when 7 divides : (a)  $2^{50}$ , (b)  $41^{65}$ .

**Sol. :** (a) Observe that  $2^3 = 8 = 7 + 1$ , have  $2^3 \equiv 1 \pmod{7}$ .

Since,  $50 = 16 \times 3 + 2$ , we calculate  $2^{48} = (2^3)^{16}$ .

Since,  $a \equiv b \pmod{m}$  implies  $a^k \equiv b^k \pmod{m}$ , when  $k > 0, m > 0$ , we get

$$(2^3)^{16} \equiv 1^{16} \pmod{7}, \text{ i.e., } 2^{48} \equiv 1 \pmod{7}.$$

Multiplying both sides by  $2^2 = 4$ , we have  $2^{50} \equiv 4 \pmod{7}$ .

Hence, the required remainder is 4.

(b) Since,  $41 = 5 \times 7 + 6$ , we have  $41 \equiv 6 \pmod{7}$ .

But  $6 \equiv -1 \pmod{7}$ . Hence, by transitivity, we have  $41 \equiv -1 \pmod{7}$ .

Using  $a \equiv b \pmod{m}$  implies  $a^k \equiv b^k \pmod{m}$ , for  $k > 0, m > 0$ , we have

$$41^{65} \equiv (-1)^{65} \pmod{7}, \text{ i.e., } 41^{65} \equiv -1 \pmod{7}.$$

$\therefore 41^{65} \equiv 6 \pmod{7}$  [By transitivity]

Hence, the required remainder is 6.

**Example 14 :** Find the remainder, obtained by dividing the following number by 12.

$$1! + 2! + 3! + \dots + 100!$$

**Sol. :** Let  $S = 1! + 2! + 3! + \dots + 100!$

Observe that  $k! = k(k-1) \dots (5)4!$ , for all  $k \geq 4$ .

and  $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24 = 2 \times 12$ .

Therefore,  $k! = c \cdot 12$  for some factor  $c$  (depending on  $k$ ) for all  $k \geq 4$ .

Therefore,  $4! + 5! + \dots + 100! = K \cdot 12$  for some integer  $K$ .

On the other hand  $1! + 2! + 3! = 1 + 2 + 6 = 9$ .

Therefore,  $S = 9 + K \cdot 12$ .

Hence,  $S \equiv (9 + K \cdot 12) \pmod{12} \equiv 9 \pmod{12}$

Hence, the required remainder is 9.

We can only imagine the amount of calculation if the direct division by 12 is performed.

**Example 15 :** Prove that 4 divides  $1^5 + 2^5 + \dots + 99^5 + 100^5$ .

**Sol. :** Let  $S = 1^5 + 2^5 + \dots + 99^5 + 100^5$ .

The integers,  $1, 2, \dots, 100$ , can be divided into four sections.

(i)  $n = 4k$ ,  $k = 1, 2, \dots, 25$       (ii)  $n = 4k+1$ ,  $k = 0, 1, 2, \dots, 24$

(iii)  $n = 4k+2$ ,  $k = 0, 1, 2, \dots, 24$       (iv)  $n = 4k+3$ ,  $k = 0, 1, 2, \dots, 24$ .

### Applied Mathematics - IV

(4-9)

- This division exhausts all  $n = 1, 2, \dots, 100$ .
- (I) If  $n = 4k$ , then,  $4 \mid 4k$ , and  $n \equiv 0 \pmod{4}$ .  
Therefore,  $n^5 \equiv 0 \pmod{4}$ , for all  $k = 1, 2, \dots, 25$
  - (II) If  $n = 4k + 1$ , then  $n \equiv (4k + 1) \pmod{4} \equiv 1 \pmod{4}$ .  
Therefore,  $n^5 \equiv 1 \pmod{4}$ , for  $k = 0, 1, 2, \dots, 24$
  - (III) If  $n = 4k + 2$ , then  $n \equiv (4k + 2) \pmod{4} \equiv 2 \pmod{4}$ .  
Therefore,  $n^5 \equiv 2^5 \pmod{4} \equiv 32 \pmod{4} \equiv 0 \pmod{4}$   
(Since  $4 \mid 32$ ), for  $k = 0, 1, 2, \dots, 24$ .
  - (IV) If  $n = 4k + 3$ , then  $n \equiv (4k + 3) \pmod{4} \equiv 3 \pmod{4}$ .  
Therefore,  $n^5 \equiv 3^5 \pmod{4} \equiv 243 \pmod{4} \equiv 1 \pmod{4}$   
Combining (I) to (IV), we get  
 $S = (0 + 1 + 0 + 3) \pmod{4} \equiv 4 \pmod{4} \equiv 0 \pmod{4}$   
Therefore,  $4 \mid S$ .

Example 16 : Prove the statements : (a)  $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$ , (b)  $43 \mid 6^{n+2} + 7^{2n+1}$ .

Sol. : (a) Observe that  $3 \cdot 2^{5n-2} = 6 \cdot 2^{5n-3}$ .

Since,  $6 \equiv (-1) \pmod{7}$ , we have

$$3 \cdot 2^{5n-2} \equiv (-1) 2^{5n-3} \pmod{7}$$

On the other hand,  $5 \equiv -2 \pmod{7}$ . Therefore, we have

$$5^{2n} \equiv (-2)^{2n} \pmod{7} \equiv 2^{2n} \pmod{7}$$

From (I) and (II), we get

$$\begin{aligned} 5^{2n} + 3 \cdot 2^{5n-2} &\equiv (2^{2n} + (-1) 2^{5n-3}) \pmod{7} \\ &\equiv 2^{2n} (1 - 2^{3n-3}) \pmod{7} \end{aligned}$$

Clearly,  $2^{3n-3} = (2^3)^{n-1}$ . But  $2^3 \equiv 8 \pmod{7} \equiv 1 \pmod{7}$ .

Therefore,  $2^{3n-3} \equiv 1^{(n-1)} \pmod{7} \equiv 1 \pmod{7}$ .

Therefore,  $(1 - 2^{3n-3}) \equiv 0 \pmod{7}$

Therefore,  $2^{2n}(1 - 2^{3n-3}) \equiv 0 \pmod{7}$

From (III) and (IV), we get

$$5^{2n} + 3 \cdot 2^{5n-2} \equiv 0 \pmod{7}$$

Hence,  $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$ .

(b) Observe that  $7 \equiv -6^2 \pmod{43}$ .

Therefore,  $7^{2n+1} \equiv (-1)^{2n+1} 6^{4n+2} \pmod{43}$

$$\text{or } 7^{2n+1} \equiv -6^{4n+2} \pmod{43}$$

Therefore,  $6^{n+2} + 7^{2n+1} \equiv (6^{n+2} - 6^{4n+2}) \pmod{43}$

$$\text{i.e., } 6^{n+2} + 7^{2n+1} \equiv 6^{n+2} (1 - 6^{3n}) \pmod{43}$$

However,  $6^3 \equiv 216 \equiv 5 \times 43 + 1$ .

Therefore,  $6^3 \equiv 1 \pmod{43}$ .

Consequently,  $6^{3n} \equiv 1 \pmod{43}$  and  $1 - 6^{3n} \equiv 0 \pmod{43}$ .

Therefore,  $6^{n+2} (1 - 6^{3n}) \equiv 0 \pmod{43}$

### Modular Arithmetic

#### Applied Mathematics - IV

(4-10)

#### Modular Arithmetic

From (II) and (III), we have

$$6^{n+2} + 7^{2n+1} \equiv 0 \pmod{43}$$

Hence,  $43 \mid 6^{n+2} + 7^{2n+1}$ .

Example 17 : Using the congruence, prove that (a)  $89 \mid 2^{44} - 1$ , (b)  $97 \mid 2^{48} - 1$ .

Sol. : (a) Observe that  $2^{11} = 2048 = 23 \times 89 + 1$ .

Therefore,  $2^{44} \equiv 1 \pmod{89}$ . Hence,  $2^{44} \equiv 1^4 \pmod{89}$ , i.e.,  $2^{44} \equiv 1 \pmod{89}$ .

Therefore,  $89 \mid 2^{44} - 1$ .

(b) Observe that  $2^{16} = 65536 = 675 \times 97 + 61$ .

Therefore,  $2^{48} \equiv 61 \pmod{97}$ .

Since,  $2^{48} = (2^{16})^3$ , we calculate  $61^3$ .

We observe that  $61^3 = 226981 = 2340 \times 97 + 1$

Therefore,  $2^{48} \equiv 61^3 \pmod{97} \equiv 1 \pmod{97}$

Therefore,  $97 \mid 2^{48} - 1$ .

Example 18 : Prove that 39 divides  $53^{103} + 103^{53}$ .

Sol. : Observe that  $53 = 39 + 14$  and hence  $53 \equiv 14 \pmod{39}$ .

$$\text{Therefore, } 53^{103} \equiv 14^{103} \pmod{39}$$

Again  $14^3 = 2744 = 70 \times 39 + 14$ . Therefore, we have  $14^3 \equiv 14 \pmod{39}$ .

But  $(14, 39) = 1$ , therefore, cancelling 14, from both sides, we have

$$14^2 \equiv 1 \pmod{39}$$

Since,  $103 = 51 \times 2 + 1$ ,  $14^{103} \equiv (14^2)^{51} \times 14 \pmod{39}$  and we have from (I) and (II)

$$53^{103} \equiv 14^{103} \pmod{39} \equiv 14 \times (14^2)^{51} \pmod{39}$$

$$\equiv 14 \times (1)^{51} \pmod{39} \quad [\text{By (I)}]$$

Thus,  $53^{103} \equiv 14 \pmod{39}$

On the other hand,  $103 = 2 \times 39 + 25$ .

Therefore,  $103 \equiv 25 \pmod{39} \equiv -14 \pmod{39}$

$$\text{Hence, } 103^{53} \equiv (-1) 14^{53} \pmod{39} \equiv (-1) 14^{26 \times 2 + 1} \pmod{39}$$

$$\equiv (-1) 14 ((14)^2)^{26} \pmod{39} \equiv (-1) \times 14 \times 1^{26} \pmod{39}$$

Therefore,  $103^{53} \equiv -14 \pmod{39}$

From adding (III) and (IV), we get

$$53^{103} + 103^{53} \equiv (14 - 14) \pmod{39} \equiv 0 \pmod{39}$$

Hence,  $39 \mid 53^{103} + 103^{53}$ .

Example 19 : Prove that  $111^{333} + 333^{111}$  is divisible by 7.

Sol. : Clearly,  $111^{333} + 333^{111} = 111^{111} (111^{222} + 3^{111})$ .

Clearly,  $7 \nmid 111$  and hence,  $7 \nmid 111^{111}$ .

Therefore, it is enough to show that  $7 \mid (111^{222} + 3^{111})$ .

Since,  $111 = 15 \times 7 + 6$ , we have  $111 \equiv 6 \pmod{7} \equiv -1 \pmod{7}$

$$\text{Therefore, } 111^{222} \equiv ((-1)^2)^{111} \equiv 1 \pmod{7}$$

On the other hand,  $3^3 = 3 \times 7 + 6$ . Therefore, we get

$$3^3 \equiv 6 \pmod{7} \equiv -1 \pmod{7}$$

Therefore, since  $111 = 37 \times 3$ , we get, from (II),  
 $3^{111} = (3^3)^{37} \pmod{7} = (-1)^{37} \pmod{7} = -1 \pmod{7}$

From (I) and (III),  
 $111^{222} + 3^{111} = (1-1) \pmod{7} = 0 \pmod{7}$

Hence,  $7 \mid 111^{222} + 3^{111}$ . Hence,  $7 \mid 111^{333} + 3^{333}$ .

**Summary :** The following rules about modulo  $m > 0$  are useful to be remembered :

1.  $a \equiv a \pmod{m}$
2. If  $a \equiv b \pmod{m}$ , then  $b \equiv a \pmod{m}$
3. If  $a \equiv b \pmod{m}$ ,  $b \equiv c \pmod{m}$ , then  $a \equiv c \pmod{m}$

If  $a \equiv b \pmod{m}$ , then

4.  $(a+c) \equiv (b+c) \pmod{m}$
5.  $(a-c) \equiv (b-c) \pmod{m}$
6.  $ac \equiv bc \pmod{m}$

In general,  $\frac{a}{c} \not\equiv \frac{b}{c} \pmod{m}$

7. If  $(a \pm c) \equiv (b \pm c) \pmod{m}$ , then  $a \equiv b \pmod{m}$ .
8. If  $d \equiv (c, m)$  and  $ac \equiv bc \pmod{m}$ , then  $a \equiv b \pmod{m/d}$ .

Let  $a \equiv b \pmod{m}$ ,  $c \equiv d \pmod{m}$ , then

9.  $a+c \equiv (b+d) \pmod{m}$
10.  $a-c \equiv (b-d) \pmod{m}$
11.  $ac \equiv bd \pmod{m}$

In general,  $\frac{a}{c} \not\equiv \frac{b}{d} \pmod{m}$

12. If  $a \equiv b \pmod{m}$ , then  $a+mk \equiv b \pmod{m}$ , for all integers  $k$ .
13.  $a^k \equiv b^k \pmod{m}$  for all integers  $k \geq 0$ .
14. If  $d \equiv (m, c)$  and  $ac \equiv bc \pmod{m}$ , then  $a \equiv b \pmod{(m/d)}$

### EXERCISE - I

1. For what values of  $m$ , the following statements are true.
  - (a)  $61 \equiv 33 \pmod{m}$
  - (b)  $171 \equiv 111 \pmod{m}$
  - (c)  $1 \equiv 1000 \pmod{m}$
  - (d)  $323 \equiv 0 \pmod{m}$

[Ans. : (a) 1, 2, 4, 7, 14, 28, (b) 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60, (c) 1, 3, 9, 27, 37, 111, 333, 999, (d) 1, 17, 19, 323.]
2. Find the least non-negative residue modulo 17 of the following :
  - (a) 40, (b) -1000, (c) -2001, (d) 115, (e) -115.

[Ans. : (a) 6, (b) 3, (c) 5, (d) 13, (e) 4.
3. Given that  $a$  and  $b$  are integers, such that,  $a \equiv b \pmod{119}$ . Prove that  $a \equiv b \pmod{7}$  and  $a \equiv b \pmod{17}$ .
4. Let  $a, b, c$  be integers and  $c > 0$ , such that  $a \equiv b \pmod{c}$ . Show that  $(a, c) = (b, c)$ .
 

(Hint : We are given that  $a = kc + b$ . Apply Theorem 1 (ii), Chapter 3 to  $(a, c) = (kc + b, c)$ )

5. Given  $a \equiv b \pmod{m}$ . Prove that  

$$(1+2a+3a^2+\dots+na^{n-1}) \equiv (1+2b+3b^2+\dots+nb^{n-1}) \pmod{m}$$
6. Let  $a, b, m$  are integers and  $m > 0$ , such that  $a \equiv b \pmod{m}$ . Let  $f(x) = c_0 + c_1x + c_2x^2 + \dots + c_nx^n$  where  $c_0, c_1, \dots, c_n$  are integers. Prove that  $f(a) \equiv f(b) \pmod{m}$ .
 

(Hint : Recall that  $a^k \equiv b^k \pmod{m}$  for all  $k = 0, 1, 2, \dots$  and  $c_k a^k \equiv c_k b^k \pmod{m}$ .)
7. Prove that  $-5, -3, -1, 1, 3, 5, 7$  is a complete system of residues modulo 7.
 

(Hint :  $-5 \equiv 2 \pmod{7}$ ,  $-3 \equiv 4 \pmod{7}$ ,  $-1 \equiv 6 \pmod{7}$ ,  $7 \equiv 0 \pmod{7}$  and  $0, 1, 2, 3, 4, 5, 6$  is a complete system. See Example 5.)
8. Prove that  $3 \mid 1^3 + 2^3 + 3^3 + \dots + 99^3$ .
 

(Hint : 1, 2, ..., 99 are divided into 3 equal parts  $n = 3k$ ,  $k = 1, \dots, 33$ ,  $n = 3k+1$ ,  $k = 0, 1, \dots, 32$  and  $n = 3k+2$ ,  $k = 0, 1, \dots, 32$ .)
9. Find the remainder after dividing the following number by 15.  
 $1! + 2! + 3! + \dots + 200!$ 

[Ans. : 3]
10. Given a complete system of residues modulo 11, consisting entirely of odd integers.
 

[Ans. : 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21.]
11. Show that if  $n \equiv 3 \pmod{4}$ ,  $n$  cannot be a sum of two square.
 

(Hint : Assume  $a = 2k, 2k+1, b = 2k', 2k'+1$ , and find why in each of the four cases  $a^2 + b^2 \not\equiv 3 \pmod{4}$ .)
12. Let  $p$  be a prime integer and  $x^2 \equiv x \pmod{p}$ . Show that either  $x \equiv 0 \pmod{p}$  or  $x \equiv 1 \pmod{p}$ .
 

(Hint :  $p \mid x^2 - x = x(x-1)$  implies  $p \mid x$  or  $p \mid x-1$ .)
13. Let  $p$  be a prime number and  $x^2 \equiv x \pmod{p^k}$  for a positive integer  $k$ . Prove that  
 $x \equiv 0 \pmod{p^k}$  or  $x \equiv 1 \pmod{p^k}$ .
14. If  $n \geq 1$ , prove the statements : (a)  $13 \mid 3^{n+2} + 4^{2n+1}$ , (b)  $27 \mid 2^{5n+1} + 5^{n+2}$ .
15. Prove that  $a^2 \equiv 1 \pmod{8}$  for all odd integers  $a$ .
 

(Hint :  $a = 2n+1$ , then  $(a^2 - 1) = (a+1)(a-1) = 4n(n+1)$ . Now, note that either  $n$  is even or  $n+1$  is even.)
16. Prove that for any integer  $a$ ,  $a^3 \equiv 0, 1$ , or  $6 \pmod{7}$ .
 

(Hint :  $a = 7k+n$ , for some  $k$  and  $n = 0, 1, 2, 3, \dots, 6$ . Therefore,  $a^3 \equiv n^3 \pmod{7}$ ,  $n = 0, 1, \dots, 6$ .)
17. Prove that for any integer  $a$ ,  $a^4 \equiv 0$  or  $1 \pmod{5}$ .
18. Prove that if  $(m, a) = 1$ , then  $c, c+a, c+2a, \dots, c+(m-1)a$  form a complete set of residues modulo  $m$ .
 

Deduce that any  $m$  consecutive integers from a complete set of residues modulo  $m$ .
 

(Hint : Prove that  $(c+ka) \equiv (c+k'a) \pmod{m}$  imply  $k = k'$ . For the deduction take  $a = 1$ .)
19. Prove that if  $m$  is a positive integer, then  $m$  is congruent to the sum of its digits modulo 9.
 

(Hint : Given  $m = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$ . Clearly  $10 \equiv 1 \pmod{9}$ ,  $10^k \equiv 1 \pmod{9}$ . Deduce that  $9 \mid (1234567890)$ .)
20. Prove that if  $p$  is a prime integer, then either  $p \equiv 1 \pmod{4}$  or  $p \equiv 3 \pmod{4}$ .
21. Prove that if  $p$  is a prime integer, then either  $p \equiv \pm 1 \pmod{8}$  or  $p \equiv \pm 3 \pmod{8}$ .
22. Prove that if  $p$  is a prime, then either  $p \equiv \pm 1 \pmod{12}$  or  $p \equiv \pm 5 \pmod{12}$ .
23. Given  $50 \equiv 20 \pmod{15}$ , deduce  $5 \equiv 2 \pmod{3}$ .

## EXERCISE - II

1. Find the inverse of  $a$  modulo  $m$ , when  $a$  and  $m$  are as given below :
- |   |                          |                      |
|---|--------------------------|----------------------|
| (a) $a = 7, m = 12$                           | (b) $a = 3, m = 5$       | (c) $a = 17, m = 21$ |
| (d) $a = 1858, m = 1013$                      | (e) $a = 1013, m = 1858$ |                      |
| [Ans. : (a) 7, (b) 2, (c) 5, (d) 609, (e) 74] |                          |                      |
2. Solve the following congruences for a positive value of  $x$  :
- |  |                              |                               |
|--|------------------------------|-------------------------------|
| (a) $32x \equiv 1 \pmod{17}$                           | (b) $17x \equiv 1 \pmod{32}$ | (c) $333x \equiv 1 \pmod{77}$ |
| (d) $707x \equiv 1 \pmod{333}$                         | (e) $47x \equiv 1 \pmod{34}$ | (f) $34x \equiv 1 \pmod{47}$  |
| [Ans. : (a) 8, (b) 17, (c) 37, (d) 65, (e) 21, (f) 18] |                              |                               |

4. Solving Linear Congruence  $ax \equiv b \pmod{m}$ 

Our objective in this and the next section is to find solution to the congruence  $ax \equiv b \pmod{m}$ . Finding inverse of  $a$  is a special cases of this congruence, when  $b = 1$ . The method that we will use to find the solution to the congruence  $ax \equiv b \pmod{m}$  is the same as that we use to find the inverse of  $a$  modulo  $m$ . Only difference between the two is that the inverse is unique congruent modulo  $m$ . There may be several incongruent solutions, in fact  $(a, m)$  number of incongruent solutions modulo  $m$ .

**Theorem :** The linear congruence  $ax \equiv b \pmod{m}$  has a solution if and only if  $d \mid b$ , where  $d = (a, m)$ . In that case, there are precisely  $d$  incongruent solutions modulo  $m$ .

**Proof :** Since  $ax \equiv b \pmod{m}$  holds if and only if  $m \mid ax - b$ , a solution to the congruence problem exists if and only if there is an integer  $y$ , such that  $ax - b = my$ . Thus, the problem of solving the congruence reduces to finding a solution to the Diophantine equation

$$ax - my = b$$

(We have studied how to solve these types of equations by Euclidean algorithm, in § 5, page 3-9 of Chapter 3.)

We know the equation (I) has a solution if and only if  $d \mid b$ , where  $d = (a, m) = (a, m)$ .

Moreover, if  $x_0, y_0$  is a solution, then these solutions are

$$x = x_0 + (m/d)t, \quad y = y_0 + (a/d)t \quad \text{where } t \text{ is arbitrary.}$$

We claim that for  $t = 0, 1, \dots, d-1$ , these solutions are mutually incongruent modulo  $m$ .

Suppose they are not incongruent. Then there exist integers  $t_1$  and  $t_2$ , such that  $t_1 \neq t_2$ ,  $0 \leq t_1 < d$ ,  $0 \leq t_2 < d$ , such that  $x_0 + (m/d)t_1 = x_0 + (m/d)t_2 \pmod{m}$ .

Subtracting  $x_0$  from both sides of the congruence, we get

$$(m/d)t_1 \equiv (m/d)t_2 \pmod{m}.$$

But  $(m/d, m) = m/d$ . Therefore, by Theorem 4, Chapter 4, we have  $t_1 \equiv t_2 \pmod{(m/d)}$ . I.e.,  $t_1 \equiv t_2 \pmod{d}$ .

This means  $d \mid t_1 - t_2$ . But this is impossible as  $0 \leq t_1 - t_2 < d$ .

Hence, our claim holds.

## Note ...

Note that  $d$  incongruent solutions are  $x_0, x_0 + (m/d), x_0 + (2m/d), \dots, x_0 + ((d-1)m/d)$ , where  $x_0$  is a known solution.

If  $(a, m) = 1$ , all solutions are congruent modulo  $m$ .

## Example 1 : Solve the following linear congruences :

$$(1) 3x \equiv 2 \pmod{7}, \quad (2) 6x \equiv 3 \pmod{9}, \quad (3) 128x \equiv 833 \pmod{1001}.$$

Sol. : (1)  $3x \equiv 2 \pmod{7}$

Since  $(3, 7) = 1$ , there is only one solution congruent modulo 7. To find the solution, we use Euclidean algorithm to establish  $(3, 7) = 1$  in the first column. And in the second column, express the remainder in each step in the Euclidean algorithm in terms of  $a = 3$  and  $m = 7$ . We continue this process till we reach  $(3, 7) = 1$ . Then the coefficient of  $a$  in this expression in the second column is the solution.

1. $m = 7 = 2 \times 3 + 1$	(I) $1 = m - 2a$	[By 1]
2. $a = 3 = 3 \times 1 + 0$		

Therefore,  $-2$  is a solution to  $3x \equiv 1 \pmod{7}$ . To get the solution of  $3x \equiv 2 \pmod{7}$ , we multiply the solution by 2. Thus,  $x_0 = -4$  is the solution of the required solution. If we are interested only in positive solution, note that  $-4 \equiv 3 \pmod{7}$  (i.e.,  $x_0' = 7 + x_0$ ).

Hence,  $x_0' = 3$  is a positive solution.

$$(2) 6x \equiv 3 \pmod{9} : \quad \text{Here, } a = 6, m = 9, b = 3, (a, m) = (6, 9) = 3 \mid b = 3.$$

Hence, there are  $(a, m) = 3$ , incongruent solutions modulo 9. Here,  $a = 6, m = 9$ . Therefore,

1. $m = 9 = 1 \times 6 + 3$	(I) $3 = m - a$	[By 1]
2. $a = 6 = 2 \times 3 + 0$	Coefficient of $a$ is $-1$ .	

Since,  $(a, m) = 3$  and there will be 3 incongruent solutions.

$x_0 = -1$  is a solution of  $6x \equiv 3 \pmod{9}$ .

The other solutions  $x = x_0 + (m/d)t$  are in this case  $x = -1 + 3t$ , where  $t$  is arbitrary.

In order to get positive values of  $x$ , we do not choose  $t = 0$ . We choose  $t = 1, 2, 3$ . So that,  $x = 2, 5, 8$  are incongruent solutions modulo 9.

$$(3) 128x \equiv 833 \pmod{1001} : \quad \text{Here } a = 128, m = 1001, b = 833.$$

In the first column, we find  $(a, m)$  using Euclidean algorithm and then, in the second column, express  $(a, m)$  as an expression in  $a$  and  $b$ .

1. $m = 1001 = 8 \times 128 - 23$	(I) $23 = 8a - m$	[By 1]
2. $a = 128 = 6 \times 23 - 10$	(II) $10 = 6(8a - m) - a$	[By 2 and (I)]
	= $47a - 6m$	
3. $23 = 2 \times 10 + 3$	(III) $3 = (8a - m) - 2(47a - 6m)$	[By 3, (I) and (II)]
	= $-86a + 11m$	
4. $10 = 3 \times 3 + 1$	(IV) $1 = (47a - 6m) - 3(-86a + 11m)$	
	= $305a - 39m$	

Hence,  $(a, m) = 1$ , and there will be only one solution. All other solution will be congruent modulo 1001.

Therefore, 305 is a solution of the congruence  $128x \equiv 1 \pmod{1001}$ .

A solution of the congruence  $128x \equiv 833 \pmod{1001}$  is  $305 \times 833 = 254065$  congruent modulo 1001.

Since,  $254065 = 253 \times 1001 + 812$ , we may choose  $x_0 = 812$  as a solution as it is a smaller positive number. This may be convenient but theoretically unnecessary.

**Example 2 :** An astronaut orbits the Earth in a space vehicle in a period that is an exact multiple of 1 hour that is less than a day. The astronaut notes that when he completes 11 orbits his clock reads 17 hours in a 24 hours clock. He started orbiting the earth at 0 hour. Find the orbital period of the space craft.

Sol.: Suppose the orbital period is  $x$  hours, where  $x$  is an integer. (This is by data that the period is an exact multiple of 1 hour). He makes 11 orbits therefore, he is in  $11x$  hours in space. If his clock shows 17 in the 24 hours clock, then assuming he was in space for  $k$  days and 17 hours, we have

$$11x = 17 + 24k$$

$$\text{Therefore, } 11x \equiv 17 \pmod{24}$$

To solve this equation let  $a = 11$ ,  $b = 17$ ,  $m = 24$ .

Since  $(a, m) = 1$ , there is unique solution modulo 24. We use Euclidean algorithm to show that  $(a, m) = 1$  in the first column and express each remainder obtained in the process in terms of  $a$  and  $m$ . Till 1 is expressed in  $a, m$  in the second column. The coefficient of  $a$  is a solution of  $11x \equiv 1 \pmod{24}$ .

$$\begin{aligned} 1. \quad m &= 24 = 2 \times 11 + 2 \\ 2. \quad a &= 11 = 5 \times 2 + 1 \end{aligned}$$

$$\begin{aligned} (\text{i}) \quad 2 &= m - 2a & [\text{By i}] \\ (\text{ii}) \quad 1 &= a - 5(m - 2a) & [\text{By 2 and (i)}] \\ &= 11a - 5m \end{aligned}$$

Hence  $x_0 = 11$  is a solution of  $11x \equiv 1 \pmod{24}$

A solution of the equation  $11x \equiv 17 \pmod{24}$  is  $11 \times 17 = 187$ .

The general solution is  $x = 187 + 24t$  where  $t$  is arbitrary. We choose  $t$ , so that, the given condition is satisfied. We are given that the period is less than a day. Therefore, we have  $0 < 187 + 24t < 24$ .

There is only one choice, i.e.,  $t = -7$ . Then  $x = 187 - 168 = 19$ .

Therefore, the orbital period is 19 hours.

#### Note ...

The strength of the above method of using Euclidean Algorithm lies in its universality. The above problems can be solved, at times more easily, by making coefficient of  $x$  unity using different tricks and finding a solution  $x_0$  of the congruence. The other solutions are  $x = x_0 + (m/d)t$  where  $t$  is arbitrary. We indicate here how the above problems can be solved more easily. We leave a reader to provide the justifications for the steps used while computing the solution.

#### Example 1 : (1) $3x \equiv 2 \pmod{7}$

Multiply by 2. Then  $4 \equiv 6x \equiv -x \pmod{7}$ . Hence,  $x \equiv -4 \equiv 3 \pmod{7}$ . Hence,  $x = 3$ .

$$(2) \quad 6x \equiv 3 \pmod{9}$$

Cancelling 3,  $2x \equiv 1 \pmod{3}$ . Hence,  $2 \equiv 4x \equiv x \pmod{3}$ . Hence,  $x \equiv 2$

$$(3) \quad 128x \equiv 833 \pmod{1001}$$

$$128x \equiv 833 \equiv -168 \pmod{1001}$$

Dividing by 8, we get

$$16x \equiv -21 \pmod{1001} \equiv 980 \pmod{1001}$$

Dividing by 4, we get

$$4x \equiv 245 \pmod{1001} \equiv -756 \pmod{1001}$$

Dividing by 4, we get

$$x \equiv -189 \pmod{1001} \equiv 812 \pmod{1001}$$

Hence,  $x = 812$ .

#### Example 2 : $11x \equiv 17 \pmod{24}$

Since  $12 \mid 24$ , we have  $11x \equiv 17 \pmod{12}$

$$\text{Therefore, } 11x \equiv 5 \pmod{12}, \quad 5 \equiv 11x \equiv -x \pmod{12}$$

$$\text{Therefore, } x \equiv -5 \equiv 7 \pmod{12}. \text{ Hence, } x = 7 + 12k.$$

Choose  $k$ , so that,  $0 < 7 + 12k < 24$ .

Clearly,  $k = 1$  and  $x = 19$ .

#### Example 3 : Solve the congruence $9x \equiv 21 \pmod{30}$ .

Sol.: Since  $(9, 30) = 3$  and  $3 \mid 21$ , the solution exists and if  $x_0$  is a solution then there are three incongruent modulo 30 solutions,

$$x = x_0 + (30/3) t, \quad t = 0, 1, 2.$$

By Theorem 4 discussed on page 4-5, the given congruence is equivalent to

$$3x \equiv 7 \pmod{30/3}, \quad \text{i.e., } 3x \equiv 7 \pmod{10}$$

But  $7 \equiv -3 \pmod{10}$ .

$$\text{Therefore, } 3x \equiv -3 \pmod{10}.$$

Again applying Theorem 4, as  $(3, 10) = 1$ , we get  $x \equiv -1 \pmod{10}$ , i.e.,  $x \equiv 9 \pmod{10}$ .

Hence, the solutions are  $x = 9 + 10t$ ,  $t = 0, 1, 2$ , i.e.,  $x = 9, 19, 29$ , modulo 30.

(Note that they are not incongruent modulo 10).

### EXERCISE - III

1. Find solutions of each of the following linear congruences :

- |                                |                               |                                  |
|--------------------------------|-------------------------------|----------------------------------|
| (a) $333x \equiv 2 \pmod{707}$ | (b) $51x \equiv 6 \pmod{111}$ | (c) $1001x \equiv 1212 \pmod{4}$ |
| (d) $63x \equiv 110 \pmod{23}$ | (e) $9x \equiv 12 \pmod{15}$  | (f) $7x \equiv 4 \pmod{12}$      |
| (g) $172x \equiv 12 \pmod{20}$ | (h) $9x \equiv 21 \pmod{60}$  |                                  |
- [Ans. : (a) -276 (positive solution is 431), (b) -26, 48, 122 (positive solution are 85, 48, 122), (c) 0, (d) 20, (e) 8, 13, 18, (f) 4, (g) 1, 6, 11, 16, (h) 9, 29, 49.]

2. Solve the following congruences :

- |                               |                                |                              |
|-------------------------------|--------------------------------|------------------------------|
| (a) $18x \equiv 30 \pmod{42}$ | (b) $45x \equiv 105 \pmod{30}$ | (c) $9x \equiv 12 \pmod{15}$ |
|-------------------------------|--------------------------------|------------------------------|

- [Ans. : (a) 4, 11, 18, 25, 32, 39; (b) 9, 19, 29; (c) 8, 13, 3.]

#### 5. Fermat's Little Theorem

Let  $p$  be a prime and  $a$  a positive integer, such that  $p \nmid a$ . Then,

$$a^{p-1} \equiv 1 \pmod{p}$$

**Proof :** Recall that  $0, 1, 2, \dots, p-1$  is a complete system of residues modulo  $p$  and therefore,  $1, 2, \dots, p-1$  is the set of (smallest) positive integers, no two of which are congruent and all of them are incongruent to 0. Consider  $a, 2a, \dots, (p-1)a$ . Clearly, they are positive (since  $a > 0$ ). We

claim that they are mutually incongruent. Suppose our claim is not true. Then, there will be positive integers  $r$  and  $s$ , with  $1 \leq r < s \leq p-1$ , such that  $ra \equiv sa \pmod{p}$ . Since  $p \nmid a$  we cancel  $a$  from both sides and get  $r \equiv s \pmod{p}$ . But this is a contradiction as  $1 \leq r < s < p$ . Therefore,  $a, 2a, \dots, (p-1)a$  are  $(p-1)$  positive integers mutually incongruent. Since  $0, 1, \dots, p-1$  is a complete system, each one in the set of positive integers  $a, 2a, \dots, (p-1)a$  must be congruent to exactly one positive integer from  $1, 2, \dots, p-1$  modulo  $p$ . Since  $x \equiv u \pmod{p}$ ,  $y \equiv v \pmod{p}$  implies  $xy \equiv uv \pmod{p}$ , we get

$$\begin{aligned} a \times 2a \times \dots \times (p-1)a &\equiv 1 \times 2 \times \dots \times (p-1) \pmod{p} \\ \text{i.e., } a^{p-1} \times (1 \times 2 \times \dots \times (p-1)) &\equiv 1 \times 2 \times \dots \times (p-1) \pmod{p} \\ \text{i.e., } a^{p-1} (p-1)! &\equiv (p-1)! \pmod{p} \\ \text{But } p \nmid (p-1)! \text{, hence, cancelling } (p-1)! \text{ from both sides, we have } a^{p-1} &\equiv 1 \pmod{p}. \end{aligned}$$

## Pierre-Simon de Fermat (1601 - 1665)

A great French mathematician Pierre-Simon de Fermat was the son of a leather merchant. Though he was lawyer by profession, he used his leisure time for mathematics. He did not publish his discoveries but had correspondence with many contemporary mathematicians. He contributed to several branches of mathematics but he is best known for his work in number theory. He used to write his results in the margins of the books he read. In one of the books he wrote, "I have discovered a truly wonderful proof of the result that the equation  $x^n + y^n = z^n$  has no positive integer solution for  $n \geq 3$ , but the margin is too small to contain it". This is known as Fermat's Last Theorem. What Fermat thought is not known but the problem is not fully solved till to-day.



**Corollary :** If  $p$  is a prime and  $a$  is a positive integer, then

$$a^p \equiv a \pmod{p}$$

**Proof :** Clearly, if  $p \nmid a$ , then we have by the above theorem  $a^{p-1} \equiv 1 \pmod{p}$  and therefore, by multiplying both sides by  $a$ , we get  $a^p \equiv a \pmod{p}$ . Hence,  $a^p \equiv a \pmod{p}$ .

If  $p \mid a$ , then clearly,  $0 \equiv a \pmod{p}$  and  $0 \equiv a^p \pmod{p}$ . Hence,  $a^p \equiv a \pmod{p}$ .

**Example 1 :** Using Fermat's little theorem, show that  $5^{38} \equiv 4 \pmod{11}$ .

Clearly,  $5^{38} = 5^{30} \times 5^8 = (5^{10})^3 \times (5^2)^4$

As  $11 \nmid 5$ , by Fermat's little theorem, we have  $5^{10} \equiv 1 \pmod{11}$

Therefore,  $(5^{10})^3 \equiv 1^3 \pmod{11}$ .

Hence,  $(5^{10})^3 \equiv 1 \pmod{11}$

Now,  $5^2 \equiv 25 \pmod{11} \equiv 25 \pmod{11} \equiv (22+3) \pmod{11} \equiv 3 \pmod{11}$

Therefore,  $5^2 \equiv 3 \pmod{11}$  and consequently

$$\begin{aligned} (5^2)^4 &\equiv 3^4 \pmod{11} \equiv 81 \pmod{11} \\ &\equiv (77+4) \pmod{11} \equiv 4 \pmod{11} \quad [\text{Since } 11 \mid 77] \end{aligned}$$

Therefore,  $(5^2)^4 \equiv 4 \pmod{11}$

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

$$5^{38} \equiv 4 \pmod{11}$$

**Note ....**

The Fermat's theorem says if  $p$  is prime and  $p \nmid a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ . Therefore, if  $p \nmid a$  and  $a^{p-1} \not\equiv 1 \pmod{p}$ , then  $p$  cannot be prime. This fact is used to test the primality of a positive integer.

**Example 2 :** Test if 117 is a prime number.

**Note ....**

No odd prime divides 2. Therefore, for testing primeness, we usually use 2, the smallest positive integer for the purpose.

**Sol. :** Since  $117 \nmid 2$ , the Fermat's little theorem must hold if 117 is prime and we must have

$$2^{116} \equiv 1 \pmod{117} \quad (I)$$

If 117 is prime, (I) must be a true congruence. If (I) is false, then 117 cannot be a prime.

$$\text{Consider, } 2^7 \equiv 128 \equiv 11 \pmod{117} \quad [\text{For, } 128 = 117 + 11] \quad (II)$$

$$\text{Then, } 2^{14} \equiv 121 \equiv 4 \pmod{117} \quad [\text{For, } 121 = 117 + 4] \quad (III)$$

But  $(4, 117) = 1$  and therefore by Theorem 4 above, we cancel 4, to get

$$2^{12} \equiv 1 \pmod{117} \quad (IV)$$

Since,  $116 = 9 \times 12 + 8$ , we get

$$2^{116} = (2^{12})^9 \times 2^8 \quad (V)$$

$$\text{But by (IV), } (2^{12})^9 \equiv 1^9 \equiv 1 \pmod{117} \quad (VI)$$

Hence,  $2^{116} \equiv 2^8 \pmod{117}$

But multiplying the congruence in (VI) by 2, we get

$$2^8 \equiv 2 \times 11 = 22 \pmod{117} \quad (VII)$$

$$\text{Hence, } 2^{116} \equiv 22 \pmod{117}$$

From (I) and (VII), we conclude that if 117 is prime, then  $22 \equiv 1 \pmod{117}$ .

But  $117 \nmid 22 - 1$ . Hence, 117 is not prime.

**Corollary 2 :** Let  $a$  be an integer and  $p$  be a prime with  $p \nmid a$ , then

$$a^{p-2} \text{ is inverse of } a \text{ modulo } p$$

**Proof :** By Fermat's Theorem,  $a^{p-1} \equiv 1 \pmod{p}$

$$\text{Hence, } a(a^{p-2}) \equiv a^{p-1} \equiv 1 \pmod{p}$$

i.e.,  $a^{p-2}$  is inverse of  $a$  modulo  $p$ .

**Corollary 3 :** Let  $a$  and  $b$  be integers,  $p$  a prime and  $p \nmid a$ , then

$$a^{p-2} b \text{ is a solution of } ax \equiv b \pmod{p}$$

**Proof :** Multiplying the given congruence by  $a^{p-2}$ , we get

$$a^{p-2}(ax) \equiv a^{p-2}b \pmod{p}$$

$$\text{i.e., } a^{p-1}x \equiv a^{p-2}b \pmod{p} \quad (I)$$

By Fermat's Theorem,  $a^{p-1} \equiv 1 \pmod{p}$ . If we multiply this congruence by  $x$ , we get

$$a^{p-1}x \equiv x \pmod{p} \quad (II)$$

Using the result (I), (II) and transitivity of congruence, we get  
 $x \equiv a^{p-2} b \pmod{p}$

Hence, the theorem.

**Example 3 :** Using Fermat's Little theorem, find the least positive residue of  $2^{1000000}$  after dividing by 17.

Sol. : Since  $17 \nmid 2$ ,  $2^{16} \equiv 1 \pmod{17}$ .

Observe  $1000000 = 62500 \times 16$ .

Therefore,  $2^{1000000} = (2^{16})^{62500}$

Hence,  $2^{1000000} = (2^{16})^{62500} \equiv 1^{62500} \pmod{17}$

Hence,  $2^{1000000} \equiv 1 \pmod{17}$ .

Therefore, the least positive residue is 1.

**Example 4 :** Show that  $3^{10} \equiv 1 \pmod{11^2}$ .

Sol. : By Fermat's Little Theorem,

$$3^{10} \equiv 1 \pmod{11}$$

Therefore, there exist an integer  $k$ , such that

$$3^{10} \equiv 11k + 1 \quad (\text{I})$$

Squaring and rearranging the terms;

$$3^{20} \equiv 11^2 k^2 + (22k + 1) \quad (\text{II})$$

Hence,  $3^{10} \times 3^{10} \equiv 3^{20} \equiv (22k + 1) \pmod{11^2}$

Substituting  $3^{10} \equiv 11k + 1$  in one of the factors in the square term, we get

$$3^{10}(11k + 1) \equiv (22k + 1) \pmod{11^2}$$

Multiplying the congruence by 11, we get

$$3^{10}(11^2 k + 11) \equiv (22k + 1) \pmod{11^2}$$

Therefore,  $3^{10} \cdot 11 \equiv 11 \pmod{11^2}$

(Since  $22k \cdot 11^2 \pmod{11^2} = 0$ ,  $3^{10} \cdot 11^2 \cdot k \pmod{11^2} = 0$ )

Splitting,  $11 = 10 + 1$ , we get

$$3^{10} \cdot 10 + 3^{10} \equiv (10 + 1) \pmod{11^2}$$

Subtracting 10 from both sides, we get

$$(3^{10} \cdot 10 - 10) + 3^{10} \equiv 1 \pmod{11^2}$$

But  $3^{10} \cdot 10 - 10 = 59049 \times 10 - 10 = 4880 \times 11^2$

Thus,  $11^2 \mid (3^{10} \cdot 10 - 10)$ , and  $(3^{10} \cdot 10 - 10) \equiv 0 \pmod{11^2}$

Hence,  $3^{10} \equiv 1 \pmod{11^2}$ .

There is some theoretical importance to this example. The example shows that  $p$  is prime for  $a^{p-1} \equiv 1 \pmod{p}$  to hold is a sufficient condition, not a necessary condition. In other words,  $a^{p-1} \equiv 1 \pmod{n}$  does not imply  $n$  is the prime  $p$ .

**Example 5 :** Find solutions of the following congruences.

$$(a) 7x \equiv 12 \pmod{17} \quad (b) 4x \equiv 11 \pmod{19}$$

Sol. : (a) By Fermat's Theorem,  $x = 7^{15} \times 12$  is a solution congruent modulo 17.

We observe that  $7^3 \times 2 = 686 = 40 \times 17 + 6$ .

$$\text{Therefore, } 7^3 \times 2 \equiv 6 \pmod{17} \quad (\text{I})$$

We will make repeated use of (I) to simplify  $x = 7^{15} \times 12 \pmod{17}$  as follows:

$$\therefore x = 7^{15} \times 12 = (7^{12} \times 6)(7^3 \times 2) \equiv (7^{12} \times 6)(6 \pmod{17})$$

$$\therefore x = (7^6 \times 6 \times 3)(7^3 \times 2) \equiv (7^6 \times 6 \times 3)(6 \pmod{17})$$

$$\therefore x = (7^3 \times 6 \times 27)(7^3 \times 2) \equiv (7^3 \times 6 \times 27)(6 \pmod{17})$$

$$\therefore x = (6 \times 81)(7^3 \times 2) \equiv (6 \times 81)(6 \pmod{17})$$

$$\therefore x = (81)(36) \equiv (81)(2 \pmod{17})$$

$$\therefore x = 162 \equiv 9 \pmod{17}$$

(b) By Fermat's Theorem  $x = 4^{17} \times 11$  is a solution modulo 19.

We observe that  $4^4 \times 11 = 256 \times 11 = 2816 \equiv 148 \times 19 + 4$ ,

$$\therefore 4^4 \times 11 \equiv 4 \pmod{19}$$

Consequently,  $x = 4^{17} \times 11 \equiv 4^{14} \pmod{19}$

$$\text{Now, } 4^2 \equiv 16 \equiv -3 \pmod{19}$$

$$\therefore 4^4 \equiv 9 \equiv -10 \pmod{19}$$

$$\text{Hence, } 4^8 \equiv 100 \equiv 5 \pmod{19}$$

$$\therefore 4^{14} \equiv 4^8 \times 4^4 \times 4^2 \equiv 5 \times 9 \times (-3) \equiv -135 \equiv -2 \equiv 17 \pmod{19}$$

$$\text{Hence, } x = 17 \pmod{19}$$

**Example 6 :** Find the last digit of the base 7 expansion of  $3^{100}$  using Fermat's Theorem.

Sol. : We need to find the remainder on dividing  $3^{100}$  by 7, i.e., to find  $3^{100} \pmod{7}$ .

By Fermat's Theorem,  $3^6 \equiv 1 \pmod{7}$ .

Observe that  $100 = 16 \times 6 + 4$

$$\text{Hence, } 3^{100} \equiv (3^6)^{16} \times 3^4 \equiv 1^{16} \times 3^4 \equiv 3^4 \equiv 81 \pmod{7}$$

Since,  $81 = 11 \times 7 + 4$ , we get  $3^{100} \equiv 4 \pmod{7}$ .

Therefore, 4 is the required last digit.

**Example 7 :** Let  $p$  and  $q$  be distinct primes, show that  $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ .

Sol. : By Fermat's little Theorem, we have  $p^{q-1} \equiv 1 \pmod{q}$  and  $q^{p-1} \equiv 1 \pmod{p}$ .

Therefore, there exist integers  $h$  and  $k$ , such that  $p^{q-1} - 1 = hq$  and  $q^{p-1} - 1 = kp$ .

On multiplication of these equations and rearranging the terms, we get

$$p^{q-1} q^{p-1} - hq \cdot kp = p^{q-1} + q^{p-1} - 1$$

$$\therefore p^{q-1} + q^{p-1} - 1 = Kpq \text{ for some integer.}$$

Hence, the result :  $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ .

#### EXERCISE - IV

- Find the least positive residue of  $3^{1000000}$  modulo 13. [Ans. : 3]
- Prove the following congruences using Fermat's Little Theorem.
  - $7x \equiv 12 \pmod{17}$
  - $4x \equiv 11 \pmod{19}$
- $7^{1000000} \equiv 1 \pmod{11}$
- $8^{57} \equiv 3 \pmod{5}$
- $3^{1000} \equiv 4 \pmod{7}$

[Ans. : No]

4. Solve the following congruences.
- (a)  $5x \equiv 11 \pmod{23}$       (b)  $11x \equiv 5 \pmod{7}$       (c)  $7x \equiv 3 \pmod{19}$   
 [Ans. : (a) 16, (b) 3, (c) 14]
5. Prove that  $2^{340} \equiv 1 \pmod{341}$ .  
 (Hint :  $341 = 11 \times 31$ ,  $2^{10} = 1024 = 33 \times 31 + 1$ ,  $2^{11} \equiv 2 \pmod{31}$ ).  
 Using Fermat's Theorem,  
 $2^{31} \equiv (2^{10})^3 \times 2 \equiv 2 \pmod{11}$   
 $2^{341} \equiv (2^{31})^{11} \times 2^{31} \equiv 2^{31} \pmod{31}$   
 But  $2^{31} \equiv 2 \pmod{31}$ . Therefore,  $2^{341} \equiv 2 \pmod{341}$ .  
 $2^{341} \equiv (2^{31})^{11} \equiv 2^{11} \pmod{11}$ ,  
 and  $2^{11} \equiv 2 \pmod{11}$  lead to  
 $2^{341} \equiv 2 \pmod{11}$ .  
 Thus,  $31 \mid 2^{341} - 2$ ,  $11 \mid 2^{341} - 2$  and by Corollary 2, Theorem 2, § 2, page 3-3 of Chapter 3  
 $31 \times 11 \mid 2^{341} - 2$ .)  
 6. Find the least positive residue of  $3^{201}$  modulo 11. [Ans. : 3]  
 7. Let  $p$  and  $q$  be distinct primes, such that  $a^p \equiv a \pmod{q}$  and  $a^q \equiv a \pmod{p}$ . Prove that  $a^{pq} \equiv a \pmod{pq}$ .  
 (Hint :  $a^{pq} \equiv a^q \pmod{q}$ ,  $q \mid a^{pq} - a$ ,  $p \mid a^{pq} - a$ .  
 Use Corollary 2 (1), Theorem 2, § 2, page 3-3 of Chapter 3.)

### 6. Euler's Theorem

Euler's Theorem is a generalization of the Fermat's little theorem. Fermat's little theorem states that  $a^{\phi(m)} \equiv 1 \pmod{m}$ , where  $m$  is a prime. This condition is no more needed in Euler's Theorem. However, we need to know, what is  $\phi(n)$ , to understand the meaning of Euler's Theorem.

**Definition :** Let  $n > 0$  be an integer. The Euler's phi-function  $\phi(n)$  is the number of positive integers not exceeding  $n$ , which are relatively prime to  $n$ .

**Illustration :**  $\phi(1) = 1$ . For  $(1, 1) = 1$  and 1 does not exceed 1 and  $1 > 0$ .

$\phi(2) = 1$ . For,  $n = 1$  is the only positive integer less than 2, such that  $(n, 2) = 1$ .

$\phi(3) = 2$ . For 1 and 2 are the only two positive integers less than 3, that are relatively prime to 3. Note that, there will be infinitely many integers relatively prime to 3 and exceeding 3.

Likewise,  $\phi(4) = 2$ , for 1 and 3 are the two positive integers less than 4, relatively prime to 4.  
 $\phi(30) = 8$  and  $\phi(80) = 16$ .

For 1, 7, 11, 13, 17, 19, 23, 29 are the eight numbers relatively prime to 30 not exceeding 30.

The positive numbers relatively prime and not exceeding 60 are the above 8 numbers in addition to the following 8 numbers :

31, 37, 41, 43, 47, 49, 53, 59.

It is easy to observe that for any prime  $p$ ,  $\phi(p) = p - 1$ .

**Definition :** Let  $n > 0$  be a positive integer. A set of integers is called a reduced residue system modulo  $n$  if

- (i) It has  $\phi(n)$  integers,

- (ii) each integer in the set is relatively prime to  $n$ , and  
 (iii) the integers are mutually incongruent modulo  $n$ .

**Illustration :** (a) The set 1, 5 is a reduced residue system modulo 6. For,  
 (i) These are  $\phi(6) = 2$  integers.  
 (ii) The integers 1 and 5 are relatively prime.

- (iii)  $1 \neq 5 \pmod{6}$

Note that 1, -1 or 5, -5 are other reduced residue systems modulo 6.

(b) 1, 3, 5, 7 is a reduced residue system modulo 8. For, they are  $\phi(8) = 4$  elements, relatively prime to 8 and mutually incongruent modulo 8.

- (c) If  $p$  is a prime integer, then 1, 2, 3, ...,  $p - 1$  is a reduced residue system modulo  $p$ .

**Theorem 1 :** Let  $n > 0$  be an integer. Let  $r_1, r_2, \dots, r_{\phi(n)}$  be a reduced residue system modulo  $n$  and  $a$  a positive integer with  $(a, n) = 1$ . Then  $ar_1, ar_2, \dots, ar_{\phi(n)}$  is also a reduced residue system modulo  $n$ .

**Proof :** To prove the theorem, we need to prove

- (i) each  $ar_j$  is relatively prime to  $n$ .

(ii)  $ar_1, ar_2, \dots, ar_{\phi(n)}$  are mutually incongruent modulo  $n$ .

To prove (i), i.e., to prove  $(ar_j, n) = 1$ .

Suppose  $(ar_j, n) > 1$ . Then  $(ar_j, n)$  has a divisor  $p$  where  $p$  is a prime. Therefore,  $p \mid n$  and  $p \mid ar_j$ . But  $p \mid ar_j$  implies  $p \mid a$  or  $p \mid r_j$  [See (1), § 3, page 3-4 of Chapter 3].

If  $p \mid n$  and  $p \mid a$ , then  $p \mid (a, n)$ . But this is impossible, as  $(a, n) = 1$ .

If  $p \mid n$  and  $p \mid r_j$ , then this also leads to contradiction. For,  $r_j$  is a member of reduced residue system modulo  $n$  and then by definition  $(r_j, n) = 1$ .

Therefore,  $p \nmid ar_j$  and thus  $(ar_j, p) = 1$  for all  $j = 1, 2, \dots, \phi(n)$ .

To prove (ii), i.e., to prove  $ar_j \not\equiv ar_k \pmod{n}$  for all  $j \neq k$ ;  $j, k = 1, 2, \dots, \phi(n)$ .

Suppose  $ar_j \equiv ar_k \pmod{n}$  for some pair  $j, k, j \neq k, 1 \leq j \leq \phi(n), 1 \leq k \leq \phi(n)$ . Since  $(a, n) = 1$ , we can cancel  $a$ , to get  $r_j \equiv r_k \pmod{n}$ .

But this contradicts the fact that  $r_1, r_2, \dots, r_{\phi(n)}$  is a reduced residue system modulo  $n$ .

Therefore,  $ar_j \not\equiv ar_k \pmod{n}$ . Hence, the theorem.

**Example 1 :** The set 1, 2, 4, 5, 7, 8 forms a reduced residue system modulo 9. Since  $(4, 9) = 1$ , we have another reduced residue system modulo 9, namely 4, 8, 16, 20, 28, 32. But these integers have more interesting properties. Note that  $4 \equiv 4 \pmod{9}$ ,  $8 \equiv 8 \pmod{9}$ ,  $16 \equiv 7 \pmod{9}$ ,  $20 \equiv 2 \pmod{9}$ ,  $28 \equiv 1 \pmod{9}$ ,  $32 \equiv 5 \pmod{9}$ . Thus, the new reduced residue system is congruent to the least positive reduced residue system 1, 2, 4, 5, 7, 8, most likely, in different order. Therefore, if we multiply these six congruences then we have

$$4 \times 8 \times 16 \times 20 \times 28 \times 32 \equiv 1 \times 2 \times 4 \times 5 \times 7 \times 8 \pmod{9}$$

By taking the common factor 4 out and rearranging the factors on the left, we get

$$4^5 (1 \times 2 \times 4 \times 5 \times 7 \times 8) \equiv (1 \times 2 \times 4 \times 5 \times 7 \times 8) \pmod{9}$$

Since  $(1 \times 2 \times 4 \times 5 \times 7 \times 8, 9) = 1$ , we can cancel the common factor and since  $6 = \phi(9)$ , we write the congruence in more elegant form

$$4^{\phi(9)} \equiv 1 \pmod{9}$$

Since  $(7, 9) = 1$ , we can get another reduced residue system  $7, 14, 28, 35, 49, 56$  modulo 9. Clearly,  $7 \equiv 7 \pmod{9}$ ,  $14 \equiv 5 \pmod{9}$ ,  $28 \equiv 1 \pmod{9}$ ,  $35 \equiv 8 \pmod{9}$ ,  $49 \equiv 4 \pmod{9}$ ,  $56 \equiv 2 \pmod{9}$ . Thus, the new system is congruent to  $1, 2, 4, 5, 7, 8$  in different order.

Therefore,  $7 \times 14 \times 28 \times 35 \times 49 \times 56 \equiv 1 \times 2 \times 4 \times 5 \times 7 \times 8 \pmod{9}$

On simplification and rearranging the terms

$$7^6 \equiv 1 \times 2 \times 4 \times 5 \times 7 \times 8 \equiv 1 \times 2 \times 4 \times 5 \times 7 \times 8 \pmod{9}$$

$$\text{or } 7^6 \equiv 1 \pmod{9}.$$

This is not an accident. The result is true in general. In fact we have

**Euler's Theorem :** Let  $m$  be a positive integer and  $a$  be any integer  $(a, m) = 1$ . Then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

**Proof :** Recall that  $1, 2, 3, \dots, m-1$  form the least positive integers residues modulo  $m$ . We pick up from these  $m-1$  integers,  $r_1, r_2, \dots, r_{\phi(m)}$  which are relatively prime to  $m$ . Clearly, they form a reduced residue system modulo  $m$ . Since, we are given that  $(a, m) = 1$ , Theorem 1 (page 4-24), above, gives another reduced residue system modulo  $m$ , namely  $ar_1, ar_2, \dots, ar_{\phi(m)}$ . By Theorem 6, § 2, page 4-7,  $ar_1, ar_2, \dots, ar_{\phi(m)}$  are congruent to  $r_1, r_2, \dots, r_{\phi(m)}$  (not necessarily in the same order).

$$\text{Let, } ar_1 \equiv r_1' \pmod{m}$$

$$ar_2 \equiv r_2' \pmod{m}$$

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

I.e.,  $7^7 \times 2 = 15 - 4 = 11 \pmod{15}$   
Hence,  $x = 11 \pmod{15}$ .

**Example 3:** If  $7^{1047}$  is divided by 31, what will be the remainder?

Sol.: By Euler's Theorem, since  $(7, 31) = 1$  and  $\phi(31) = 30$ , we have

$$7^{30} \equiv 1 \pmod{31}$$

Since,  $1047 = 34 \times 30 + 27$ ,

$$7^{1047} = 7^{34 \times 30} \times 7^{27} = 1^{34} \times 7^{27} = 7^{27} \pmod{31}$$

Clearly,

$$7^2 \equiv 49 \equiv 2 \times 31 - 13 \equiv -13 \pmod{31}$$

$$7^4 \equiv (-13)^2 \equiv 169 \equiv 14 \pmod{31}$$

$$7^8 \equiv (7^4)^2 \equiv (14)^2 \equiv 196 \equiv 10 \pmod{31}$$

$$7^{16} \equiv (7^8)^2 \equiv (10)^2 \equiv 100 \equiv 7 \pmod{31}$$

$$7^{17} \equiv 7^{16} \times 7 \equiv 7^2 \equiv -13 \pmod{31}$$

$$7^{19} \equiv 7^{17} \times 7^2 \equiv (-13)(-13) \equiv 169 \equiv 14 \pmod{31}$$

$$\text{Therefore, } 7^{27} \equiv 7^{19} \times 7^8 \equiv 14 \times 10 \equiv 140 \equiv 16 \pmod{31}$$

Hence, 16 will be the required remainder.

**Example 4:** Show that if  $m$  is a positive integer relatively prime to  $a$  and  $a-1$ , then  $m \mid 1 + a + a^2 + \dots + a^{m-1}$

Sol.: Since  $m$  is relatively prime to  $a$ , we have by Euler's Theorem

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

$$\text{Therefore, } m \mid (a^{\phi(m)} - 1) = (a-1)(a^{\phi(m)-1} + \dots + a^2 + a + 1)$$

Since  $(m, a-1) = 1$ , by Euclid's lemma, it follows that

$$m \mid (a^{\phi(m)-1} + \dots + a^2 + a + 1)$$

**Note ...**

The condition  $(m, a-1) = 1$  is necessary.

For choose  $m = 4$  and  $a = 5$ . Then  $\phi(m) = 2$ ,

$$(a^{\phi(m)-1} + \dots + a^2 + a + 1) = (5^{2-1} + 1) = 6 \text{ and } 4 \nmid 6.$$

$$\text{Here, } (m, a-1) = (4, 5-1) = 4 \neq 1.$$

**Example 5:** If  $c_1, c_2, \dots, c_{\phi(m)}$  is a reduced residue system modulo  $m$ , where  $m > 1$ , then  $c_1 + c_2 + \dots + c_{\phi(m)} \equiv 0 \pmod{m}$ .

Sol.: Let  $a_1, a_2, \dots, a_{\phi(m)}$  be the least positive reduced residue system modulo  $m$ . Our claim is, if a positive integer  $a$  is in the system, then  $(m-a)$  also will be in the system.

Clearly, as  $1 \leq a < m$ , we have  $1 \leq m-a < m$ . Moreover

$$(m-a, m) = (-a, m) \quad [\text{By Theorem 1, § 2, Chapter 3}]$$

Therefore,  $(m-a, m) = (-a, m) = (a, m) = 1$ . Hence, the claim.

Thus, there are pairs  $a$  and  $m-a$  in the least positive reduced system  $a_1, a_2, \dots, a_{\phi(m)}$ . Since,  $\phi(m)$  is an even number for  $m > 1$ , there will be  $\phi(m)/2$  such pairs.

$$\text{Therefore, } a_1 + a_2 + \dots + a_{\phi(m)} = \frac{\phi(m)}{2} (a + m - a) = m \frac{\phi(m)}{2} \pmod{m}$$

$$\text{Therefore, } a_1 + a_2 + \dots + a_{\phi(m)} \equiv 0 \pmod{m}.$$

If  $c_1, c_2, \dots, c_{\phi(m)}$  is any other reduced residue system, then  $c_1, c_2, \dots, c_{\phi(m)}$  can be reordered, so that  $c_i \equiv a_i \pmod{m}$ .

Therefore,  $c_1 + c_2 + \dots + c_{\phi(m)} \equiv a_1 + a_2 + \dots + a_{\phi(m)} \equiv 0 \pmod{m}$

for any reduced residue system  $c_1 + c_2 + \dots + c_{\phi(m)}$ .

**Example 6:** Find the last two digits in the decimal expression of  $3^{100}$ .

Sol.: Clearly the last two digits in  $3^{100}$  are the remainder of  $3^{100}$  on the division by 100.

By Euler's Theorem,

$$3^{\phi(100)} \equiv 1 \pmod{100}$$

$$\text{Since, } \phi(100) = \phi(2^2 \times 5^2) = (2^2 - 2)(5^2 - 5) = 2 \times 20 = 40.$$

$$\text{We have, } 3^{40} \equiv 1 \pmod{100}$$

$$\text{Therefore, } 3^{80} \equiv (3^{40})^2 \equiv 1 \pmod{100}$$

Hence, on multiplying the last congruence by  $3^{20}$ , we get

$$3^{100} \equiv 3^{80} \times 3^{20} \equiv 3^{20} \pmod{100}$$

$$\text{Now, } 3^4 \equiv 81 \pmod{100}$$

$$3^8 \equiv (3^4)^2 \equiv 81^2 \equiv 6561 \pmod{100} \equiv 61 \pmod{100}$$

$$3^{16} \equiv (3^8)^2 \equiv 61^2 \equiv 3721 \equiv 21 \pmod{100}$$

$$\text{Therefore, } 3^{20} \equiv 3^{16} \times 3^4 \equiv 21 \times 81 \equiv 1701 \pmod{100}$$

Hence, the last two digits are 01.

### EXERCISE - V

1. Find a reduced residue system modulo :

(a) 4, (b) 8, (c) 9, (d) 12, (e) 13, (f) 14, (g) 18.

[Ans.: (a) 1, 3; (b) 1, 3, 5, 7; (c) 1, 2, 4, 5, 7, 8; (d) 1, 5, 7, 11;

(e) 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12; (f) 1, 3, 5, 9, 11, 13;

(g) 1, 5, 7, 11, 13, 17.]

2. Find a reduced residue system for  $2^m$  where  $m$  is a positive integers.

[Ans.: All odd integers from 1 to  $2^m - 1$ .]

(Hint : If  $p$  is a prime, note that all integers from 1 to  $p^k$ , barring  $p, 2p, 3p, \dots, (p^k - 1)p$  are relatively prime to  $p$ .)

3. Find a reduced residue system for  $3^m$ , where  $m$  is a positive integer.

[Ans.: 1, 2, 4, 5, 7, 8, ...,  $3^m - 2, 3^m - 1$ , all integers upto  $3^m$  barring multiples of 3.]

4. Use Euler's Theorem, to compute :

(a)  $7^{1615} \pmod{31}$  (b)  $11^{100000} \pmod{54}$  (c)  $3^{1000} \pmod{7}$

[Ans.: (a) 25, (b) 43, (c) 4.]

5. Let  $m = 30$ . Verify that the sum of all integers in a reduced residue system modulo  $m$  is zero modulo  $m$ .

6. Let  $a$  and  $b$  be relatively prime integers, show that  $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$

(Hint :  $a^{\phi(b)} + b^{\phi(a)} - 1 = kab$  for some  $k$ .)



Similarly, from (v),

$$\begin{aligned} 1 &= 21x \pmod{5} = (20x + x) \pmod{5} \\ &= x \pmod{5} \quad [\text{Since } 5 \mid 20x] \end{aligned}$$

i.e.,  $x \equiv 1 \pmod{5}$ .

Since, this equation is reduced from (v), we get

$$x_2 \equiv 1 \pmod{5}$$

Similarly, from (vi), we get

$$\begin{aligned} 1 &= 15x \pmod{7} = (14x + x) \pmod{7} \\ &= x \pmod{7} \quad [\text{Since } 7 \mid 14x] \end{aligned}$$

Therefore, (vi) reduces to  $x \equiv 1 \pmod{7}$  and we have  $x_3 \equiv 1 \pmod{7}$ . (ix)

Now, substitute the values of  $M_1, M_2, M_3$  and those of  $x_1, x_2, x_3$  obtained in (ix), (x) and (xi) in the equation (vii) to get

$$\begin{aligned} x &= 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 \\ &= 157 \pmod{M} = 105. \end{aligned}$$

Thus,  $x \equiv 105 \pmod{105}$

$$\equiv (105 + 52) \pmod{105}$$

$$\equiv 52 \pmod{105} \quad [\text{Since } 105 \mid 105]$$

Therefore, 52 is a number that leaves remainder 1, 2, 3 when divided by 3, 5, 7 respectively.

**Method 2:** The above problem can be solved without using the Chinese Remainder Theorem. This can be done by using iterative process, starting from the solutions of 1st equation and substituting it in the next, till all equations are exhausted. This method is a little less elegant but is more general and hence can be applied even if the moduli of the congruences are not relatively prime.

We illustrate the method by solving the previously given problem.

Solving  $x \equiv 1 \pmod{3}$ , we have  $x = 3t + 1$  for some integer  $t$ , substituting this value of  $x$  in (ii), we get

$$3t + 1 \equiv 2 \pmod{5} \quad \text{i.e.,} \quad 2 \equiv (3t + 1) \pmod{5}$$

Multiplying by 2, we have

$$4 \equiv (6t + 2) \pmod{5} = (t + 2) \pmod{5} \quad [\text{Since } 6t = 5t + t \text{ and } 5 \mid 5]$$

Adding 3, both sides, we get,

$$7 \equiv t \pmod{5} \quad \text{i.e.,} \quad t \equiv 7 \pmod{5}.$$

Therefore,  $t = 5u + 7$  for some integer  $u$ .

Substituting this value of  $t$  in  $x = 3t + 1$ , we have

$$x = 3(5u + 7) + 1 = 15u + 22$$

Therefore, (iii) becomes,

$$15u + 22 \equiv 3 \pmod{7}$$

i.e.,  $3 \equiv (15u + 22) \pmod{7}$

$$\equiv (14u + u + 21 + 1) \pmod{7}$$

$$\equiv (u + 1) \pmod{7}$$

$$[\text{Since } 7 \mid 14u \text{ and } 7 \mid 21]$$

Adding 6 on both sides of  $3 \equiv (u + 1) \pmod{7}$ , we get

$$9 \equiv u \pmod{7}$$

$$[\text{Since } 7 \mid 7]$$

$$u \equiv 9 \pmod{7}$$

Substituting  $u = 9$ , we get  $t = 5 \times 9 + 7 = 52$ .

Substituting this value of  $t$ , we get  $x = 3 \times 52 + 1 = 157$ .

The rest is as before.

**Example 2:** Solve the simultaneous congruences given below :

$$x \equiv 1 \pmod{5} \quad \text{(i)}$$

$$x \equiv 2 \pmod{6} \quad \text{(ii)}$$

$$x \equiv 3 \pmod{7} \quad \text{(iii)}$$

**Sol.:** Method 1, by the Chinese remainder theorem.

For the given simultaneous congruences, we have

$$M = 5 \times 6 \times 7 = 210, \quad M_1 = 6 \times 7 = 42, \quad M_2 = 5 \times 7 = 35 \quad \text{and} \quad M_3 = 5 \times 6 = 30.$$

Therefore, we consider the following congruences in one variable.

$$42x \equiv 1 \pmod{5} \quad \text{(iv)}$$

$$35x \equiv 1 \pmod{6} \quad \text{(v)}$$

$$30x \equiv 1 \pmod{7} \quad \text{(vi)}$$

If  $x_1, x_2, x_3$  are solutions to (iv), (v) and (vi) respectively, then, by Chinese remainder theorem, the solution to the given problem is  $x$ , where

$$x = 1 M_1 x_1 + 2 M_2 x_2 + 3 M_3 x_3, \text{ congruent modulo } M. \quad \text{(vii)}$$

To compute  $x_1, x_2, x_3$ , we first simplify the congruences (iv), (v), (vi).

From (iv), we have

$$1 \equiv 42x \pmod{5} = 2x \pmod{5} \quad [\text{Since } 42 = 40 + 2 \text{ and } 5 \mid 40]$$

Multiplying by 3, we get

$$3 \equiv 6x \pmod{5} \equiv x \pmod{5} \quad [\text{Setting } 6 = 5 + 1]$$

Therefore, (iv) is equivalent to

$$x \equiv 3 \pmod{5} \quad \text{(viii)}$$

$\therefore x_1 \equiv 3 \pmod{5}$

To compute  $x_2$ , consider (v). We have

$$1 \equiv 35x \pmod{6} = (36x - x) \pmod{6}$$

$$\therefore 1 \equiv -x \pmod{6}$$

$$\therefore -x \equiv 1 \pmod{6}.$$

Multiplying by -1, we get

$$x \equiv -1 \pmod{6} \equiv 5 \pmod{6}$$

Since, this is equivalent to (v), we have

$$x_2 \equiv 5 \pmod{6} \quad \text{(ix)}$$

To compute  $x_3$ , consider (vi). We have

$$1 \equiv 30x \pmod{7} = (28x + 2x) \pmod{7}$$

$$= 2x \pmod{7} \quad [\text{Since } 28 \mid 28]$$

Multiplying both sides by 4, we get

$$4 \equiv 8x \pmod{7} = (7x + x) \pmod{7}$$

$$= x \pmod{7} \quad [\text{Since } 7 \mid 7x]$$

$$\therefore x \equiv 4 \pmod{7}.$$

Since, this is equivalent to (vi), we have

$$x_3 = 4 \pmod{7}$$

Substituting the values of  $x_1, x_2, x_3$  from (vii), (ix), (x) and those of  $M_1, M_2, M_3$  in (vii), we get

$$x = 1 \times 42 \times 3 + 2 \times 35 \times 5 + 3 \times 30 \times 4$$

$= 836$  modulo  $M = 210$ .

To simplify  $x$  (modulo 210), consider

$$\begin{aligned} x &= 836 \pmod{210} = (630 + 206) \pmod{210} \\ &= 206 \pmod{210} \end{aligned} \quad [\text{Since } 210 \mid 630]$$

#### Method 2, by iteration

Since  $x \equiv 1 \pmod{5}$ , there exist an integer  $t$ , such that

$$x = 5t + 1$$

Substituting this value of  $x$  in (ii), we get

$$5t + 1 \equiv 2 \pmod{6} \quad (\text{ii})$$

$$\text{i.e., } 2 \equiv (5t + 1) \pmod{6}$$

$$\therefore 2 \equiv (6t - t + 1) \pmod{6}$$

$$\text{or } 2 \equiv (-t + 1) \pmod{6}$$

Subtracting 1 from both sides, we get

$$1 \equiv -t \pmod{6}$$

Multiplying both sides by -1, we have

$$-1 \equiv t \pmod{6}$$

$$\text{or } t \equiv (-1) \pmod{6}$$

But  $-1 \pmod{6} = 5 \pmod{6}$ . Therefore, we have

$$t \equiv 5 \pmod{6}$$

Therefore, there exist an integer  $u$ , such that  $t = 6u + 5$ . From (xi), therefore,

$$x = 5(6u + 5) + 1 = 30u + 26 \quad (\text{xii})$$

Substituting this value of  $x$  in (iii), we get

$$30u + 26 \equiv 3 \pmod{7}$$

$$\therefore 3 \equiv (30u + 26) \pmod{7}$$

$$\text{i.e., } 3 \equiv (2u + 5) \pmod{7} \quad [\text{Since, } 30u + 26 = 7(4u + 3) + (2u + 5)]$$

Multiplying both sides by 4, we have

$$12 \equiv (8u + 20) \pmod{7}$$

$$\therefore 12 \equiv (u - 1) \pmod{7} \quad [\text{Since, } 8u + 20 = 7(u + 3) + (u - 1)]$$

Subtracting 6, from both sides, we get

$$6 \equiv (u - 7) \pmod{7}$$

$$\text{i.e., } 6 \equiv u \pmod{7} \text{ or } u \equiv 6 \pmod{7}$$

Therefore, there exists an integer  $v$ , such that

$$u = 7v + 6$$

Now, we substitute in reverse order to recover  $x$ .

Starting from (xii), we get

$$x = 30u + 26 = 30(7v + 6) + 26 = 210v + 206.$$

This in other words,  $x = 206 \pmod{210}$ .

Example 3 : Find a solution to the simultaneous congruences :

$$x \equiv 2 \pmod{11}$$

$$x \equiv 3 \pmod{12}$$

$$x \equiv 4 \pmod{13}$$

$$x \equiv 5 \pmod{17}$$

$$x \equiv 6 \pmod{19}$$

$$\text{Sol. : Here, } M = 11 \times 12 \times 13 \times 17 \times 19 = 554268$$

$$M_1 = 50388, M_2 = 46189, M_3 = 42636, M_4 = 32604, M_5 = 29172$$

$$m_1 = 11, m_2 = 12, m_3 = 13, m_4 = 17, m_5 = 19$$

$$a_1 = 2, a_2 = 3, a_3 = 4, a_4 = 5, a_5 = 6.$$

$$\text{Solution is } x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 + a_4 M_4 x_4 + a_5 M_5 x_5 \quad (\text{i})$$

where,  $x_i$  is a solution of  $M_i x \equiv 1 \pmod{m_i}$ ,  $i = 1, \dots, 5$ .

We find that  $M_1 = 50388 = 4580 \times 11 + 8$

Therefore,  $M_1 x \equiv 1 \pmod{11}$  implies  $1 \equiv M_1 x \equiv 8x \pmod{11}$

$$4 \equiv -x \pmod{11} \quad [\text{Since } 32 = (3 \times 11 - 1)]$$

Hence,  $x \equiv -4 \equiv 7 \pmod{11}$

Hence,  $x_1 \equiv 7 \pmod{11}$

Therefore,  $x_1 = 7$

$$M_2 = 46189 = 3849 \times 12 + 1$$

Therefore,  $M_2 x \equiv 1 \pmod{12}$  leads to  $1 \equiv x \pmod{12}$

$$x_2 \equiv 1 \pmod{12}$$

$$M_3 = 42636 = 3279 \times 13 + 9$$

Therefore,  $M_3 x \equiv 1 \pmod{13}$  leads to  $1 \equiv 9x \pmod{13}$ .

Multiplying by 3, we have  $3 \equiv 27x \equiv x \pmod{13}$ .

$$x_3 \equiv 3 \pmod{13}$$

$$M_4 = 32604 = 1917 \times 17 + 15$$

Therefore,  $M_4 x \equiv 1 \pmod{17}$  leads to  $1 \equiv 15x \pmod{17}$ .

Multiplying by 8, we have  $8 \equiv 120x \equiv x \pmod{17}$

$$[\text{Since } 120 = 7 \times 17 + 1]$$

$$x_4 \equiv 8 \pmod{17}$$

$$M_5 = 29172 = 1535 \times 19 + 7$$

Therefore,  $M_5 x \equiv 1 \pmod{19}$  leads to  $1 \equiv 7x \pmod{19}$ .

Multiplying by 8, we have  $8 \equiv 56x \equiv -x \pmod{19}$

$$[\text{Since } 56 = 3 \times 19 - 1]$$

$$x_5 \equiv 8 \pmod{19}$$

$$x_6 \equiv -8 \equiv 11 \pmod{19}$$

$$x_6 \equiv 11 \pmod{19} \quad (\text{vi})$$

Substituting the values of  $a_i, M_i$  for  $i = 1, 2, 3, 4, 5$  and those of  $x_i$  from (ii) to (vi) in (i), we get

$$\begin{aligned} x &= 2 \times 50388 \times 7 + 3 \times 46189 \times 1 + 4 \times 42636 \times 3 \\ &\quad + 5 \times 32604 \times 8 + 6 \times 29172 \times 11 \end{aligned}$$

$$= 4585143 \pmod{M} = 554268$$

On simplification,  $x = 150999 \pmod{554268}$ .

**Example 4 :** Find three consecutive integers having cubes of, respectively, three consecutive primes as factors.

**Sol. :** Let  $a$ ,  $a+1$  and  $a+2$  be the three integers and we choose 2, 3, 5 as the three consecutive prime. [A reason for choosing 2, 3, 5 is that they are the smallest three consecutive primes.] We are given that

$$\begin{aligned} a &= 0 \pmod{8} \\ a &= -1 \pmod{27} \\ \text{and } a &= -2 \pmod{125}. \end{aligned}$$

We find  $a$  using Chinese remainder theorem.

Here,  $M = 8 \times 27 \times 125 = 27000$ ,  $M_1 = 3375$ ,  $M_2 = 1000$ ,  $M_3 = 216$ .

Then,  $a = 0 \times M_1 x_1 + (-1) \times (1000) x_2 + (-2) \times 216 x_3$

where  $x_1, x_2, x_3$  are, respectively, solutions of

$$M_1 x \equiv 1 \pmod{8}, M_2 x \equiv 1 \pmod{27} \text{ and } M_3 x \equiv 1 \pmod{125}.$$

Since the coefficient of  $M_1 x_1$  is 0, we need not compute  $x_1$ .

To compute  $x_2$ , consider

$$1 = 1000x \equiv (37 \times 27 + 1)x \pmod{27} \equiv x \pmod{27}$$

Hence,  $x_2 = 1$ .

To compute  $x_3$ , consider  $1 \equiv 216x \pmod{125}$ . Since  $216 = 2 \times 125 - 34$ , we get

$$1 \equiv -34x \pmod{125}.$$

Multiplying by 4, we have

$$4 \equiv -136x \pmod{125}$$

Hence,  $4 \equiv -11x \pmod{125}$

$$\therefore 44 \equiv -121x \pmod{125}$$

i.e.,  $44 \equiv 4x \pmod{125}$ .

Since  $(4, 125) = 1$ , we cancel 4 from both sides to get

$$11 \equiv x \pmod{125}$$

$$\therefore x_3 = 11$$

Substituting these values of  $x_2$  and  $x_3$  in (i), we get

$$a = -1000 - 2 \times 216 \times 11 = -5752 \pmod{27000}$$

We may obtain a positive integer  $27000 - 5752 = 21248$ .

Thus, the three consecutive integers are 21248, 21249, 21250.

**Example 5 :** A gang of 17 thieves stole a sack of gold biscuits. When they tried to divide the booty into equal parts three biscuits remained. There was a fight among themselves to get those extra biscuits in which one thief was killed. They again tried to divide the wealth into equal parts in which 10 biscuits remained. Again a thief was killed in the ensuing fight. The wealth was then redistributed among the survivors. This time they were successful in making equal distribution with no extra biscuit. How many biscuits were there in the sack?

**Sol. :** Suppose there were  $x$  biscuits in the sack. While three remained after equal distribution in some heap, we get the congruence

$$x \equiv 3 \pmod{17}$$

Similarly, we get  $x \equiv 10 \pmod{16}$

and  $x \equiv 0 \pmod{15}$

Using the Chinese remainder theorem, we find in this case

$$M = 17 \times 16 \times 15 = 4080, \quad M_1 = 240, \quad M_2 = 255, \quad M_3 = 272 \quad \dots \dots \dots \text{(i)}$$

The total number of biscuits are

$$x \equiv 3 M_1 x_1 + 10 M_2 x_2 + 0 M_3 x_3 \pmod{4080} \quad \dots \dots \dots \text{(ii)}$$

where  $x_1, x_2, x_3$  are solutions of the congruences  $M_1 x \equiv 1 \pmod{17}$ ,  $M_2 x \equiv 1 \pmod{16}$ ,  $M_3 x \equiv 1 \pmod{15}$ . We need not solve the last congruence as the coefficient of  $M_3 x_3$  is 0.

To find  $x_1$  we observe that

$$1 \equiv 240x \pmod{17}$$

$$\therefore 1 \equiv 2x \pmod{17}$$

On multiplication by 9,

$$9 \equiv 18x \equiv x \pmod{17}$$

$$x_1 \equiv 9 \pmod{17} \quad \dots \dots \dots \text{(iii)}$$

To find  $x_2$  we observe that

$$1 \equiv 255x \pmod{16}$$

$$\therefore 1 \equiv 15x \pmod{16}$$

$$1 \equiv -x \pmod{16} \quad \text{and hence we have}$$

$$x_2 \equiv -1 \equiv 15 \pmod{16} \quad \dots \dots \dots \text{(iv)}$$

Substituting the values of  $M_1, M_2$  and  $x_1, x_2$  in (ii), we get

$$x = 3 \times 240 \times 9 + 10 \times 255 \times 15 = 44730 \pmod{4080}$$

$$x = 44730 \equiv 3930 \pmod{4080}$$

Hence, the minimum number of biscuits in the sack is 3930 (modulo 4080).

### EXERCISE - VI

1. Solve the simultaneous congruences :

- |                           |                           |
|---------------------------|---------------------------|
| (a) $x \equiv 1 \pmod{2}$ | (b) $x \equiv 4 \pmod{4}$ |
| $x \equiv 2 \pmod{3}$     | $x \equiv 5 \pmod{5}$     |
| $x \equiv 3 \pmod{5}$     | $x \equiv 8 \pmod{7}$     |
| $x \equiv 4 \pmod{7}$     | $x \equiv 2 \pmod{9}$     |

[ Ans. : (a)  $x \equiv 53 \pmod{210}$ , (b)  $x \equiv 1100 \pmod{1260}$  ]

(Hint : Calculations reduces, if you note that equivalent problem is

$$x \equiv 0 \pmod{4}, \quad x \equiv 0 \pmod{5}, \quad x \equiv 1 \pmod{7}, \quad x \equiv 2 \pmod{9}.)$$

2. Find a positive integer which leaves the remainder 2, if divided by 3, the remainder 3, if divided by 5, the remainder 2, if divided by 7. [ Ans. : 23 modulo 105 ]

3. There are some eggs in a bucket. If they are removed from it picking 2 at a time one remains in the basket, if they are removed three at a time, two remains in the bucket, if they are removed 5 at a time, 4 remains. No egg remains if we remove them in a group of 7. What is the smallest number of eggs in the bucket. [ Ans. : 119 ]

4. Solve the following system of simultaneous congruences :  
 $x \equiv 3 \pmod{4}$   
 $x \equiv 4 \pmod{5}$   
 $x \equiv 5 \pmod{7}$  [Ans. :  $x \equiv 19 \pmod{140}$ ]
5. Find the smallest integer  $a > 2$ , such that  $2 \mid a$ ,  $3 \mid a+1$  and  $5 \mid a+3$ . [Ans. : 32]
6. Find three consecutive integers each divisible by a square of integers.  
(Hint : Find  $a$ ,  $a+1$ ,  $a+2$  divisible by 4, 9, 25.) [Ans. : 54]
7. Solve the following :  
(a)  $x \equiv 11 \pmod{20}$  (b)  $x \equiv 1 \pmod{9}$   
 $x \equiv 26 \pmod{45}$   $x \equiv 2 \pmod{10}$   
 $x \equiv 4 \pmod{12}$   $x \equiv 7 \pmod{15}$   
(Hint : Use iteration.) [Ans. : (a)  $x \equiv 71 \pmod{180}$ , (b)  $x \equiv -8 \pmod{180}$ ]



## Solvability of Quadratic Congruences

### 1. Introduction

One of the most beautiful results in the number theory is Quadratic Reciprocity Law. Almost every eminent mathematician of nineteenth century has worked on it. Roughly speaking, the law is related to the solvability of the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

where  $a, b, c$  are integers,  $p \neq 2$  is a prime number and  $p \nmid a$ . It is obvious that  $a \neq 0$ . This problem can, very easily, be reduced to the simple expression  $x^2 \equiv d \pmod{p}$ . But this reduction process, we will postpone for discussion at the end of this chapter.

In the previous chapter, we discuss the solvability of the linear congruence

$$ax \equiv b \pmod{m}$$

In this chapter, we discuss the solvability of the quadratic congruence

$$x^2 \equiv a \pmod{p}, \quad (a, p) = 1, \quad p \neq 2.$$

The condition  $p \neq 2$ , is imposed to avoid discussion on trivialities. For, if  $p = 2$ , then  $x^2 \equiv 0 \pmod{p}$ . If  $a$  is even and  $x^2 \equiv 1 \pmod{p}$  if  $a$  is odd. In both the cases, solutions are obvious and trivial.

We are, broadly, interested in the following problems.

1. Given a prime integer  $p$ , what are the integers  $a$  which are congruent to a perfect square modulo  $p$ ?
2. Given an integer  $a$ , what are the prime integers  $p$ , for which  $a$  is congruent to a perfect square modulo  $p$ ?
3. What are the conditions under which the problem  $x^2 \equiv a \pmod{p}$  has a solution, even though we may not know the actual solution?

Obviously, a passage to the first two questions passes through the third. So we start from the discussion on the third question.

### 2. Quadratic Residue

**Definition :** Let  $m$  be a positive integer and  $a$  be an integer relatively prime to  $m$ . The integer  $a$  is called a **quadratic residue** of  $m$ , if the congruence  $x^2 \equiv a \pmod{m}$  has a solution. If it does not have a solution, then  $a$  is called a **quadratic non-residue** of  $m$ .

For example,  $4^2 \equiv 7 \pmod{9}$ . Hence,  $x^2 \equiv 7 \pmod{9}$  has a solution  $x = 4$ . Hence, 7 is a quadratic residue of 9. It can be proved that 2 is a non-residue of 3.

Consider a quadratic congruence  $x^2 \equiv a \pmod{m}$ . If  $a$  is a quadratic residue of  $m$ , then we have an integer  $x = x_0$ , such that  $x_0^2 \equiv a \pmod{m}$ . If  $a \equiv b \pmod{m}$ , then by transitivity  $x_0^2 \equiv b \pmod{m}$ . Therefore, if  $a$  is a quadratic residue of  $m$ , then all integers congruent to  $a$  modulo  $m$  are also quadratic residues of  $m$ .

Given  $m > 1$ , we know that  $0, 1, 2, \dots, m-1$  form a complete system of residues. We avoid the trivial case of 0. In order to find quadratic residues of  $m$ , therefore, we need to test only  $m-1$  cases namely  $1, 2, \dots, m-1$ .

We however, restrict our discussion when  $m$  is a prime number  $p \neq 2$ .

**Example 1 :**

- (a) For  $p = 3$ , we need to consider only  $a = 1$  and  $a = 2$ , clearly  $1^2 \equiv 1 \pmod{3}$  and  $2^2 \equiv 1 \pmod{3}$ .

Thus, 1 is the only quadratic residue of 3 and 2 is a non-residue of 3.

- (b) For  $p = 5$ , we need to consider  $a = 1, 2, 3, 4$ .

Clearly  $1^2 \equiv 1 \pmod{5}$ ,  $2^2 \equiv 4 \pmod{5}$ ,  $3^2 \equiv 9 \pmod{5} \equiv 4 \pmod{5}$ ,

$$4^2 \equiv 16 \pmod{5} \equiv 1 \pmod{5}.$$

Thus, 1 and 4 are quadratic residues of 5 and others namely 2 and 3 are non-residues.

- (c) For  $p = 7$ , we need to consider  $a = 1, 2, 3, 4, 5, 6$ .

$$1^2 \equiv 1 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 3^2 \equiv 9 \equiv 2 \pmod{7},$$

$$4^2 \equiv 8 \equiv 1 \pmod{7}, \quad 5^2 \equiv 25 \equiv 4 \pmod{7}, \quad 6^2 \equiv 36 \equiv 1 \pmod{7}.$$

Thus, 1, 2 and 4 are quadratic residues and 3, 5, 6 are non-residues.

- (d) For  $p = 11$ , we need to consider  $1, 2, \dots, 10$ .

$$1^2 \equiv 1 \pmod{11}, \quad 10^2 \equiv 100 \equiv (9 \times 11 + 1) \equiv 1 \pmod{11},$$

$$2^2 \equiv 4 \pmod{11}, \quad 9^2 \equiv 81 \equiv (7 \times 11 + 4) \equiv 4 \pmod{11},$$

$$3^2 \equiv 9 \pmod{11}, \quad 8^2 \equiv 64 \equiv (5 \times 11 + 9) \equiv 9 \pmod{11},$$

$$4^2 \equiv 16 \equiv 5 \pmod{11}, \quad 7^2 \equiv 49 \equiv (4 \times 11 + 5) \equiv 5 \pmod{11},$$

$$5^2 \equiv 25 \equiv 3 \pmod{11}, \quad 6^2 \equiv 36 \equiv (3 \times 11 + 3) \equiv 3 \pmod{11}.$$

Thus, 1, 3, 4, 5 and 9 are quadratic residues of 11 and consequently, 2, 6, 7, 8, 10 are non-residues.

- (e) As a final example, consider  $p = 13$ . We need to consider  $a = 1, 2, \dots, 12$ .

$$1^2 \equiv 1 \pmod{13}, \quad 12^2 \equiv 144 \equiv (11 \times 13 + 1) \equiv 1 \pmod{13},$$

$$2^2 \equiv 4 \pmod{13}, \quad 11^2 \equiv 121 \equiv (9 \times 13 + 4) \equiv 4 \pmod{13},$$

$$3^2 \equiv 9 \pmod{13}, \quad 10^2 \equiv 100 \equiv (7 \times 13 + 9) \equiv 9 \pmod{13},$$

$$4^2 \equiv 16 \equiv 3 \pmod{13}, \quad 9^2 \equiv 81 \equiv (6 \times 13 + 3) \equiv 3 \pmod{13},$$

$$5^2 \equiv 25 \equiv 12 \pmod{13}, \quad 8^2 \equiv 64 \equiv (4 \times 13 + 12) \equiv 12 \pmod{13},$$

$$6^2 \equiv 36 \equiv 10 \pmod{13}, \quad 7^2 \equiv 49 \equiv (3 \times 13 + 10) \equiv 10 \pmod{13}.$$

Thus, 1, 3, 4, 9, 10, 12 are quadratic residues and others 2, 5, 6, 7, 8, 11 are non-residues of 13.

**Note ...**

In all the above illustrations, for  $p = 3, 5, 7, 11$  and 13, there were exactly  $(p-1)/2 = 1, 2, 3, 5$  and 6 quadratic residues and equal number of non-residues of  $p$  among  $1, 2, \dots, p-1$ . This is no accident. In fact, we shall prove it in Theorem 2, below.

**Theorem 1 :** If  $p$  is an odd prime and  $p \nmid a$ , then the quadratic congruence  $x^2 \equiv a \pmod{p}$  has precisely two incongruent solutions modulo  $p$ , or no solution at all.

**Proof :** It is obvious that if  $x_0^2 \equiv a \pmod{p}$ , then  $(-x_0)^2 \equiv a \pmod{p}$ . Thus, if  $x_0$  is a solution, then  $-x_0$  is also a solution.

We claim that  $x_0 \not\equiv (-x_0) \pmod{p}$ .

If  $x_0 \equiv -x_0 \pmod{p}$ , then, clearly,  $p \mid 2x_0$ . As  $p \nmid 2$ , we have that  $p \mid x_0$ . But that is impossible. For if  $p \mid x_0$ , then  $p \mid x_0^2$ . Therefore, we have that  $p \mid a$ , which is a contradiction.

The proof is complete, if we show that any other solution to  $x^2 \equiv a \pmod{p}$  is either congruent to  $x_0$  or to  $-x_0$ .

Let  $x_1$  be any other solution. Then,  $x_1^2 \equiv a \pmod{p}$  and therefore,  $x_1^2 \equiv x_0^2 \pmod{p}$ . But then  $p \mid (x_1^2 - x_0^2) = (x_1 - x_0)(x_1 + x_0)$ . Therefore,  $p \mid (x_1 - x_0)$  or  $p \mid (x_1 + x_0)$ . If  $p \mid (x_1 - x_0)$ , then,  $x_1 \equiv x_0 \pmod{p}$ . If  $p \mid (x_1 + x_0)$ , then  $x_1 \equiv -x_0 \pmod{p}$ . Hence, the theorem.

**Note ...**

The above lemma shows that quadratic residues occur in pairs,  $x_0$  and  $-x_0$ . Since  $p-x_0 \equiv -x_0 \pmod{p}$ , we can consider the pair to be  $x_0$  and  $p-x_0$  also, so that both  $x_0$  and  $p-x_0$  lie between 1 and  $p-1$ .

The following theorem counts the number of residues and non-residues (modulo  $p$ ) for a given odd prime  $p$ .

**Theorem 2 :** Let  $p$  be an odd prime. Then there exist exactly  $(p-1)/2$  quadratic residues of  $p$  among  $1, 2, \dots, p-1$ . The remaining  $(p-1)/2$  integers are non-residues of  $p$ .

**Proof :** Consider  $x^2 \equiv a \pmod{p}$ , where  $a$  takes values  $1, 2, \dots, p-1$ . We are to show that the congruence has solutions only for  $(p-1)/2$  integers among them. For the remaining  $(p-1)/2$  integer, it has no solution.

Consider the squares  $1^2, 2^2, \dots, (p-1)^2$ . Let  $r_1, r_2, \dots, r_{p-1}$  be the remainders of these squares on division by  $p$ . We claim that these  $r_k$  are not distinct.

Let  $k^2 = q_k p + r_k, \quad 1 \leq r_k \leq p-1, \quad k = 1, 2, \dots, p-1$ .

Then,  $k^2 \equiv r_k \pmod{p}$  i.e.,  $r_k$  is a quadratic residue of  $p$ .

However, as  $(p-k)^2 = (p-2k)p + k^2$ , we have  $(p-k)^2 \equiv k^2 \pmod{p}$ .

But,  $(p-k)^2 \equiv q_{p-k}p + r_{p-k}, \quad 1 \leq r_{p-k} \leq p-1$ .

Therefore,  $r_{p-k} \equiv (p-k)^2 \equiv k^2 \equiv r_k \pmod{p}$ .

Hence,  $p \mid r_{p-k} - r_k$ . Since, both  $r_k$  and  $r_{p-k}$  lie between 1 and  $p-1$ ,  $p$  can divide  $r_{p-k} - r_k$  only when  $r_{p-k} = r_k$ . Thus,  $r_1, \dots, r_{p-1}$  occur in pairs. Since,  $x^2 \equiv a \pmod{p}$  has either two solutions or no solution, by Theorem 1, there will be exactly  $(p-1)/2$  pairs.

Hence, there will be exactly  $(p-1)/2$  quadratic residues of  $p$  among  $1, 2, \dots, p-1$ .

**Corollary :** There are exactly  $(p-1)/2$  incongruent quadratic residues of  $p$ .

**Proof :** This follows from the fact that  $1, 2, \dots, p-1$  are incongruent.

**Example :** Prove that quadratic residues of  $p \neq 2$  are congruent (modulo  $p$ ) to  $(p-1)/2$  integers  $1^2, 2^2, \dots, ((p-1)/2)^2$ . (Observe the pattern on the page 5-2, Example 1 (d), (e))

**Sol :** If  $a$  is any integer and  $a$  is congruent modulo  $p$  to any one of  $1^2, 2^2, \dots, ((p-1)/2)^2$ , then, by definition  $a$  is a quadratic residue of  $p$ . We know by the above theorem, that there are exactly  $(p-1)/2$  quadratic residues of  $p \neq 2$ , which are incongruent modulo  $p$ . Hence, to prove the claim in the question, it is enough to show that  $1^2, 2^2, \dots, ((p-1)/2)^2$  are mutually incongruent.

Let if possible,  $1 \leq h \leq \frac{p-1}{2}$ ,  $1 \leq k \leq \frac{p-1}{2}$ ,  $h < k$  be two integers such that  $h^2 \equiv k^2 \pmod{p}$ . This means  $p \mid h^2 - k^2 = (h-k)(h+k)$ . Since,  $p$  is prime,  $p \mid h-k$  or  $p \mid h+k$ . Since,  $1 \leq h < p$ ,  $1 \leq k < p$ , we get  $1 \leq k-h < p$ . Hence,  $p \nmid k-h$ . Since,  $1 \leq h \leq \frac{p-1}{2}$ ,  $1 \leq k \leq \frac{p-1}{2}$ ,  $h < k$ , we have  $1 \leq h+k < p$  and hence  $p \nmid h+k$ . Hence,  $p \nmid h^2 - k^2$  and thus,  $h^2 \not\equiv k^2 \pmod{p}$ . Hence, the claim.

### 3. Legendre Symbol

The special notation, introduced by the French mathematician Andrien Marie Legendre, described in the following definition is specially useful in determining the existence of quadratic residues of prime  $p \neq 2$ .

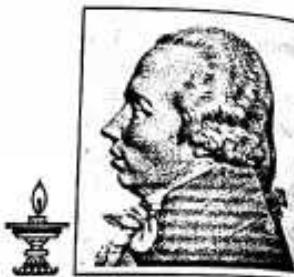
**Definition :** Let  $p$  be an odd prime and  $a$  be an integer with  $(a, p) = 1$ . The Legendre symbol  $(a/p)$  is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p \\ -1, & \text{if } a \text{ is a quadratic non-residue of } p \end{cases}$$

#### Adrien-Marie Legendre (1752 - 1833)

Legendre was one of the great French Mathematicians. He got his Ph.D. in 1770. He was a member of French academy of sciences. He was made an officer Légion d'Honneur. Most of his work was brought to perfection by others like Galois, Abel, Gauss. He made significant contributions in the fields of roots of polynomials, elliptic functions, elliptic integrals, curve fitting, number theory, etc. He is known for Legendre's differential equation, Legendre's polynomials and Legendre's transformations. He is best known as the author of "Éléments de géométrie" which was a leading text for over hundred years.

His name is among the 72 names inscribed on the Eiffel Tower.



**Example 1 :** Refer to Example 1 (e), § 2, page 5-2.

1, 3, 4, 9, 10, 12 are quadratic residues of 13. Hence, their Legendre symbols have value 1.

$$\text{i.e., } \left(\frac{1}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{12}{13}\right) = 1.$$

On the other hand 2, 5, 6, 7, 8, 11 are quadratic non-residues. Hence, their Legendre symbols have value -1.

$$\text{i.e., } \left(\frac{2}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{11}{13}\right) = -1.$$

Euler has given the following criterion for determining the Legendre Symbol.

**Euler's Criterion :** Let  $p$  be an odd prime,  $a$  an integer and  $p \nmid a$ . Then

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}$$

Thus, given integer  $a$ , and a prime  $p \neq 2$ ,  $p \nmid a$ .

If  $a^{(p-1)/2} \pmod{p} = 1$ ,  $a$  is a quadratic residue.  
If  $a^{(p-1)/2} \pmod{p} = -1$ ,  $a$  is a quadratic non-residue.

**Example 2 :** Test if 12, 8, 11 are quadratic residues of 13.

**Sol :** Here  $p = 13$ . Hence,  $\frac{p-1}{2} = \frac{12}{2} = 6$ .

(i) For  $a = 12$ , the Euler Criterion gives

$$\left(\frac{12}{13}\right) = 12^6 \pmod{13}$$

$$12 \equiv (-1) \pmod{13},$$

$$12^6 \equiv (-1)^6 \equiv 1 \pmod{13}$$

$$\therefore \left(\frac{12}{13}\right) = 1, \text{ i.e., } 12 \text{ is a quadratic residue modulo 13.}$$

(ii) For  $a = 8$ ,  $\left(\frac{8}{13}\right) = 8^6 \pmod{13}$

$$8^2 \equiv 64 \equiv 4 \times 13 + 12 \equiv 12 \equiv -1 \pmod{13}$$

$$8^6 \equiv (8^2)^3 \equiv (-1)^3 \equiv -1 \pmod{13}$$

$$\text{Hence, } \left(\frac{8}{13}\right) = -1, \text{ i.e., } 8 \text{ is not a quadratic residue of 13.}$$

(iii) For  $a = 11$ ,  $\left(\frac{11}{13}\right) = 11^6 \pmod{13}$

$$11^2 \equiv 121 \equiv 9 \times 13 + 4 \equiv 4 \pmod{13}$$

$$11^6 \equiv (11^2)^3 \equiv (4)^3 \equiv 64 \equiv 5 \times 13 - 1 \equiv -1 \pmod{13}$$

$$\text{Thus, } \left(\frac{11}{13}\right) = -1, \text{ i.e., } 11 \text{ is not a quadratic residue of 13.}$$

### 4. Properties of Legendre Symbols

**Theorem 3 :** Let  $p$  be an odd prime,  $a, b$  be integer and  $p \nmid a, p \nmid b$ . Then the following results hold:

1. If  $a \equiv b \pmod{p}$ , then  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2.  $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
3.  $\left(\frac{a^2}{p}\right) = 1$ , in particular  $\left(\frac{1}{p}\right) = 1$ .

**Proof :** (1) Let  $a \equiv b \pmod{p}$ , if  $x_0^2 \equiv a \pmod{p}$ , then by transitivity  $x_0^2 \equiv b \pmod{p}$ . Therefore,  $x_0$  is a solution of  $x^2 \equiv a \pmod{p}$  if and only if it is a solution of  $x^2 \equiv b \pmod{p}$ . In other words,  $a$  is a quadratic residue of  $p$  if and only if  $b$  is a quadratic residue of  $p$ . Hence,

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

(2) By Euler's criterion, we have

$$(i) \quad \left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p},$$

$$(ii) \quad \left(\frac{b}{p}\right) = b^{(p-1)/2} \pmod{p}, \quad \text{and}$$

$$(iii) \quad \left(\frac{ab}{p}\right) = (ab)^{(p-1)/2} \pmod{p}.$$

On multiplication of congruences in (i) and (ii), we have

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{(p-1)/2} \cdot b^{(p-1)/2} \pmod{p}$$

$$\therefore \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (ab)^{(p-1)/2} \pmod{p} \quad (\text{A})$$

By symmetry, (iii) gives  $(ab)^{(p-1)/2} = \left(\frac{ab}{p}\right) \pmod{p}$ .

Combining this with (A) and using transitivity, we get

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \pmod{p}$$

Recall that Legendre symbols  $\left(\frac{a}{p}\right)$ ,  $\left(\frac{b}{p}\right)$  and  $\left(\frac{ab}{p}\right)$  have value either 1 or -1. Therefore

$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right)$  will be either 0 or  $\pm 2$ . But  $p \nmid 2$ .

Therefore,  $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) \neq \pm 2$

Therefore,  $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) = 0 \quad \text{i.e.,} \quad \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ .

(3) Since  $\left(\frac{a}{p}\right) = \pm 1$ ,  $\left(\frac{a}{p}\right)^2 = 1$ . Therefore,  $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2 = 1$ .

The result (2) above has useful consequences.

- (i) If  $a$  and  $b$  are quadratic residues, then  $ab$  is a quadratic residue.
- (ii) If  $a$  and  $b$  are quadratic non-residues, then  $ab$  is a quadratic residue.
- (iii) If one of  $a, b$  is quadratic residue and the other non-residue, then  $ab$  is a quadratic non-residue modulo  $p$ .

(iv)  $\left(\frac{ab^{2n}}{p}\right) = \left(\frac{a}{p}\right)$  for any positive integer  $n$ .

**Example 1 :** Prove that

- (a) 1272 is a quadratic residue of 43.
- (b) 319 is a quadratic residue of 7.
- (c) 530 is a quadratic residue of 193.

Sol. : (a)  $1272 = 29 \times 43 + 25$ . Therefore,  $1272 \equiv 25 \pmod{43}$ .

Hence, by Theorem 3 (1),  $\left(\frac{1272}{43}\right) = \left(\frac{25}{43}\right)$ .

But  $25 = 5 \times 5$ . Hence, by above Theorem 3 (3),  $\left(\frac{25}{43}\right) = 1$ .

Therefore,  $\left(\frac{1272}{43}\right) = 1$ . Hence, the result.

(b)  $319 = 45 \times 7 + 4 = 45 \times 7 + 2^2$

Therefore,  $\left(\frac{319}{7}\right) = \left(\frac{4}{7}\right) = 1$  [By Theorem 3 (1) and (3)]

Hence, the result.

(c)  $530 = 2 \times 193 + 144$ .

Therefore,  $\left(\frac{530}{193}\right) = \left(\frac{144}{193}\right)$ .

But  $144 = 16 \times 9 = 4^2 \times 3^2$ .

Therefore,  $\left(\frac{530}{193}\right) = \left(\frac{4^2}{193}\right) \left(\frac{3^2}{193}\right) = 1 \times 1 = 1$ . Hence, the result.

**Example 2 :** Let  $a$  and  $b$  be integers not divisible by an odd prime  $p$ . Show that either one of  $a, b$  and  $ab$  or all the three are quadratic residues.

Sol. : Recall that  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ . Then, there are three mutually exclusive cases :

(1)  $\left(\frac{a}{p}\right) = 1 = \left(\frac{b}{p}\right)$ , (2)  $\left(\frac{a}{p}\right) = -1 = \left(\frac{b}{p}\right)$ , (3) Only one of  $\left(\frac{a}{p}\right)$  and  $\left(\frac{b}{p}\right)$  has value 1.

**Case 1 :** If  $\left(\frac{a}{p}\right) = 1 = \left(\frac{b}{p}\right)$ , then  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$ .

In this case, by the definition of Legendre symbol,  $a, b$  and  $ab$  are quadratic residues.

**Case 2 :** If  $\left(\frac{a}{p}\right) = -1 = \left(\frac{b}{p}\right)$ , then  $a$  and  $b$  are quadratic non-residues.

But then  $\left(\frac{ab}{p}\right) = (-1)^2 = 1$ .

Therefore,  $ab$  will be a quadratic residues.

**Case 3 :** If only one of  $\left(\frac{a}{p}\right)$  and  $\left(\frac{b}{p}\right)$  is equal to one (and the other equal to -1), then one of them will be quadratic residue and the other, whose value is (-1) will be quadratic non-residue.

But then their product  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$  will be equal to -1.

Hence,  $ab$  will be quadratic non-residue.

**Example 3 :** Let  $n = p_1^{2k_1+1} p_2^{2k_2+1} \dots p_m^{2k_m+1}$ , where  $p_1, p_2, \dots, p_m$  are distinct primes. Let  $q$  be an odd prime and  $q \nmid n$ .

Show that  $\left(\frac{n}{q}\right) = \left(\frac{p_1}{q}\right) \left(\frac{p_2}{q}\right) \dots \left(\frac{p_m}{q}\right)$ .

Sol. : Recall that if  $q \nmid a, q \nmid b$ , then  $\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right) \left(\frac{b}{q}\right)$ .

Applying this result repeatedly, we have

$$\left(\frac{n}{q}\right) = \left(\frac{p_1}{q}\right)^{2k_1+1} \left(\frac{p_2}{q}\right)^{2k_2+1} \dots \left(\frac{p_m}{q}\right)^{2k_m+1}$$

$$\text{Clearly, } \left(\frac{p_i}{q}\right)^{2k_i} = (\pm 1)^{k_i} = 1$$

and therefore,  $\left(\frac{p_i}{q}\right)^{2k_i+1} = \left(\frac{p_i}{q}\right)$  for  $i = 1, 2, \dots, m$ .

$$\therefore \left(\frac{n}{q}\right) = \left(\frac{p_1}{q}\right) \left(\frac{p_2}{q}\right) \dots \left(\frac{p_m}{q}\right)$$

**Example 4 :** If  $b$  is an integer not divisible by an odd prime  $p$ , then

$$\left(\frac{b}{p}\right) + \left(\frac{2b}{p}\right) + \dots + \left(\frac{(p-1)b}{p}\right) = 0.$$

Sol. : Since,  $\left(\frac{kb}{p}\right) = \left(\frac{k}{p}\right) \left(\frac{b}{p}\right)$  for  $k = 1, 2, \dots, p-1$ , we have that

$$\begin{aligned} \text{L.H.S. of the given equation} &= \left(\frac{b}{p}\right) \left(\frac{1}{p}\right) + \left(\frac{b}{p}\right) \left(\frac{2}{p}\right) + \dots + \left(\frac{b}{p}\right) \left(\frac{p-1}{p}\right) \\ &= \left(\frac{b}{p}\right) \left\{ \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \dots + \left(\frac{p-1}{p}\right) \right\} \end{aligned}$$

But exactly  $\frac{p-1}{2}$  of  $1, 2, \dots, p-1$  are quadratic residues and the remaining  $\frac{p-1}{2}$  are quadratic non-residues. Therefore, only half of  $\left(\frac{1}{p}\right), \dots, \left(\frac{p-1}{p}\right)$  have value 1 and the other have value -1.

Therefore, L.H.S. = 0.

**Theorem 4 :** If  $p$  is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv -1 \pmod{4} \end{cases}$$

**Proof : Case 1 :** Let  $p \equiv 1 \pmod{4}$ . Therefore, there exists an integer  $k$ , such that  $p = 4k+1$ . Therefore, Euler's Criterion gives

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{(4k+1-1)/2} = (-1)^{2k} = 1 \pmod{p}$$

Therefore,  $\left(\frac{-1}{p}\right) - 1 = k'p$  for some integer  $k'$ .

Since,  $\left(\frac{-1}{p}\right)$  is either 1 or -1,  $k'p = 0$  or -2.

But  $p \neq 2$ . Hence,  $k'p \neq -2$ . Therefore,  $k'p = 0$ . Hence,  $\left(\frac{-1}{p}\right) = 1$ .

**Case 2 :** Let  $p \equiv -1 \pmod{4}$ , i.e.,  $p \equiv 3 \pmod{4}$ .

Therefore, there exists an integer  $k$ , such that  $p = 4k+3$ .

Therefore, Euler's Criterion gives

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{(4k+3-1)/2} = (-1)^{2k+1} = (-1) \pmod{p}$$

Therefore,  $\left(\frac{-1}{p}\right) + 1 = k'p$  for some integer  $k'$ .

Again as in the previous case  $\left(\frac{-1}{p}\right) + 1$  is either 0 or 2. But as  $p \neq 2$ ,  $k'p \neq 2$ .

Hence,  $k'p = 0$ . Therefore,  $\left(\frac{-1}{p}\right) = -1$ .

**Note ...**

Note that  $p \equiv 1 \pmod{4}$  if and only if  $p = 4k+1$  for some integer  $k$ .

Also  $p \equiv -1 \pmod{4}$ , if and only if  $p = 4k+3$  or equivalently  $p = 4k-1$ . Therefore,

If $p = 4k+1$ , $\left(\frac{-1}{p}\right) = 1$ .	If $p = 4k+3$ , $\left(\frac{-1}{p}\right) = -1$ .	If $p = 4k-1$ , $\left(\frac{-1}{p}\right) = -1$
---	--	--

**Example 5 :** (a)  $\left(\frac{-1}{5}\right) = 1$ , for  $5 = 4+1$ ,  $\left(\frac{-1}{13}\right) = 1$ , for  $13 = 3 \times 4+1$ ,

$$\left(\frac{-1}{17}\right) = 1, \text{ for } 17 = 4 \times 4+1.$$

(b)  $\left(\frac{-1}{7}\right) = -1$ , for  $7 = 4+3$  [Also  $7 = 2 \times 4-1$ ]

$$\left(\frac{-1}{11}\right) = -1, \text{ for } 11 = 2 \times 4+3 \quad [\text{Also } 11 = 3 \times 4-1]$$

$$\left(\frac{-1}{19}\right) = -1, \text{ for } 19 = 4 \times 4+3 \quad [\text{Also } 19 = 5 \times 4-1]$$

**Example 6 :** Prove that if  $p$  is an odd prime  $p \nmid a$ , then

$\left(\frac{-a}{p}\right) = \left(\frac{a}{p}\right)$ , if $p = 4k+1$ ;	$\left(\frac{-a}{p}\right) = -\left(\frac{a}{p}\right)$ , if $p = 4k+3$
--	---

for any integer  $k$ .

**Sol. :** By Euler's Criterion, we have

$$\left(\frac{\pm a}{p}\right) = (\pm a)^{(p-1)/2} \pmod{p}$$

**Case 1:** Let  $p = 4k + 1$ . Then  $\frac{p-1}{2} = 2k$

$$\therefore \left(\frac{a}{p}\right) = a^{2k} \pmod{p} \quad \text{and} \quad \left(\frac{-a}{p}\right) = (-a)^{2k} = a^{2k} \pmod{p}$$

Combining the two congruences,

$$\left(\frac{a}{p}\right) = \left(\frac{-a}{p}\right) \pmod{p}. \quad \therefore p \mid \left(\frac{a}{p}\right) - \left(\frac{-a}{p}\right)$$

Since  $\left(\frac{a}{p}\right)$  and  $\left(\frac{-a}{p}\right)$  assume values 1 and -1 only,

$$\left(\frac{a}{p}\right) - \left(\frac{-a}{p}\right) = 0 \text{ or } 2 \text{ or } -2.$$

But  $p \neq \pm 2$ . Hence,  $\left(\frac{a}{p}\right) - \left(\frac{-a}{p}\right) = 0$ , i.e.,  $\left(\frac{a}{p}\right) = \left(\frac{-a}{p}\right)$ .

**Case 2:** Let  $p = 4k + 3$ . Then  $\frac{p-1}{2} = 2k + 1$ .

$$\therefore \left(\frac{a}{p}\right) = a^{2k+1} \pmod{p} \quad \text{and} \quad \left(\frac{-a}{p}\right) = (-a)^{2k+1} \pmod{p}$$

Combining the two congruences,

$$\left(\frac{a}{p}\right) = -\left(\frac{-a}{p}\right) \pmod{p}. \quad \therefore p \mid \left(\frac{a}{p}\right) + \left(\frac{-a}{p}\right)$$

Since  $\left(\frac{a}{p}\right) + \left(\frac{-a}{p}\right) = 0 \text{ or } \pm 2$  and  $p \neq \pm 2$ , we get  $\left(\frac{-a}{p}\right) = -\left(\frac{a}{p}\right)$ .

#### Note ...

A reader should note that in this problem and earlier,  $p = 4k + 1$  and  $p = 4k + 3$  cover all integers. Because, every integer is precisely one of the forms  $n = 4k$ ,  $n = 4k + 1$ ,  $n = 4k + 2$  and  $n = 4k + 3$ . Since,  $p$  is prime,  $p \neq 4k$ ,  $p \neq 4k + 2$ . So, either  $p = 4k + 1$  or  $p = 4k + 3$  holds.

Similar situation exists when we put similar restrictions on  $p$  in other theorems.

There is a very interesting corollary to Theorem 4.

**Corollary:** There are infinitely many primes of the form  $4k + 1$ ,  $k \geq 1$ .

**Proof:** We assume that the result is not true. Then there will be only finitely many such primes, say  $p_1, p_2, \dots, p_m$  where  $p_i = 4k_i + 1$  for some  $k_i \geq 1$ .

Consider the integer  $N = (2p_1 p_2 \dots p_m)^2 + 1$ .

Since  $N$  is odd,  $N = 4(p_1 p_2 \dots p_m)^2 + 1$ , and  $N$  is not in the list  $p_1, p_2, \dots, p_m$ .  $N$  cannot be a prime. Therefore, there exists a prime  $p \mid N$ . (Clearly,  $p \neq 2$ ).

Therefore,  $(2p_1 p_2 \dots p_m)^2 \equiv -1 \pmod{p}$ .

In other words -1 is a quadratic residue, and hence, in Legendre Symbol  $\left(\frac{-1}{p}\right) = 1$ . But this is possible only when  $p \equiv 1 \pmod{4}$ , i.e.,  $p = 4k + 1$  for some  $k > 0$ .

Therefore,  $p = p_i$  for some  $i = 1, 2, \dots, m$ .

Therefore,  $p \mid (2p_1 p_2 \dots p_m)^2$ .

But then,  $p \mid N - 1$ . Hence,  $-1 \equiv N \pmod{p}$ . But by choice  $p \nmid N$ . Hence,  $0 \equiv N \pmod{p}$ . This leads to absurd statement  $p \mid 1$ . Hence, the result holds.

The following Lemma due to Gauss gives one more criterion to test whether an integer  $a$  relatively prime to  $p$  is a quadratic residue of  $p$ .

#### 5. Gauss' Lemma

Let  $p$  be an odd prime,  $a$  an integer with  $(a, p) = 1$ . If  $s$  is the number of least positive residues modulo  $p$  of integers  $a, 2a, 3a, ((p-1)/2)a$  that are greater than  $p/2$ , then the Legendre symbol

$$\left(\frac{a}{p}\right) = (-1)^s$$

#### How to apply Gauss' Lemma

Given integers  $a, p$ ;  $p$  is an odd prime;  $(a, p) = 1$ .

(i) Compute  $\frac{p-1}{2}$ .

(ii) Compute  $a, 2a, 3a, \dots, \frac{(p-1)a}{2}$ .

(iii) Retain those which are less than  $p$  and divide others by  $p$ , so that the remainders are less than  $p$ . This way we have all integers lying between 1 and  $p-1$ .

(iv) Count all the numbers in (iii), which are greater than  $p/2$ .

(v) If  $s$  is the number obtained in the stage (iv),

$$\left(\frac{a}{p}\right) = (-1)^s$$

**Example 1:** Verify Gauss Theorem for  $p = 17$ ; (i)  $a = 4$ , (ii)  $a = 3$ .

Sol.: (i) 1. Here  $\frac{p-1}{2} = \frac{17-1}{2} = 8$ .

2. Consider 1, 2, 3, 4, 5, 6, 7, 8.

3. Multiplying by 4 : 4, 8, 12, 16, 20, 24, 28, 32.

4. The least positive residues modulo 17 are 4, 8, 12, 16,

$$3 = 20 \pmod{17}, \quad 7 = 24 \pmod{17}, \quad 11 = 28 \pmod{17}, \quad 15 = 32 \pmod{17}.$$

5. Numbers greater than  $17/2 = 8.5$  are 12, 16, 11, 15. They are 4 in number.

$$\therefore \left(\frac{4}{17}\right) = (-1)^4 = 1. \quad \text{i.e.,} \quad 4 \text{ is a quadratic residue modulo 17.}$$

In fact,  $15^2 = 4 \pmod{17}$ .

Note that by Euler's Criteria,  $4^8 \equiv 1 \pmod{17}$ .

And hence,  $\left(\frac{4}{17}\right) = 1$ . We already know  $\left(\frac{4}{17}\right) = \left(\frac{2}{17}\right)^2 = 1$ .

(ii) Here the first two steps are the same.

3. Multiplying by 3 : 3, 6, 9, 12, 15, 18, 21, 24.

4. The least positive residues modulo 17 are 3, 6, 9, 12, 15,

$$1 = 18 \pmod{17}, \quad 4 = 21 \pmod{17}, \quad 7 = 24 \pmod{17}.$$

5. The numbers greater than 8-5; 9, 12, 15. They are 3 in number.  
 $\therefore \left(\frac{3}{17}\right) = (-1)^3 = -1$

Therefore, 3 is a quadratic non-residue modulo 17.  
 Check that by Euler's Criterion, we get the same result.

Another useful criterion to determine  $(a/p)$  is given by the following theorem. The criterion is for  $(a/p)$ , when  $a = 2$ .

**Theorem 5:** If  $p$  is an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

This has an interesting corollary.

**Corollary:** Let  $p$  be an odd prime.

1. If  $p \equiv 1 \pmod{8}$  or  $p \equiv -1 \pmod{8}$ , i.e., if  $8 \mid p \pm 1$ , then  $\left(\frac{2}{p}\right) = 1$ .
2. If  $p \equiv 3 \pmod{8}$  or  $p \equiv -3 \pmod{8}$ , i.e., if  $8 \nmid p \pm 3$ , then  $\left(\frac{2}{p}\right) = -1$ .

We prove the corollary.

**Proof:** 1. Let  $p \equiv 1 \pmod{8}$ , i.e.,  $p = 8k + 1$  for some integer  $k$ . Then

$$(p^2 - 1) = (p-1)(p+1) = 8k(p+1).$$

If  $p \equiv -1 \pmod{8}$ , then  $p = 8k' - 1$  for some integer  $k'$ .

$$\therefore (p^2 - 1) = (p+1)(p-1) = 8k'(p-1).$$

Since  $p$  is odd,  $p+1$  and  $p-1$  are even and thus in either case  $(p^2 - 1) = 16K$  for some integer  $K$ . But then  $\frac{p^2 - 1}{8} = 2K$  and  $(-1)^{(p^2-1)/8} = (-1)^{2K} = 1$ . Rest follows.

2. If  $p \equiv 3 \pmod{8}$ , then  $p = 8k + 3$  for some integer  $k$ . Therefore,  $(p^2 - 1) = (8k+4)(8k+2) = 8(2k+1)(4k+1)$ .

$$\therefore \left(\frac{p^2 - 1}{8}\right) = (2k+1)(4k+1).$$

Thus,  $\left(\frac{p^2 - 1}{8}\right)$  is a product of odd numbers and hence is odd.

We leave it to readers to check, that  $\left(\frac{p^2 - 1}{8}\right)$  is odd when  $p \equiv -3 \pmod{8}$ .

Therefore, in either case  $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = -1$ .

**Illustration:** We observe that 8 divides 7+1, 17-1, 23+1, 31+1, 41-1, 47+1, 127+1

$$\therefore \left(\frac{2}{7}\right) = \left(\frac{2}{17}\right) = \left(\frac{2}{23}\right) = \left(\frac{2}{31}\right) = \left(\frac{2}{41}\right) = \left(\frac{2}{47}\right) = \left(\frac{2}{127}\right) = 1$$

Similarly, we observe that 8 divides 3-3, 5+3, 11-3, 13+3, 19-3, 29+3, 43-3, 163-3.

$$\therefore \left(\frac{2}{3}\right) = \left(\frac{2}{5}\right) = \left(\frac{2}{11}\right) = \left(\frac{2}{13}\right) = \left(\frac{2}{19}\right) = \left(\frac{2}{29}\right) = \left(\frac{2}{43}\right) = \left(\frac{2}{163}\right) = -1$$

**Example 2:** Show that, if  $p$  is an odd prime, then

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 3 \pmod{8} \\ -1, & \text{if } p \equiv -1 \text{ or } -3 \pmod{8} \end{cases}$$

Sol.: Note that  $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$  ..... (i)

By Euler's Criterion

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \pmod{p} \quad \dots \dots \dots \text{(ii)}$$

$$\text{On other hand, } \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \quad \dots \dots \dots \text{(iii)}$$

**Case 1:** If  $p \equiv 1 \pmod{8}$ , then  $p = 8k + 1$  for some integer  $k$ . Then  $\frac{p-1}{2} = 4k$ .

$$\therefore \left(\frac{-1}{p}\right) = (-1)^{4k} = 1 \pmod{p}$$

$$\text{Hence, } \left(\frac{-1}{p}\right) = 1. \quad \dots \dots \dots \text{(A)}$$

On the other hand,

$$\frac{p^2 - 1}{8} = \frac{(p-1)(p+1)}{8} = \frac{8k(8k+2)}{8} = 2k(4k+1)$$

$$\text{Hence, } \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{2k(4k+1)} = 1 \quad \dots \dots \dots \text{(B)}$$

Combining (A) and (B), we get, in view of (i)

$$\left(\frac{-2}{p}\right) = 1 \times 1 = 1$$

**Case 2:** If  $p \equiv 3 \pmod{8}$ , then  $p = 8k + 3$ , for some integer  $k$ . Then

$$\frac{p-1}{2} = \frac{8k+2}{2} = 4k+1$$

$$\therefore \left(\frac{-1}{p}\right) = (-1)^{4k+1} = -1 \pmod{p}$$

$$\text{Hence, } \left(\frac{-1}{p}\right) = -1 \quad \dots \dots \dots \text{(A')}$$

On the other hand,

$$\frac{p^2 - 1}{8} = \frac{(p-1)(p+1)}{8} = \frac{(8k+4)(8k+2)}{8} = (2k+1)(4k+1)$$

which is a product of odd integers and hence is an odd integer.

$$\therefore \left( \frac{2}{p} \right) = (-1)^{(2k+1)(4k+1)} = -1$$

Combining (A') and (B'), in the light of (i), we get

$$\left( \frac{-2}{p} \right) = (-1) \times (-1) = 1$$

**Case 3 :** If  $p \equiv -1 \pmod{8}$ , then  $p = 8k - 1$  for some integer  $k$ . Then as before a reader will find that  $\frac{p-1}{2} = 4k - 1$ , which is an odd integer and  $\frac{p^2-1}{8} = 2k(4k+1)$  which is an even integer.

$$\therefore \left( \frac{-1}{p} \right) = 1 \text{ and } \left( \frac{2}{p} \right) = 1$$

Hence, their product  $\left( \frac{-2}{p} \right) = -1$ .

**Case 4 :** If  $p \equiv -3 \pmod{8}$ , then  $p = 8k - 3$ , for some integer  $k$ .

Then  $\frac{p-1}{2} = \frac{8k-4}{2} = 2(2k-1)$  is an even integer and  $\frac{p^2-1}{8} = (2k-1)(4k-1)$  which is an odd number. But then  $\left( \frac{-1}{p} \right) = 1$  and  $\left( \frac{2}{p} \right) = -1$ .

$$\therefore \left( \frac{-2}{p} \right) = -1.$$

The above result can be restated as below : If  $p$  is an odd prime then,

$$\text{If } p = 8k+1 \text{ or } p = 8k+3, \text{ then } \left( \frac{-2}{p} \right) = 1.$$

$$\text{If } p = 8k-1 \text{ or } p = 8k-3, \text{ then } \left( \frac{-2}{p} \right) = -1.$$

**Example 3 :** Test if  $-2$  is a quadratic residue of the following integers.

- (a) 17, (b) 43, (c) 7, (d) 13.

**Sol. :** Recall that  $-2$  is a quadratic residue of an odd prime  $p$  if  $p$  is of the form  $p = 8k+1$  or  $8k+3$  and non-residue if  $p$  is of the form  $p = 8k-1$  or  $8k-3$ .

- (a)  $17 = 2 \times 8 + 1$ . Hence,  $-2$  is a quadratic residue of 17.  
 (b)  $43 = 5 \times 8 + 3$ . Hence,  $-2$  is a quadratic residue of 43.  
 (c)  $7 = 8 - 1$ . Hence,  $-2$  is a quadratic non-residue of 7.  
 (d)  $13 = 4 \times 4 - 3$ . Hence,  $-2$  is a quadratic non-residue of 13.

## 6. Solving $x^2 \equiv a \pmod{pq}$ using Chinese Remainder Theorem

So far we discussed the quadratic congruence of the type  $x^2 \equiv a \pmod{p}$  where  $p$  is a prime integer. Now, we consider  $x^2 \equiv a \pmod{n}$  where  $n$  is a product of two (and possibly three) primes. The method runs as follows :

Suppose given quadratic congruence is  $x^2 \equiv a \pmod{pq}$ .

Without the loss of generality, we can assume  $0 < a < pq$ . Consider the two quadratic congruences :

$$x^2 \equiv a \pmod{p} \quad \text{and} \quad x^2 \equiv a \pmod{q}$$

Suppose  $x_1$  (and naturally  $p - x_1$ ) are the solutions of  $x^2 \equiv a \pmod{p}$  and  $x_2$  and  $p - x_2$  are solutions of  $x^2 \equiv a \pmod{q}$ . Then, we consider four sets of simultaneous equations, namely

(i) $x = x_1 \pmod{p}$	(ii) $x = x_1 \pmod{p}$
$x = x_2 \pmod{q}$	$x = (p - x_2) \pmod{q}$
(iii) $x = (p - x_1) \pmod{p}$	(iv) $x = (p - x_1) \pmod{p}$
$x = x_2 \pmod{q}$	$x = (p - x_2) \pmod{q}$

The solutions to these linear congruences give the four incongruent solutions of the given problem. In practice, sets (iii) and (iv) may not be needed. For, if  $x_0$  and  $x_0'$  are solutions of the sets (i) and (ii), there  $-x_0$  (or equivalently  $n - x_0$ ) and  $-x_0'$  (or equivalently  $n - x_0'$ ) may be other two incongruent solutions. In case  $x_0$  or  $pq - x_0$  and  $x_0'$  happen to be the same, we may turn to (iii) or (iv).

**Example 1 :** Solve the quadratic congruence  $x^2 \equiv 1 \pmod{15}$ .

**Sol. :** Since  $15 = 3 \times 5$ , we consider the following two quadratic congruences :

$$(a) x^2 \equiv 1 \pmod{3}, \quad (b) x^2 \equiv 1 \pmod{5}$$

We observe that (a) has two incongruent solutions, 1 and  $(3 - 1) = 2$ ; (b) has solutions 1 and  $(5 - 1) = 4$ . This leads to the following sets of simultaneous linear congruences :

(i) $x = 1 \pmod{3}$	(ii) $x = 1 \pmod{3}$
$x = 1 \pmod{5}$	$x = 4 \pmod{5}$
(iii) $x = 2 \pmod{3}$	(iv) $x = 2 \pmod{3}$
$x = 1 \pmod{5}$	$x = 4 \pmod{5}$

For all the four sets of linear congruences usual notations in the Chinese remainder theorem have the following values.

$$M = 15, \quad M_1 = 5, \quad M_2 = 3, \quad m_1 = 3, \quad m_2 = 5.$$

Let  $x_1$  be inverse of  $M_1$  modulo  $m_1$  and  $x_2$  be inverse of  $M_2$  modulo  $m_2$ . Then

$$1 = M_1 x_1 \pmod{m_1} = 5x_1 \pmod{3} = 2x_1 \pmod{3}$$

$$\text{i.e.,} \quad 2x_1 = 1 \pmod{3}.$$

By inspection  $x_1 = 2$  (modulo 3).

$$\text{Similarly,} \quad 1 = M_2 x_2 \pmod{m_2} = 3x_2 \pmod{5}$$

$$\text{i.e.,} \quad 3x_2 = 1 \pmod{5}.$$

Hence, by inspection  $x_2 = 2$  (modulo 5). Therefore, the solutions of the four systems of simultaneous congruences are of the form

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 = a_1 10 + a_2 6 \pmod{15}$$

**Case (i) :** Here,  $a_1 = 1 = a_2$ . Therefore,  $x = 10 + 6 = 16 \pmod{15}$ .

$$\text{i.e.,} \quad x = 1 \pmod{15}$$

The other solution is  $x = 15 - 1 = 14 \pmod{15}$ .

**Case (ii) :** Here  $a_1 = 1, a_2 = 4$ . Therefore,  $x = 10 + 4 \times 6 = 34 \pmod{15}$ .

$$\text{i.e.,} \quad x = 4 \pmod{15}$$

The other solution is  $x = 15 - 4 = 11 \pmod{15}$ .

Thus, the four incongruent solutions are 1, 4, 11, 14 modulo 15.  
(Using cases (iii) and (iv), we will get the same solutions modulo 15.)

**Example 2 :** Find  $x$ , so that  $x^2 \equiv 4 \pmod{15}$ .

Sol. : Since  $15 = 3 \times 5$ , we consider the following two quadratic congruences.

$$(a) x^2 \equiv 4 \pmod{3}, \quad (b) x^2 \equiv 4 \pmod{5}$$

Clearly, (a) has incongruent solutions 1 and 2 and (b) has solutions 2 and 3.

This leads to the following sets of simultaneous linear congruences.

$$\begin{array}{ll} (i) x \equiv 1 \pmod{3} & (ii) x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} & x \equiv 3 \pmod{5} \\ (iii) x \equiv 2 \pmod{3} & (iv) x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{5} & x \equiv 3 \pmod{5} \end{array}$$

For all the four sets of simultaneous linear congruences, the usual notations in the Chinese remainder theorem have the following values.

$$M = 15, M_1 = 5, M_2 = 3, m_1 = 3, m_2 = 5.$$

Let  $x_1$  be the inverse of  $M_1$  modulo  $m_1$  and  $x_2$  be the inverse of  $M_2$  modulo  $m_2$ . Then  $x$  obtained in the previous example

$$x_1 = x_2 = 2 \text{ and } x = a_1 + a_2 M_1 x_1 + a_3 M_2 x_2 \pmod{15}$$

Case (i) : Here,  $a_1 = 1, a_2 = 2$  and  $x = 1 \times 10 + 2 \times 6 = 22$  modulo 15, i.e.,  $x \equiv 22 \equiv 7 \pmod{15}$

The other solution is  $x \equiv 15 - 7 \equiv 8 \pmod{15}$ .

Case (ii) : Here  $a_1 = 1, a_2 = 3$  and  $x_1 = 1 \times 10 + 3 \times 6 = 28$ . Therefore,  $x \equiv 28 \equiv 13 \pmod{15}$

The other solution is  $x \equiv 15 - 13 \equiv 2 \pmod{15}$ .

Thus, the four congruent solutions are 2, 7, 8 and 13 modulo 15.

(The remaining sets (iii) and (iv) yield the same solutions modulo 15.)

**Example 3 :** Solve  $x^2 \equiv 1 \pmod{105}$ .

Sol. : Since  $105 = 3 \times 5 \times 7$ , we consider the three quadratic congruences

$$(a) x^2 \equiv 1 \pmod{3}, \quad (b) x^2 \equiv 1 \pmod{5}, \quad (c) x^2 \equiv 1 \pmod{7}.$$

Here, (a) has incongruent solutions 1 and 2 modulo 3.

(b) has incongruent solutions 1 and 4 modulo 5.

(c) has incongruent solutions 1 and 6 modulo 7.

Therefore, we have eight sets of simultaneous linear congruences.

$$\begin{array}{ll} (i) x \equiv 1 \pmod{3} & (ii) x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} & x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{7} & x \equiv 6 \pmod{7} \\ (iii) x \equiv 1 \pmod{3} & (iv) x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} & x \equiv 4 \pmod{5} \\ x \equiv 1 \pmod{7} & x \equiv 6 \pmod{7} \\ (v) x \equiv 2 \pmod{3} & (vi) x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} & x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{7} & x \equiv 6 \pmod{7} \end{array}$$

$$\begin{array}{ll} (vii) x \equiv 2 \pmod{3} & (viii) x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} & x \equiv 4 \pmod{5} \\ x \equiv 1 \pmod{7} & x \equiv 6 \pmod{7} \end{array}$$

For all the eight sets of simultaneous linear congruences, the usual notations in the Chinese remainder theorem have the following values.

$$M = 105, M_1 = 35, M_2 = 21, M_3 = 15, m_1 = 3, m_2 = 5, m_3 = 7.$$

Let  $x_1, x_2, x_3$  be inverses, respectively of  $M_1, M_2, M_3$  modulo  $m_1, m_2, m_3$ . Then

$$1 \equiv M_1 x_1 \pmod{m_1} \Rightarrow 35x_1 \equiv 2x_1 \pmod{3}$$

$$\therefore 2x_1 \equiv 1 \pmod{3}.$$

Therefore, by inspection  $x_1 \equiv 2 \pmod{3}$ .

$$\text{Similarly, } 1 \equiv M_2 x_2 \pmod{m_2} \Rightarrow 21x_2 \equiv x_2 \pmod{5}$$

$$\therefore x_2 \equiv 1 \pmod{5} \text{ or } x_2 \equiv 1 \pmod{5}.$$

$$\text{Similarly, } 1 \equiv M_3 x_3 \pmod{m_3} \Rightarrow 15x_3 \equiv x_3 \pmod{7}$$

$$\therefore x_3 \equiv 1 \pmod{7} \text{ or } x_3 \equiv 1 \pmod{7}.$$

Therefore, the common solutions of all the eight systems of linear congruences have solutions of the form

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 \pmod{105}$$

$$\therefore x = a_1 \times 35 \times 2 + a_2 \times 21 \times 1 + a_3 \times 15 \times 1 \pmod{105}$$

$$\therefore x = a_1 \times 70 + a_2 \times 21 + a_3 \times 15 \pmod{105}$$

$$\text{Case (i) : Here } a_1 = a_2 = a_3 = 1. \text{ Hence, } x = 70 + 21 + 15 = 106 \pmod{105}.$$

$$\therefore x \equiv 1 \pmod{105}$$

The other solution is  $x \equiv 105 - 1 \equiv 104 \pmod{105}$ .

$$\text{Case (ii) : Here } a_1 = a_2 = 1, a_3 = 6. \text{ Hence, } x = 70 + 21 + 6 \times 15 = 181 \pmod{105}.$$

$$\therefore x = 181 - 105 = 76 \pmod{105}$$

The other solution is  $x \equiv 105 - 76 \equiv 29 \pmod{105}$ .

$$\text{Case (iii) : Here } a_1 = 1, a_2 = 4, a_3 = 1. \text{ Hence, } x = 1 \times 70 + 4 \times 21 + 1 \times 15 = 169 \pmod{105}.$$

$$\therefore x = 169 - 64 = 64 \pmod{105}$$

The other solution is  $x \equiv 105 - 64 \equiv 41 \pmod{105}$ .

$$\text{Case (iv) : Here } a_1 = 1, a_2 = 4, a_3 = 6. \text{ Hence, } x = 70 + 4 \times 21 + 6 \times 15 = 244 \pmod{105}.$$

$$\therefore x = 244 - 34 = 71 \pmod{105}$$

The other solution is  $x \equiv 105 - 71 \equiv 34 \pmod{105}$ .

Thus, the eight incongruent solutions are 1, 29, 34, 41, 64, 71, 76, 104 modulo 105.

A reader may verify that the computation from the remaining four cases will yield the same result.

**Example 4 :** We know that the quadratic congruence  $x^2 \equiv 860 \pmod{11021}$  has a solution. Find all incongruent solutions using Chinese remainder theorem. ( Hint :  $11021 = 103 \times 107$  )

Sol. : Since  $11021 = 103 \times 107$ , we consider the following quadratic congruences :

$$(a) x^2 \equiv 860 \pmod{103}, \quad (b) x^2 \equiv 860 \pmod{107}$$

Consider (a) : Since  $860 = 8 \times 103 + 36, x^2 \equiv 860 \equiv 36 \pmod{103}$

Therefore, it has incongruent solutions 6 and -6. Since  $-6 \equiv 103 - 6 \equiv 97 \pmod{103}$ .

We choose 6 and 97.

Consider (b) : Since  $860 = 8 \times 107 + 4$ , we have  $x^2 = 860 \equiv 4 \pmod{107}$ .

Therefore, it has incongruent solutions 2 and  $(107 - 2) = 105$ .

This leads to the following sets of simultaneous equations.

$$(I) \quad x \equiv 6 \pmod{103}$$

$$x \equiv 2 \pmod{107}$$

$$(II) \quad x \equiv 6 \pmod{103}$$

$$x \equiv 105 \pmod{107}$$

We get the following equations, which we do not need.

$$(III) \quad x \equiv 97 \pmod{103}$$

$$x \equiv 2 \pmod{107}$$

$$(IV) \quad x \equiv 97 \pmod{103}$$

$$x \equiv 105 \pmod{107}$$

For these four sets of simultaneous congruences, the values of the usual notations in the Chinese remainder theorem are

$$M = 11021, M_1 = 107, m_1 = 103, m_2 = 107.$$

Let  $x_1$  be the inverse of  $M_1$  modulo  $m_1$  and  $x_2$  be the inverse of  $M_2$  modulo  $m_2$ . Then,

$$1 \equiv M_1 x_1 \pmod{m_1} \Rightarrow 107x_1 \equiv 1 \pmod{103} \Rightarrow 4x_1 \equiv 1 \pmod{103}$$

$$\text{Therefore, } 4x_1 \equiv 1 \pmod{103}.$$

$$\text{By inspection, } x_1 \equiv 26 \pmod{103}.$$

$$\text{Similarly, } 1 \equiv M_2 x_2 \pmod{m_2} \Rightarrow 103x_2 \equiv 1 \pmod{107} \Rightarrow -4x_2 \equiv 1 \pmod{107}.$$

$$\text{Therefore, } -4x_2 \equiv 1 \pmod{107}.$$

$$\text{By inspection, } x_2 \equiv -27 \pmod{107}. \quad \text{To get } x_2 \text{ positive}$$

$$x_2 \equiv 107 - 27 = 80 \pmod{107}$$

$$\text{Thus, } x_2 \equiv 80 \pmod{107}.$$

Therefore, solutions of the systems of the congruences have form

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 = a_1 \times 107 \times 26 + a_2 \times 103 \times 80$$

$$\therefore x = 2782a_1 + 8240a_2 \pmod{11021}.$$

$$\text{Case (I) : Here, } a_1 = 6 \text{ and } a_2 = 2.$$

$$\therefore x = 2782 \times 6 + 8240 \times 2 = 33172 \pmod{11021}.$$

$$\therefore x = 33172 \equiv 3 \times 11021 + 109 = 109 \pmod{11021}$$

The other solution is  $x = -109 \pmod{11021}$ .

Case (II) : Here,  $a_1 = 6$  and  $a_2 = 105$ .

$$\therefore x = 2782 \times 6 + 8240 \times 105 = 881892 \pmod{11021}.$$

$$\therefore x = 881892 \equiv 80 \times 11021 + 212 = 212 \pmod{11021}$$

The other solution is  $x = -212 \pmod{11021}$ .

## 7. Quadratic Congruence with Composite Moduli (Continued)

Let  $a, n, p$  be integers, with  $n > 0$  and  $p$  an odd prime. If  $x^2 \equiv a \pmod{p^n}$  has a solution  $x_0$  then  $p^n \mid x_0^2 - a$  and therefore,  $p \mid x_0^2 - a$  and hence  $x_0$  is a solution of  $x^2 \equiv a \pmod{p}$ .

Converse is not that easy. Suppose  $x_0$  is a solution of the congruence

$$x^2 \equiv a \pmod{p} \quad (I)$$

where,  $(a, p) = 1$ . Let  $x_0^2 \equiv a + bp$  (II)

Consider,  $2x_0y \equiv -b \pmod{p}$  (III)

This congruence has a solution; for,  $(2x_0, p) = 1$ .

Let  $y_0$  be the solution modulo  $p$ .

Then it can be easily proved that

$$x_1 = x_0 + y_0 p \quad (\text{IV})$$

is a solution of  $x^2 \equiv a \pmod{p^2}$ .

(Observe that  $x_1^2 = x_0^2 + 2x_0y_0 p + p^2 = a + (b + 2x_0 y_0) p + p^2$ . Since, from (III),  $2x_0y_0 + b$  is a multiple of  $p$ ,  $x_1^2 = a + kp^2$  for some integer  $k$ ).

Thus, if we know a solution of  $x^2 \equiv a \pmod{p}$ , then we can find a solution of  $x^2 \equiv a \pmod{p^2}$ .

More generally, if we know a solution  $x_0$  of  $x^2 \equiv a \pmod{p^n}$ , then consider  $x_0^2 = a + b p^n$  for appropriate  $b$  and find a solution  $y_0$  for the congruence

$$2x_0y \equiv -b \pmod{p}$$

$$\text{Then, } x_1 = x_0 + y_0 p^n$$

is a solution of  $x^2 \equiv a \pmod{p^{n+1}}$ .

Thus, if  $x^2 \equiv a \pmod{p}$  has a solution, then inductively we can find a solution of  $x^2 \equiv a \pmod{p^n}$  for all positive integers  $n$ .

**Example 1 :** Solve  $x^2 \equiv 7 \pmod{3^3}$ .

Sol. : Consider  $x^2 \equiv 7 \pmod{3}$ . This is equivalent to the congruence

$$x^2 \equiv 1 \pmod{3}$$

Therefore,  $x_0 = 1$  is a solution of  $x^2 \equiv 1 \pmod{3}$ .

$$1 = 7 + (-2)3$$

This gives  $b = -2$ . So consider  $2y = 2 \pmod{3}$ .

Since  $(2, 3) = 1$ , we get  $y = 1 \pmod{3}$ . Hence,  $y_0 = 1$ .

$$x_1 = x_0 + y_0 p$$

$$= 1 + 1 \times 3 = 4 \text{ is a solution of}$$

$$x^2 \equiv 7 \pmod{9}$$

Now, we have  $x_0' = 4$  and  $16 = 7 + 1 \times 9$ .

Therefore,  $b = 1$ . Consider  $8y = -1 \pmod{9}$ .

Clearly, its solution is  $y_0' = 1$ .

Therefore, the solution of the given problem is

$$x_1' = 4 + 1 \times 9 = 13 \pmod{27}$$

The other solution is  $27 - 13 = 14 \pmod{27}$ .

So far, we considered prime  $p \neq 2$ , for the simple reason that  $1 \equiv a \pmod{2}$  if  $a$  is odd and  $0 \equiv a \pmod{2}$  if  $a$  is even. Hence,  $x^2 \equiv a \pmod{2}$  will have obvious solution according as  $a$  is odd or even.

For  $x^2 \equiv a \pmod{4}$ , it has a solution if and only if  $a \equiv 1 \pmod{4}$  and in that case  $x$  is either 3 or 1.

For  $x^2 \equiv a \pmod{2^n}$ ,  $n \geq 3$  has a solution if and only if  $a \equiv 1 \pmod{8}$ , i.e.,  $a = 8k + 1$ .

The problem of  $x^2 \equiv a \pmod{n}$ ,  $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ ,  $k_i \geq 0$ ,  $i = 0, 1, \dots, m$ , where,  $p_i$  are distinct odd primes can be solved by solving the following simultaneous congruences as illustrated in § 6, using Chinese remainder theorem,

$$\begin{aligned}x^2 &= a \pmod{2^{k_1}} \\x^2 &= a \pmod{p_1^{k_1}} \\&\vdots \\x^2 &= a \pmod{p_n^{k_n}}\end{aligned}$$

**EXERCISE - I**

- Find all quadratic residues of (a) 17, (b) 19, (c) 23.  
[Ans.: (a) 1, 2, 4, 8, 9, 13, 15, 16; (b) 1, 4, 5, 6, 7, 9, 11, 16, 17, 18; (c) 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.]
- Find the values of Legendre Symbol.  
 $\left(\frac{a}{11}\right), a = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.$   
[Ans.: For 1, 3, 4, 5, 9, it is +1; For 2, 6, 7, 8, 10, it is -1.]
- Prove that  $x^2 \equiv a \pmod{p}$  has a solution (without actually finding it) where  $a$  and  $p$  are given as  
(i)  $a = 317, p = 11$ , (ii)  $a = 1272, p = 29$ , (iii)  $a = 319, p = 5$ .
- Use Euler's Criterion to compute (a)  $\left(\frac{7}{11}\right)$ , (b)  $\left(\frac{8}{23}\right)$ , (c)  $\left(\frac{13}{23}\right)$ , (d)  $\left(\frac{5}{17}\right)$ , (e)  $\left(\frac{12}{13}\right)$ .  
[Ans.: (a) -1, (b) 1, (c) 1, (d) -1, (e) 1.]
- Use Gauss' Lemma to evaluate the Legendre symbols:  
(a)  $\left(\frac{7}{11}\right)$ , (b)  $\left(\frac{3}{7}\right)$ , (c)  $\left(\frac{8}{11}\right)$ , (d)  $\left(\frac{10}{13}\right)$ .  
[Ans.: (a) -1, (b) -1, (c) -1, (d) 1.]
- Compute the following (using any method)  
(a)  $\left(\frac{27}{31}\right)$ , (b)  $\left(\frac{-27}{31}\right)$ , (c)  $\left(\frac{-14}{23}\right)$ , (d)  $\left(\frac{-36}{41}\right)$ , (e)  $\left(\frac{36}{41}\right)$ , (f)  $\left(\frac{-882}{37}\right)$ , (g)  $\left(\frac{-2178}{2179}\right)$ .  
[Ans.: (a) -1, (b) 1, (c) 1, (d) 1, (e) 1, (f) -1, (g) 1.]
- Let  $a$  be a quadratic residue of a prime  $p$ . Show that if  $p \equiv 1 \pmod{4}$ , then  $-a$  is also a quadratic residue and if  $p \equiv 3 \pmod{4}$  then  $-a$  is a quadratic non-residue of  $p$ .  
(Hint: Given  $\left(\frac{a}{p}\right) = 1$ , we have  $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)$ . Now apply Theorem 4.)
- Solve the quadratic congruence,  
(a)  $x^2 \equiv 4 \pmod{21}$  (b)  $x^2 \equiv 16 \pmod{21}$  (c)  $x^2 \equiv 9 \pmod{35}$   
(d)  $x^2 \equiv 31 \pmod{75}$  (e)  $x^2 \equiv 58 \pmod{63}$  (f)  $x^2 \equiv 1 \pmod{1155}$   
[Ans.: (a) 2, 5, 16, 19; (b) 4, 10, 11, 17; (c) 3, 17, 18, 32; (d) 16, 34, 41, 59;  
(e) 11, 25, 38, 52;  
(f) 1, 34, 76, 274, 386, 419, 461, 496, 659, 694, 736, 769, 881, 1079, 1121, 1154.]

**6. The Law of Quadratic Reciprocity**

Let  $p$  and  $q$  be two distinct odd primes. Then we have two Legendre symbols  $(p/q)$  and  $(q/p)$ . It is, then, natural to ask : Is there any relationship between  $(p/q)$  and  $(q/p)$ ? The law of reciprocity states :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{[(p-1)/2] \cdot [(q-1)/2]} \quad (1)$$

This is one of the most useful laws governing Legendre symbols. This law has some important consequences.

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \text{ or both} \\ -1, & \text{if } p \equiv q \equiv 3 \pmod{4} \end{cases}$
- $\left(\frac{p}{q}\right) = \begin{cases} (q/p), & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \text{ or both} \\ -(q/p), & \text{if } p \equiv q \equiv 3 \pmod{4} \end{cases}$

**Proof:** (1) Let  $p \equiv 1 \pmod{4}$ . Then, there is a positive integer  $k$ , such that  $p-1 = 4k$ . Then

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = k(q-1)$$

Since,  $q$  is an odd integer,  $k(q-1)$  is an even integer.

$$\text{Therefore, } \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2} \cdot (q-1) = 1$$

Similarly, when  $q \equiv 1 \pmod{4}$ ,

If  $p \equiv q \equiv 3 \pmod{4}$ , there exist integers  $k$  and  $k'$ , such that  $p-3 = 4k$  and  $q-3 = 4k'$ .

$$\text{Therefore, } \frac{p-1}{2} \cdot \frac{q-1}{2} = (2k+1)(2k'+1), \text{ which is an odd integer.}$$

$$\text{Therefore, } \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1.$$

Hence, the result 1.

(2) Since  $(p/q)$  and  $(q/p)$  have values either 1 or -1, their product will be +1 if and only if either both are equal to 1 or both are equal to -1.

$$\text{i.e., } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

Their product is -1, if one of them is +1 and the other is -1.

$$\text{Therefore, } \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Hence, the result 2.

**Example 1 :** Evaluate the following :

$$(a) \left(\frac{3}{41}\right), (b) \left(\frac{31}{67}\right), (c) \left(\frac{111}{991}\right), (d) \left(\frac{11}{4271}\right), (e) \left(\frac{105}{1009}\right), (f) \left(\frac{19}{3547}\right).$$

**Sol. :** (a) Since  $41 \equiv 1 \pmod{4}$ ,  $\left(\frac{3}{41}\right) = \left(\frac{41}{3}\right)$  [By reciprocity]

$$\text{Since, } 41 \equiv 2 \pmod{3}, \left(\frac{41}{3}\right) = \left(\frac{2}{3}\right).$$

But 2 is non-residue of 3. Therefore,  $\left(\frac{3}{41}\right) = \left(\frac{2}{3}\right) = -1$ .

(b) Here,  $31 \equiv 3 \pmod{4}$  and  $67 \equiv 3 \pmod{4}$ .

$$\text{Therefore, } \left(\frac{31}{67}\right) = -\left(\frac{67}{31}\right)$$

[By reciprocity]

$$\text{But } 67 \equiv 5 \pmod{31} \quad \therefore \left(\frac{67}{31}\right) = \left(\frac{5}{31}\right)$$

$$\text{But } 5 \equiv 1 \pmod{4} \quad \therefore \left(\frac{5}{31}\right) = \left(\frac{31}{5}\right)$$

[By reciprocity]

$$\text{Since, } 31 \equiv 1 \pmod{5} \quad \therefore \left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1$$

Combining (i) to (iv), we get  $\left(\frac{31}{67}\right) = -1$ .

$$(c) \left(\frac{111}{991}\right) = \left(\frac{3 \times 37}{991}\right) = \left(\frac{3}{991}\right) \left(\frac{37}{991}\right)$$

Since,  $3 \equiv 3 \pmod{4}$  and  $991 \equiv 3 \pmod{4}$ , we have by reciprocity.

$$\left(\frac{3}{991}\right) = -\left(\frac{991}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

Since,  $37 \equiv 1 \pmod{4}$ , we have by reciprocity.

$$\left(\frac{37}{991}\right) = \left(\frac{991}{37}\right) = \left(\frac{29}{37}\right) = \left(\frac{37}{29}\right) = \left(\frac{8}{29}\right)$$

But  $8 = 2^3$ . Hence,  $\left(\frac{8}{29}\right) = \left(\frac{2^2}{29}\right) \left(\frac{2}{29}\right) = 1 \times \left(\frac{2}{29}\right) = \left(\frac{2}{29}\right)$ .

By Theorem 5, § 5 (page 5-12), we get

$$\left(\frac{2}{29}\right) = (-1)^{(29+1)(29-1)/8} = (-1)^{15 \times 7}$$

$$\text{Hence, } \left(\frac{2}{29}\right) = -1$$

Combining (i), (ii), (iii), (iv) and (v), we get  $\left(\frac{111}{991}\right) = (-1)(-1) = 1$ .

(d) Here,  $11 \equiv 3 \pmod{4}$  and  $4471 \equiv 3 \pmod{4}$

$$\text{Therefore, } \left(\frac{11}{4471}\right) = -\left(\frac{4471}{11}\right) \quad [\text{By reciprocity}]$$

$$\text{Since, } 4471 \equiv 3 \pmod{11} \quad \therefore \left(\frac{4471}{11}\right) = \left(\frac{3}{11}\right)$$

Since,  $3 \equiv 3 \pmod{4}$  and  $11 \equiv 3 \pmod{4}$

$$\therefore \left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right)$$

$$\text{But, } 11 \equiv 2 \pmod{3} \quad \therefore \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Combining (i) to (iv), we get  $\left(\frac{11}{4271}\right) = -1$ .

$$(e) \text{Here, } \left(\frac{105}{1009}\right) = \left(\frac{3 \times 5 \times 7}{1009}\right) = \left(\frac{3}{1009}\right) \left(\frac{5}{1009}\right) \left(\frac{7}{1009}\right)$$

$$= \left(\frac{1009}{3}\right) \left(\frac{1009}{5}\right) \left(\frac{1009}{7}\right) \quad [\text{Since } 1009 \equiv 1 \pmod{4}]$$

$$= \left(\frac{1}{3}\right) \left(\frac{4}{5}\right) \left(\frac{6}{7}\right) = (1)(1)(-1) = -1.$$

(f) Here,  $19 \equiv 3 \pmod{4}$  and  $3547 \equiv 3 \pmod{4}$

$$\text{Therefore, by reciprocity, we get } \left(\frac{19}{3547}\right) = -\left(\frac{3547}{19}\right)$$

$$\text{Since, } 3547 \equiv 13 \pmod{19} \quad \therefore \left(\frac{3547}{19}\right) = \left(\frac{13}{19}\right)$$

$$\text{Since, } 13 \equiv 1 \pmod{4} \quad \therefore \left(\frac{13}{19}\right) = \left(\frac{19}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{2}{13}\right) \left(\frac{3}{13}\right)$$

(Since  $19 \equiv 5 \pmod{13}$ )

$$\text{But, } \left(\frac{2}{13}\right) = (-1)^{(13^2-1)/8} = (-1)^{21} = -1$$

$$\text{and } \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$$

(Since,  $13 \equiv 1 \pmod{12}$ . See also next example.)

$$\text{Combining (i) to (v), we get } \left(\frac{19}{3547}\right) = 1.$$

**Example 2 :** Let  $p$  be an odd prime. Then,

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12} \\ -1, & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

Sol. : Case (i)  $p \equiv 1 \pmod{12}$

Since,  $p \equiv 1 \pmod{12}$  and  $4 \nmid 12$ , we have  $p \equiv 1 \pmod{4}$

$$\text{Therefore, by reciprocity, } \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right).$$

To evaluate  $\left(\frac{p}{3}\right)$ , consider  $p^2 - p = p(p-1)$ . Substituting  $p = 12k + 1$ ,

$$p^2 - p = 12k + 1 - 12k = 1 \quad (\text{say})$$

Therefore,  $3 \nmid p^2 - p$ . Hence,  $p^2 \equiv p \pmod{3}$ .

$$\text{Therefore, } \left(\frac{p}{3}\right) = 1 \text{ and consequently } \left(\frac{3}{p}\right) = 1.$$

**Case (ii) :**  $p \equiv -1 \pmod{12}$

Since,  $p \equiv -1 \pmod{12}$  and  $4 \mid 12$ ,  $p \equiv -1 \pmod{4}$ .

Thus,  $p \equiv 3 \pmod{4}$ , clearly  $3 \equiv 3 \pmod{4}$ .  
Therefore, by reciprocity,  $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ .

Since,  $p \equiv 1 \pmod{12}$  and  $3 \nmid 12$ ,  $p \equiv 1 \pmod{3}$  or that  $p \equiv 2 \pmod{3}$ .  
Since, 2 is non-residue of 3,  $p$  is non-residue of 3.

Therefore,  $\left(\frac{p}{3}\right) = -1$ . Therefore,  $\left(\frac{3}{p}\right) = -(-1) = 1$ .

**Case (III) :**  $p \equiv 5 \pmod{12}$

Since,  $p \equiv 5 \pmod{12}$  and  $4 \mid 12$ ,  $p \equiv 5 \pmod{4}$ , i.e.,  $p \equiv 1 \pmod{4}$ .  
Therefore, by reciprocity,  $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ .

Since  $p \equiv 5 \pmod{12}$  and  $3 \mid 12$ , we have  $p \equiv 5 \pmod{3}$ , i.e.,  $p \equiv 2 \pmod{3}$ .  
As 2 is non-residue,  $p$  is non-residue of 3.

Therefore,  $\left(\frac{p}{3}\right) = -1$ . Therefore,  $\left(\frac{3}{p}\right) = -1$ .

**Case (IV) :**  $p \equiv -5 \pmod{12}$

Since,  $p \equiv -5 \pmod{12}$  and  $4 \mid 12$ ,  $p \equiv -5 \pmod{4}$ , i.e.,  $p \equiv 3 \pmod{4}$ .  
Therefore, by reciprocity,  $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ .

Since  $p \equiv -5 \pmod{12}$  and  $3 \mid 12$ , we have  $p \equiv -5 \pmod{3}$ , i.e.,  $p \equiv 1 \pmod{3}$ .  
Therefore,  $\left(\frac{p}{3}\right) = 1$ . Therefore,  $\left(\frac{3}{p}\right) = -1$ .

**Example 3 :** Evaluate the Legendre symbols : (a)  $\left(\frac{21}{53}\right)$ , (b)  $\left(\frac{102}{37}\right)$ .

Sol. : (a)  $\left(\frac{21}{53}\right) = \left(\frac{7}{53}\right)\left(\frac{3}{53}\right)$

Since,  $53 = 4 \times 12 + 5$ ,  $\left(\frac{3}{53}\right) = -1$ .

To evaluate  $\left(\frac{7}{53}\right)$ , observe that  $53 = 13 \times 4 + 1$ .

Hence, by reciprocity  $\left(\frac{7}{53}\right) = \left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = 1$ . Hence,  $\left(\frac{21}{53}\right) = -1$ .

(b)  $\left(\frac{102}{37}\right) = \left(\frac{17}{37}\right)\left(\frac{3}{37}\right)\left(\frac{2}{37}\right)$  [ Since,  $102 = 17 \times 3 \times 2$  ]

Since,  $37 = 3 \times 12 + 1$ ,  $\left(\frac{3}{37}\right) = 1$ .

Using  $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ , we have  $\left(\frac{2}{37}\right) = (-1)^{(38 \times 36)/8}$ .

Since  $\frac{38 \times 36}{8} = 19 \times 9$ ,  $\left(\frac{2}{37}\right) = -1$ .

Since,  $37 = 9 \times 4 + 1$ , by reciprocity,  $\left(\frac{17}{37}\right) = \left(\frac{37}{17}\right) = \left(\frac{3}{17}\right) = -1$  [ Since  $17 = 12 + 5$  ].

Hence,  $\left(\frac{102}{37}\right) = \left(\frac{17}{37}\right)\left(\frac{3}{37}\right)\left(\frac{2}{37}\right) = (-1) \times 1 \times (-1) = 1$ .

Alternatively :  $\left(\frac{102}{37}\right) = \left(\frac{28}{37}\right)$  [ Since  $102 = 2 \times 37 + 28$  ].

$$= \left(\frac{7}{37}\right)\left(\frac{4}{37}\right) = \left(\frac{7}{37}\right)\left(\frac{37}{7}\right) = \left(\frac{7}{7}\right) = 1$$
 [ Since  $37 = 9 \times 4 + 1$  ].

$$= \left(\frac{2}{7}\right)$$
 [ Since  $37 = 5 \times 7 + 2$  ].

$$= (-1)^{(7^2-1)/8} = (-1)^6 = 1$$
.

**Example 4 :** Find all odd primes  $p$  for which 3 is a quadratic residue.

Sol. : Recall that an odd prime  $p$  is either of the form  $4k+1$  or  $4k+3$ ,  
i.e.,  $p \equiv 1 \pmod{4}$  or  $p \equiv 3 \pmod{4}$ .

If  $p \equiv 1 \pmod{4}$ , we have by reciprocity that  $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ .

If  $p \equiv 3 \pmod{4}$ , then as  $3 \equiv 3 \pmod{4}$ , we know, by reciprocity that,  $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ .

Hence, the problem reduces to computing  $\left(\frac{p}{3}\right)$ .

Again for odd prime  $p \neq 3$  either we have  $p \equiv 1 \pmod{3}$  or  $p \equiv 2 \pmod{3}$ .

When  $p \equiv 1 \pmod{3}$ , then  $\left(\frac{p}{3}\right) = 1$ . When  $p \equiv 2 \pmod{3}$ , then  $\left(\frac{p}{3}\right) = -1$ .

This leads to four combinations.

(a)  $p \equiv 1 \pmod{4}$ ;  $p \equiv 1 \pmod{3}$

$$\text{In this case } \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

(b)  $p \equiv 1 \pmod{4}$ ;  $p \equiv 2 \pmod{3}$

$$\text{In this case } \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

(c)  $p \equiv 3 \pmod{4}$  (and  $3 \equiv 3 \pmod{4}$ );  $p \equiv 1 \pmod{3}$

$$\text{In this case } \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

(d)  $p \equiv 3 \pmod{4}$  (and  $3 \equiv 3 \pmod{4}$ );  $p \equiv 2 \pmod{3}$

$$\text{In this case } \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1.$$

The four simultaneous congruences in (a) to (d) can be solved for  $p$ , by Chinese remainder theorem. In usual notations, in all the four sets, we have

$$M = 12, M_1 = 3, M_2 = 4, m_1 = 4, m_2 = 3.$$

If we denote the inverse of  $M_1$  by  $x_1$  modulo  $m_1$ , then  
 $1 = M_1 x_1 \pmod{m_1} \Rightarrow 3x_1 \equiv 1 \pmod{4}$

Therefore,  $x_1 \equiv 3 \pmod{4}$ .

If we denote the inverse of  $M_2$  by  $x_2$  modulo  $m_2$ , then,  
 $1 = M_2 x_2 \pmod{m_2} \Rightarrow 4x_2 \equiv 1 \pmod{3}$

Therefore,  $x_2 \equiv 1 \pmod{3}$ .

Then the solutions of the four sets of simultaneous equations are of the form  
 $p = a_1 \times 3 + a_2 \times 4 + 1$   
*i.e.*,  $p = a_1 \times 9 + a_2 \times 4 \pmod{12}$ .

In the case of (a) :  $a_1 = 1 = a_2$ . Therefore,  $p \equiv 13 \equiv 1 \pmod{12}$ .

Therefore,  $\left(\frac{3}{p}\right) = 1 \quad \text{for } p \equiv 1 \pmod{12}$ .

In the case of (b) :  $a_1 = 1, a_2 = 2$  and  $p \equiv 9 + 8 \equiv 17 \equiv 5 \pmod{12}$ .

Therefore,  $\left(\frac{3}{p}\right) = -1 \quad \text{for } p \equiv 5 \pmod{12}$ .

In the case of (c) :  $a_1 = 3, a_2 = 1$  and  $p \equiv 27 + 4 \equiv 31 \equiv -5 \pmod{12}$ .

Therefore,  $\left(\frac{3}{p}\right) = -1 \quad \text{for } p \equiv -5 \pmod{12}$ .

In the case of (d) :  $a_1 = 3, a_2 = 2$  and  $p \equiv 3 \times 9 + 2 \times 4 \equiv 35 \equiv -1 \pmod{12}$ .

Therefore,  $\left(\frac{3}{p}\right) = 1 \quad \text{for } p \equiv -1 \pmod{12}$ .

Combining (I) to (IV), we have

$\left(\frac{3}{p}\right) = 1, \text{ for } p \equiv \pm 1 \pmod{12}; \text{ and } \left(\frac{3}{p}\right) = -1, \text{ for } p \equiv \pm 5 \pmod{12}$ .

Note ....

1. The result in Example 2 and 4 are converses of each other. Therefore,

For prime  $p \neq 2$ ,  $\left(\frac{3}{p}\right) = 1 \quad \text{if and only if } p \equiv \pm 1 \pmod{12}$   
 $\left(\frac{3}{p}\right) = -1 \quad \text{if and only if } p \equiv \pm 5 \pmod{12}$ .

2.  $-1 \equiv 11 \pmod{12}$  and  $-5 \equiv 7 \pmod{12}$ . Therefore,  $p \equiv \pm 1 \pmod{12}$  and  $p \equiv \pm 5 \pmod{12}$  cover all odd primes. For  $p = 12k + r$  is not prime for  $r = 2, 3, 4, 6, 8, 9$  and 10.

3. Instead of Chinese remainder theorem, we may use iteration (substitution) method :

Case (a) :  $p \equiv 1 \pmod{4}$  implies  $p \equiv 4u + 1$ , therefore, we have  $4u + 1 \equiv 1 \pmod{3}$  for some integer  $u$ .

Therefore,  $1 \equiv 1 + 4u \equiv (1 + u) + 3u \equiv (1 + u) \pmod{3}$   
*i.e.*,  $1 + u \equiv 1 \pmod{3}$ .

On subtracting 1 from both sides of the congruence, we get

$$u \equiv 0 \pmod{3}, \text{ i.e., } u = 3v$$

Substituting this value of  $u$ , we get

$$p \equiv 12v + 1 \quad \text{or} \quad p \equiv 1 \pmod{12}$$

The other value of  $p \equiv 12 - 1 \equiv 11$ , i.e.,  $p \equiv -1 \pmod{12}$ .

Case (b) : Substituting  $p \equiv 4u + 1$  in  $p \equiv 2 \pmod{3}$ , we get

$$2 \equiv 4u + 1 \equiv 3u + (u + 1) \equiv (u + 1) \pmod{3}$$

Subtracting 1 from both sides of the congruence

$$1 \equiv u \pmod{3} \quad \text{or} \quad u \equiv 1 \pmod{3}$$

i.e.,  $u = 3v + 1$  for some integer  $v$ .

Hence,  $p = 4(3v + 1) + 1 \equiv 12v + 5$ , i.e.,  $p \equiv 5 \pmod{12}$ .

The over value is  $12 - 5 \equiv 7 \equiv -5 \pmod{12}$ .

This way calculating is relatively simple but conceptually a little involved one.

Example 5 : Find all odd primes  $p$  for which  $-3$  is a quadratic residue.

Sol. : Clearly,  $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$

Since, either we have  $p \equiv 1 \pmod{4}$  or  $p \equiv 3 \pmod{4}$ , we separate 2 cases.

Case (I) :  $p \equiv 1 \pmod{4}$

For  $p \equiv 1 \pmod{4}$ , we already know,  $\left(\frac{-1}{p}\right) = 1$ . [ See Theorem 4, § 4, page 5-8 ]

By Example 2 and 4 above, we know,  $\left(\frac{3}{p}\right) = 1$  if and only if  $p \equiv \pm 1 \pmod{12}$ .

$p \equiv a \pmod{12}$  implies  $p \equiv a \pmod{4}$ , and since  $p \equiv 1 \pmod{4}$  to hold we must have  $p \equiv 1 \pmod{12}$ . (And not  $p \equiv -1 \pmod{12}$ )

Therefore,  $\left(\frac{-3}{p}\right) = 1$ , if  $p \equiv 1 \pmod{12}$ .

Case (II) :  $p \equiv 3 \pmod{4}$

For  $p \equiv 3 \pmod{4}$ ,  $\left(\frac{-1}{p}\right) = -1$  and therefore  $\left(\frac{-3}{p}\right) = -\left(\frac{3}{p}\right)$ .

Therefore,  $\left(\frac{-3}{p}\right) = 1$ , if and only if  $\left(\frac{3}{p}\right) = -1$ .

But  $\left(\frac{3}{p}\right) = -1$ , if and only if  $p \equiv \pm 5 \pmod{12}$ , i.e.,  $p \equiv 5 \pmod{12}$  or  $p \equiv 7 \pmod{12}$ .

As  $p \equiv 5 \pmod{12}$  implies  $p \equiv 5 \pmod{4}$ , i.e.,  $p \equiv 1 \pmod{4}$ , we rule out the first case. Hence,  $p \equiv 7 \pmod{12}$ .

Thus,  $\left(\frac{-3}{p}\right) = 1$ , if and only if either  $p \equiv 1 \pmod{12}$  or  $p \equiv 7 \pmod{12}$ .

We may combine the two conditions into a single one. If  $p \equiv a \pmod{12}$ , then  $p \equiv a \pmod{6}$ . Therefore,  $p \equiv 1 \pmod{12}$  implies  $p \equiv 1 \pmod{6}$  and  $p \equiv 7 \pmod{12}$ , implies  $p \equiv 7 \pmod{6}$ .

But  $7 \equiv 1 \pmod{6}$ . Hence,  $\left(\frac{-3}{p}\right) = 1$ , if and only if  $p \equiv 1 \pmod{6}$ .

### 9. The Jacobi Symbol

The Jacobi symbol is an extension of Legendre symbol to a composite number. We use same notation to denote a Jacobi and Legendre symbol without creating a confusion. The symbol  $(a/n)$ , where  $a$  and  $n > 1$  are integers, stands for a Legendre symbol, if  $n$  is a prime number. It stands for a Jacobi symbol, if  $n$  is not necessarily prime number.

**Definition :** Let  $a$  and  $n > 1$  be integers and  $(a, n) = 1$ . Let  $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$  be the prime factorization of  $n$  into odd primes. Then the Jacobi symbol  $(a/n)$  is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \left(\frac{a}{p_2}\right)^{k_2} \dots \left(\frac{a}{p_m}\right)^{k_m}$$

where the symbols on the right hand side of the equation are Legendre symbols.

Carl Gustav Jacob Jacobi (1804 - 1851)

He was educated at the university of Berlin. He was initially an unsalaried lecturer paid from the fees of the students. But was made professor of mathematics at Königsberg two years later. He was prolific contributor to various fields of mathematics. He made significant contributions to Elliptic Functions, Analysis, Differential Equations, Calculus of Variations and Infinite Series.



#### (a) Important difference between Jacobi and Legendre Symbols

If  $a$  is a quadratic residue of a prime  $p \neq 2$ , then  $(a/p) = 1$  and conversely. If  $a$  is a quadratic residue of a composite integer  $n$ , then  $(a/n) = 1$ , but the  $(a/n) = 1$  need not imply  $a$  is a quadratic residue of  $n$ .

For example,  $\left(\frac{2}{3}\right) = -1 = \left(\frac{2}{5}\right)$ . Therefore,  $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ .

But 2 is not a quadratic residue of 15. For, if 2 is a quadratic residue of 15,  $x_0^2 \equiv 2 \pmod{15}$ . Therefore,  $x_0^2 = k'15 + 2$  for some integer  $k$ . But then  $x_0^2 = k'3 + 2$  ( $k' = k \times 5$ ). This means  $x_0^2 \equiv 2 \pmod{3}$ , which is not true as 2 is a non-residue of 3. Similarly, it can be proved that 2 is a non-residue of 5.

#### (b) Properties of Jacobi Symbol

**Theorem 1 :** Let  $n$  be any positive odd integer greater than 1. Let  $a$  and  $b$  be integers relatively prime to  $n$ . Then, the following hold :

(1) If  $a \equiv b \pmod{n}$ , then  $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ .

(3)  $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$

(5)  $\left(\frac{a^2}{n}\right) = 1$ . In particular  $\left(\frac{1}{n}\right) = 1$

(2)  $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

(4)  $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/2}$

(6)  $\left(\frac{a}{n^2}\right) = 1$

We leave these results for readers to prove as exercise.

**Example 1 :** Evaluate : (a)  $\left(\frac{2}{75}\right)$ , (b)  $\left(\frac{5}{21}\right)$ , (c)  $\left(\frac{1009}{2307}\right)$ , (d)  $\left(\frac{20001}{91091}\right)$ , (e)  $\left(\frac{2657}{9897}\right)$ .

Sol. : (a)  $\left(\frac{2}{75}\right) = \left(\frac{2}{3 \times 5 \times 5}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)^2 = \left(\frac{2}{3}\right)(1) = (-1)(1) = -1$

(b)  $\left(\frac{5}{21}\right) = \left(\frac{5}{7}\right)\left(\frac{5}{3}\right) = \left(\frac{5}{7}\right)\left(\frac{2}{3}\right) = \left(\frac{5}{7}\right)(-1) = -\left(\frac{5}{7}\right)$

Since,  $5 \equiv 1 \pmod{4}$ ,  $\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right)$

But  $\left(\frac{2}{5}\right) = (-1)^{(5^2-1)/8} = -1$ .

Combining (I), (II) and (III),  $\left(\frac{5}{21}\right) = 1$ .

(c)  $\left(\frac{1009}{2307}\right) = \left(\frac{1009}{3}\right)\left(\frac{1009}{769}\right)$  [ Since  $2307 = 3 \times 769$  ]

Again, as  $1009 = 336 \times 3 + 1$ ,  $\left(\frac{1009}{3}\right) = \left(\frac{1}{3}\right) = 1$

As  $1009 = 769 + 240$  and  $240 = 4^2 \times 5 \times 3$

$\left(\frac{1009}{769}\right) = \left(\frac{4}{769}\right)^2 \left(\frac{5}{769}\right)\left(\frac{3}{769}\right) = \left(\frac{5}{769}\right)\left(\frac{3}{769}\right)$

As  $769 \equiv 1 \pmod{4}$ , we get  $\left(\frac{5}{769}\right) = \left(\frac{769}{5}\right)$  and  $\left(\frac{3}{769}\right) = \left(\frac{769}{3}\right)$ .

As  $769 \equiv 4 \pmod{5}$ , we get  $\left(\frac{5}{769}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1$ .

As  $769 \equiv 1 \pmod{3}$ , we get  $\left(\frac{3}{769}\right) = \left(\frac{1}{3}\right) = 1$ .

Therefore, combining (I) and (VI), we get  $\left(\frac{1009}{2307}\right) = 1$ .

(d)  $\left(\frac{20001}{91091}\right) = \left(\frac{20001}{11 \times 7^2 \times 13^2}\right) = \left(\frac{20001}{11}\right)\left(\frac{20001}{7}\right)^2\left(\frac{20001}{13}\right)^2$

$= \left(\frac{20001}{11}\right) = \left(\frac{3}{11}\right)$  [ Since  $2001 \equiv 3 \pmod{11}$  ]

Since,  $11 \equiv -1 \pmod{12}$ ,  $\left(\frac{3}{11}\right) = 1$ . Hence,  $\left(\frac{20001}{91091}\right) = 1$ .

(e)  $\left(\frac{2657}{9897}\right) = \left(\frac{2657}{3 \times 3299}\right) = \left(\frac{2657}{3}\right)\left(\frac{2657}{3299}\right)$

Clearly,  $\left(\frac{2657}{3}\right) = \left(\frac{2}{3}\right) = -1$ .

Since,  $2657 \equiv 1 \pmod{4}$ , we have

$$\begin{aligned} \left(\frac{2657}{3299}\right) &= \left(\frac{3299}{2657}\right) = \left(\frac{642}{2657}\right) \quad [\text{Since } 3299 = 2657 + 642] \\ &= \left(\frac{3 \times 2 \times 107}{2657}\right) = \left(\frac{3}{2657}\right) \left(\frac{2}{2657}\right) \left(\frac{107}{2657}\right) \end{aligned} \quad (\text{III})$$

Since,  $2657 \equiv 5 \pmod{12}$ ,  $\left(\frac{3}{2657}\right) = -1$

$$\left(\frac{2}{2657}\right) = (-1)^{(2658)(2656)/8} = (-1)^{\frac{2658 \times 2656}{8}} = 1 \quad (\text{IV})$$

Using reciprocity,

$$\begin{aligned} \left(\frac{107}{2657}\right) &= \left(\frac{2657}{107}\right) = \left(\frac{89}{107}\right) \\ &= \left(\frac{107}{89}\right) = \left(\frac{18}{89}\right) = \left(\frac{9 \times 2}{89}\right) = \left(\frac{9}{89}\right)^2 \left(\frac{2}{89}\right) = \left(\frac{2}{89}\right) \end{aligned} \quad (\text{V})$$

Finally,  $\left(\frac{2}{89}\right) = (-1)^{(90 \times 88)/8} = 1$ .

Combining the results (I) to (VII), we get  $\left(\frac{2657}{9897}\right) = (-1)(-1)(1)(1) = 1$ .

#### (c) How to Compute $(a/n)$ (summary)

Here,  $a$  and  $n > 0$  are integers,  $n = p_1^{k_1}, p_2^{k_2}, \dots, p_m^{k_m}$ ,  $p_1, \dots, p_m$  are distinct odd prime integers,  $k_1, k_2, \dots, k_m$  are non-negative integers and  $(a, n) = 1$ .

**Step 1:** Write  $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \left(\frac{a}{p_2}\right)^{k_2} \dots \left(\frac{a}{p_m}\right)^{k_m}$  ..... (I)

**Step 2:** If any  $k$  is even then corresponding  $\left(\frac{a}{p_k}\right)^k = 1$ . So we remove that factor from (I). If  $k$  is odd, say  $2m+1$ , then  $\left(\frac{a}{p_k}\right)^k = \left(\frac{a}{p_k}\right)^{2m} \left(\frac{a}{p_k}\right)$ .

Thus,  $\left(\frac{a}{p_k}\right)^k = \left(\frac{a}{p_k}\right)$ . ..... (II)

**Step 3:** Using step 1 and step 2, we reduce (I) as a product of Legendre symbols  $(a/p)$ .

**Step 4:** If  $a = 2^s q_1^{k_1} \dots q_r^{k_r}$ ,  $s, k_1, \dots, k_r$  positive integers,  $p, q_1, \dots, q_r$  distinct odd primes, then write  $\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^s \left(\frac{q_1}{p}\right)^{k_1} \dots \left(\frac{q_r}{p}\right)^{k_r}$ .

Again if  $s$ , or any  $k_i$  is even replace the corresponding factor safely by 1; if odd replace it by  $(2/p)$  or  $(q_i/p)$  as the case may be.

If  $a$  is negative write  $\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{-a}{p}\right)$ .

**Step 5:** We have special formulae for  $(2/p)$  and  $(-1/p)$ , given below. So consider the problem  $(q/p)$ , where  $q$  and  $p$  are odd primes.

**Step 6:** If  $q > p$  write  $q = kp + r$  where  $r < p$  using Euclidean algorithm and reduce

$$\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right)$$

If  $q < p$ , use reciprocity property and then use Euclidean algorithm.

Thus, the whole problem is of the form  $(a/p)$  where  $0 < a < p$  and  $p$  is an odd prime.

After reduction of the problem to  $(q/p)$ , use the following special formulae at discretion.

**1. Reciprocity:**  $\left(\frac{q}{p}\right) = \begin{cases} (p/q), & \text{if } p = 1 \pmod{4} \text{ or } q = 1 \pmod{4} \\ -(p/q), & \text{if } p = q = 3 \pmod{4} \end{cases}$

Go to step 6, if necessary after using this formula. Then use any of the special formulae given below.

**2.**  $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p = 1 \pmod{4} \\ -1, & \text{if } p = 3 \pmod{4} \end{cases} = -1 \pmod{4}$

**3.**  $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{(p-1)(p+1)/8}$

**4. General formulae:** Euler :  $p \nmid a$   $(a/p) = a^{(p-1)/2} \pmod{p}$

**5. Gauss :** If  $p \neq 2$ ,  $(a, p) = 1$ .

(i) Compute  $\frac{p-1}{2}$ .

(ii) List 1, 2, 3, ...,  $\frac{p-1}{2}$ .

(iii) List  $a, 2a, 3a, \dots, \left(\frac{p-1}{2}\right)a$

(iv) If necessary divide  $ka$  by  $p$  and write the remainder, so that the list in (iii) is reduced to positive integers between 1 and  $p-1$ .

(v) Find the number  $s$  of integers found in (iv), which are greater than  $p/2$ . Then  $(a/p) = (-1)^s$

**6.** If  $x^2 \equiv a \pmod{2^m}$ ,  $a$  is odd then

$$\left(\frac{a}{2}\right) = 1$$

$$\left(\frac{a}{4}\right) = 1, \quad \text{if and only if } a \equiv 1 \pmod{4}$$

$$\left(\frac{a}{2^m}\right) = 1, \quad \text{for } m \geq 3 \text{ if and only if } a \equiv 1 \pmod{8}$$

The judicious use of the following formulae reduces the work of computing  $(a/n)$ .

**7.**  $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8} \\ -1, & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$

**8.**  $\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12} \\ -1, & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$

**10. An Efficient Algorithm for Jacobi Symbols**

Let  $a, b$  be relatively prime positive integers. Let  $a > b$ . Set  $R_0 = a$  and  $R_1 = b$ . We compute by division algorithm

$$R_0 = R_1 q_1 + 2^{s_1} R_2$$

where  $2^{s_1} R_2$  is the remainder after dividing  $R_0$  by  $R_1$  and  $s_1$  is the highest index of 2 in the remainder after its factoring. We continue applying division algorithm till the remainder is expressible in the power of 2, as follows.

$$R_1 = R_2 q_2 + 2^{s_2} R_3$$

$$R_2 = R_3 q_3 + 2^{s_3} R_4$$

.....

$$R_{n-3} = R_{n-2} q_{n-2} + 2^{s_{n-2}} R_{n-1}$$

$$R_{n-2} = R_{n-1} q_{n-1} + 2^{s_{n-1}} \cdot 1$$

**Note ...**

Note that  $s_1, s_2, \dots, s_{n-1}$  are non-negative integers and  $R_2, R_3, \dots, R_{n-1}$  are odd positive integers. It can be observed that number of divisions required in this process does not exceed the number of divisions required in finding the greatest common divisor of  $a$  and  $b$  using Euclidean algorithm.

$$\text{Let } N = \frac{s_1(R_1^2 - 1)}{8} + \frac{s_2(R_2^2 - 1)}{8} + \dots + \frac{s_{n-1}(R_{n-1}^2 - 1)}{8} + \left( \frac{R_1 - 1}{2} \cdot \frac{R_2 - 1}{2} \right) + \left( \frac{R_2 - 1}{2} \cdot \frac{R_3 - 1}{2} \right) + \dots + \left( \frac{R_{n-2} - 1}{2} \cdot \frac{R_{n-1} - 1}{2} \right)$$

$$\text{Then, } \left( \frac{a}{b} \right) = (-1)^N.$$

The method is complicated for manual calculation. But it has several advantages for machine calculation. It puts no restrictions on  $a, b$ , except that  $a > b$  and that they are positive integers, which are relatively prime. They need not be prime. Again, since we want to know, whether  $(a/b)$  is +1 or -1, we need not perform the sum  $N$ . We neglect the summand in  $N$  if it is an even integer. For, it corresponds to a factor 1. Therefore, all we need to do is to count the summands in  $N$  which produce odd integers. If these summands are odd in number, then  $(-1)^N = -1$ . If they are even in number, then  $(-1)^N = 1$ .

**Example 1 :** Evaluate  $\left( \frac{401}{111} \right)$ .

Sol. : Choose  $R_0 = 401, R_1 = 111$ . Then

$$\begin{aligned} 401 &= 111 \times 3 + 2^2 \times 17 & [\text{As } 401 = 111 \times 3 + 68] \\ 111 &= 17 \times 6 + 2^0 \times 9 & [\text{As } 111 = 17 \times 6 + 9] \\ 17 &= 9 \times 1 + 2^3 \times 1 & [\text{As } 17 = 9 + 8] \end{aligned}$$

Hence,  $R_1 = 111, R_2 = 17, R_3 = 9, s_1 = 2, s_2 = 0, s_3 = 3$ .

$$\text{Therefore, } \frac{s_1(R_1^2 - 1)}{8} = \frac{2 \times (111+1)(111-1)}{8} = \frac{2 \times 112 \times 110}{8}$$

which is clearly an even number  $2 \times 14 \times 110$ . So we move ahead.

$$\frac{s_2(R_2^2 - 1)}{8} = 0$$

$$\frac{s_3(R_3^2 - 1)}{8} = \frac{3(10) \times 8}{8} \text{ is even}$$

$$\frac{(R_1 - 1)(R_2 - 1)}{4} = \frac{110 \times 16}{4} \text{ is even}$$

$$\frac{(R_2 - 1)(R_3 - 1)}{4} = \frac{16 \times 8}{4} \text{ is even.}$$

Hence,  $N$  is even and  $(-1)^N = 1$ . Therefore,  $\left( \frac{401}{111} \right) = 1$ .

A reader may calculate,

$$\left( \frac{401}{111} \right) = \left( \frac{401}{3} \right) \left( \frac{401}{37} \right) = \left( \frac{2}{3} \right) \left( \frac{3}{31} \right) = 1.$$

**Example 2 :** Evaluate  $\left( \frac{2663}{3299} \right)$ .

Sol. : Choose  $R_0 = 3299, R_1 = 2663$ . Then

$$\begin{aligned} 3299 &= 2663 \times 1 + 636 & 2663 \times 1 + 2^2 \times 159 \\ 2663 &= 159 \times 16 + 119 & 159 \times 16 + 2^0 \times 119 \\ 159 &= 119 \times 1 + 40 & 119 \times 1 + 2^3 \times 5 \\ 119 &= 5 \times 23 + 4 & 5 \times 23 + 2^2 \end{aligned}$$

Hence,  $R_1 = 2663, R_2 = 159, R_3 = 119, R_4 = 5, s_1 = 2, s_2 = 0, s_3 = 3, s_4 = 2$ .

$$\text{Therefore, } \frac{s_1(R_1^2 - 1)}{8} = \frac{2 \times (2662)(2664)}{8} = \frac{2 \times 2 \times (1331) \times 2 \times (1332)}{8}$$

which is clearly an even number.

$$\frac{s_2(R_2^2 - 1)}{8} = 0$$

$$\frac{s_3(R_3^2 - 1)}{8} = \frac{3(118)(120)}{8} = 3(118)15 \text{ is even}$$

$$\frac{s_4(R_4^2 - 1)}{8} = \frac{2(6)(4)}{8} \text{ is even number.}$$

$$\frac{(R_1 - 1)(R_2 - 1)}{4} = \frac{(2662)(158)}{4} = (1331)(79) \text{ is odd}$$

$$\frac{(R_2 - 1)(R_3 - 1)}{4} = \frac{(158)(118)}{4} = 79 \times 59 \text{ is odd.}$$

$$\frac{(R_3 - 1)(R_4 - 1)}{4} = \frac{(118)(4)}{4} = 118 \text{ is an even integer.}$$

There are exactly two summand which are odd all other are even. Therefore,  $N$  is a even integer and thus,

$$\left(\frac{3299}{2663}\right) = (-1)^N = 1$$

Now,  $3299 \equiv 3 \pmod{4}$ ,  $2663 \equiv 3 \pmod{4}$ . Therefore, by reciprocity

$$\left(\frac{2663}{3299}\right) = -\left(\frac{3299}{2663}\right) = -1$$

$$\begin{aligned} \text{Alternative: } \left(\frac{2663}{3299}\right) &= -\left(\frac{3299}{2663}\right) = -\left(\frac{636}{2663}\right) = -\left(\frac{4 \times 3 \times 53}{2663}\right) \\ &= -\left(\frac{3}{2663}\right)\left(\frac{53}{2663}\right) = \left(\frac{2663}{3}\right)\left(\frac{2663}{53}\right) \\ &= \left(\frac{2}{3}\right)\left(\frac{13}{53}\right) = (-1)\left(\frac{53}{13}\right) = (-1)\left(\frac{1}{13}\right) = -1. \end{aligned}$$

### 11. General Problem $ax^2 + bx + c \equiv 0 \pmod{p}$

Finally let us have a look at the general problem of solving quadratic congruence, which we mentioned at the beginning :

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad \dots \dots \dots (I)$$

We are to find  $x$  satisfying the above congruence when  $p$  is an odd prime  $p \nmid a$ , (otherwise, problem does not remain quadratic).

Since  $p \nmid 2$ , we have  $p \nmid 4$  and consequently  $p \nmid 4a$ . Therefore, we can multiply both sides of (I) by  $4a$  without disturbing the congruence. Consider

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p} \quad \dots \dots \dots (II)$$

We write,  $4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$

Therefore, (II) can be written as

$$(2ax + b)^2 - (b^2 - 4ac) \equiv 0 \pmod{p}$$

$$\text{i.e., } (2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}$$

Writing  $(2ax + b) = y$  and  $(b^2 - 4ac) = d$ , we have

$$y^2 \equiv d \pmod{p} \quad \dots \dots \dots (III)$$

And this is the problem we discussed in this chapter for solution.

**Example 1 :** Find all possible values of  $x$ , so that

$$(a) x^2 + x + 1 \equiv 0 \pmod{7}, \quad (b) x^2 + 5x + 1 \equiv 0 \pmod{7}, \quad (c) x^2 + 3x + 1 \equiv 0 \pmod{7}.$$

**Sol. :** (a) Since  $7 \nmid 4$ , we multiply both sides of the given congruence, by 4, to get

$$4(x^2 + x + 1) \equiv 0 \pmod{7}$$

$$\text{Clearly, } 4(x^2 + x + 1) = (2x + 1)^2 + 3$$

$$\therefore (2x + 1)^2 + 3 \equiv 0 \pmod{7}$$

$$\text{i.e., } (2x + 1)^2 \equiv -3 \equiv 4 \pmod{7}$$

Substituting  $y = 2x + 1$ , we get the quadratic congruence

$$y^2 \equiv 4 \pmod{7}$$

Clearly,  $y = \pm 2$  are the solutions of congruence modulo 7. But this representation of  $y$  does not yield integral values for  $x = (y - 1)/2$ . So we choose odd values for  $y$ . This can be done as  $-2 \equiv 5 \pmod{7}$  and  $+2 \equiv 9 \pmod{7}$ .

Choosing  $y = 5$ , we get  $x = 2$ , for  $y = 9$ , we get  $x = 4$ .

Thus,  $x = 2$  and 4 modulo 7 are the solutions.

(b) Multiplying both sides of the congruence by 4, we get

$$4(x^2 + 5x + 1) \equiv 0 \pmod{7}$$

Clearly,

$$4(x^2 + 5x + 1) \equiv (2x + 5)^2 - 21$$

$$\therefore (2x + 5)^2 - 21 \equiv 0 \pmod{7}$$

Since  $7 \mid 21$ , we get  $(2x + 5)^2 \equiv 0 \pmod{7}$

Since  $(2x + 5)^2$  is congruent to 0 (modulo 7), we have  $(2x + 5)^2 = k^2$  for some integer  $k$ . For integral value of  $x$ ,  $k$  must be non-zero. And for the right hand side to be a perfect square  $k$  must be a multiple of 7.

We choose  $k = 7$ . Then  $(2x + 5)^2 = 7^2$  or  $2x + 5 \equiv \pm 7$ . This gives  $x = 1$  or  $x = -6$ .

Clearly,  $1 \equiv -6 \pmod{7}$ . Hence,  $x = 1$  is the only solution modulo 7.

(c) Multiplying both sides of the congruence by 4, we get

$$4(x^2 + 3x + 1) \equiv 0 \pmod{7}$$

Clearly,

$$4(x^2 + 3x + 1) \equiv (2x + 3)^2 - 5$$

$$\therefore (2x + 3)^2 - 5 \equiv 0 \pmod{7}$$

Or putting  $2x + 3 = y$  and rearranging the terms,

$$y^2 \equiv 5 \pmod{7}$$

It can be verified that  $7 \nmid k^2 - 5$ , for  $k = 1, 2, 3, \dots, 6$ .

Hence, the given equation has no solution.

**Example 2 :** Solve the following quadratic congruences :

$$(a) 3x^2 + 9x + 7 \equiv 0 \pmod{13}, \quad (b) 5x^2 + 6x + 1 \equiv 0 \pmod{23}$$

**Sol. :** (a) Multiplying both sides of the given congruence, by 12, we get

$$36x^2 + 108x + 84 \equiv 0 \pmod{13}$$

$$\text{Clearly, } 36x^2 + 108x + 84 \equiv (6x + 9)^2 + 3$$

$$\therefore (6x + 9)^2 + 3 \equiv 0 \pmod{13}$$

Substituting  $6x + 9 = y$  and rearranging the terms, we get

$$y^2 \equiv -3 \pmod{13}$$

Clearly, this has solutions  $y^2 \equiv \pm 6 \pmod{13}$ .

(i) Let  $y \equiv 6 \pmod{13}$ . Resubstituting  $y \equiv 6x + 9$ , we get

$$6x + 9 \equiv 6 \pmod{13}$$

$$\text{i.e., } 6x \equiv -3 \pmod{13}$$

Since  $(3, 13) = 1$ , we cancel 3, to get  $2x \equiv -1 \pmod{13}$ .

$$\therefore x \equiv 6 \pmod{13}$$

(ii) Let  $y \equiv -6 \pmod{13}$ . Following parallel steps, we get

$$6x + 9 \equiv -6 \pmod{13}$$

$$\text{i.e., } 6x \equiv -15 \pmod{13}$$

$$\therefore 2x \equiv -5 \pmod{13}$$

Therefore, by inspection  $x \equiv 4 \pmod{13}$ .

Thus, the solutions are  $x \equiv 6$  and 4 modulo 13.

(b) Multiplying both sides of the given congruence by 20, we get  
 $100x^2 + 120x + 20 \equiv 0 \pmod{23}$

Clearly,  $100x^2 + 120x + 20 \equiv (10x + 6)^2 - 16 \pmod{23}$   
 $\therefore (10x + 6)^2 - 16 \equiv 0 \pmod{23}$

Substituting  $10x + 6 = y$  and rearranging the terms, we get  
 $y^2 \equiv 16 \pmod{23}$ .

Clearly, this has solutions  $y \equiv \pm 4 \pmod{23}$ .

(i) Let  $y \equiv 4 \pmod{23}$ . Resubstituting  $y \equiv 10x + 6$ , we get  
 $10x + 6 \equiv 4 \pmod{23}$  i.e.,  $10x \equiv -2 \pmod{23}$

Since  $(2, 23) = 1$ , we cancel 2, to get  $5x \equiv -1 \pmod{23}$ .

$x \equiv 9 \pmod{23}$

(ii) Let  $y \equiv -4 \pmod{23}$ . Following parallel steps as in the previous case, we get  
 $10x + 6 \equiv -4 \pmod{23}$  i.e.,  $10x \equiv -10 \pmod{23}$

Since  $(10, 23) = 1$ , we cancel 10, to get  $x \equiv -1 \pmod{23}$ .

Clearly, the solution is  $x \equiv 22 \pmod{23}$ .

Thus, the solutions are  $x \equiv 9$  and  $22$  modulo 23.

### EXERCISE - II

- Calculate the following :  
(a)  $\left(\frac{13}{17}\right)$ , (b)  $\left(\frac{15}{19}\right)$ , (c)  $\left(\frac{5}{79}\right)$ , (d)  $\left(\frac{21}{53}\right)$ , (e)  $\left(\frac{2}{45}\right)$ , (f)  $\left(\frac{109}{385}\right)$ , (g)  $\left(\frac{401}{111}\right)$ , (h)  $\left(\frac{219}{419}\right)$ ,  
(i)  $\left(\frac{12703}{3658}\right)$ , (j)  $\left(\frac{631}{1099}\right)$ , (k)  $\left(\frac{215}{253}\right)$ , (l)  $\left(\frac{24}{101}\right)$ , (m)  $\left(\frac{-24}{101}\right)$ , (n)  $\left(\frac{2663}{3299}\right)$ .  
[Ans. : (a) 1, (b) -1, (c) 1, (d) -1, (e) -1, (f) -1, (g) 1, (h) 1,  
(i) -1 ( Hint :  $3658 = 2 \times 31 \times 59$  ),  
(j) 1, (k) -1, (l) 1, (m) 1, (n) -1.]
- Find all odd primes  $p$  for which 5 is a quadratic residue. In other words find all odd primes for which  $(5/p) = 1$ .  
[ Ans. : 1, 9, 11 or 19  $\pmod{20}$  ]
- Find all odd primes  $p$  for which 7 is a quadratic residue.  
( Hint :  $7 \equiv 3 \pmod{4}$  and  $p \equiv 1 \pmod{4}$  or  $p \equiv 3 \pmod{4}$ . See Ex. 4, above. )  
[ Ans. :  $p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$  ]
- Find all prime  $p$  of which 6 is a residue.  
[ Ans. :  $p = 1, 5, 19$  or  $23 \pmod{24}$  ]
- Check if the following quadratic congruences have a solution, and find all the solutions if exists.  
(a)  $3x^2 + 6x + 5 \equiv 0 \pmod{89}$ , (b)  $2x^2 + 5x - 9 \equiv 0 \pmod{101}$   
[ Ans. : (a)  $(-24/89) = -1$ , hence no solution.  
(b)  $(97/101) = 1$ , has solutions  $x \equiv 19, 29 \pmod{101}$  ]
- Calculate the Jacobi symbols in the problem 1 by the algorithm given in § 7.
- Show that  $x^2 \equiv 3 \pmod{13}$  has a solution but  $x^2 \equiv 3 \pmod{31}$  has no solution.



## Random Variables

### 1. Introduction

You have studied probability in XII Std., we shall now discuss a very important concept which plays a key role in probability theory i.e. random variable which itself is a function. After defining it clearly we shall then consider discrete and continuous random variables and functions associated with them.

Clear understanding of this rich concept of random variable is essential for the understanding of another equally important concept of random process. As random process is a collection of random variables, for better understanding of random variables we shall discuss the following examples.

### 2. Random Variable

In the previous chapter we learnt how to find the probability of an outcome and the laws of probability. We saw that the outcome of an experiment can be anything : it may be colour (black-white-red ....) of a ball, a gender (male-female) of a child, a suit (club-diamond-spade-heart) of a card or a number (1 - 2 - 3 - 4 - 5 - 6) of a die or a logical answer (yes - no) of a question or result of a toss (head - tail) of a coin. In most of the problems the outcome of an experiment is a number e.g. the salary of a person, the height of a student, the temperature at a place, the rainfall on a particular day. However, when the outcome is not a number we can express these outcomes in numbers by agreeing to denote,

- (a) head by 1 and tail by 0      (b) boy by 1 and girl by 0
- (c) yes by 1 and no by 0      (d) club by 1, diamond by 2, spade by 3 and heart by 4
- (e) red by 1, white by 2 and black by 3, etc.

In probability problems it is found convenient to think of a variable and consider the values of the variable which describe the outcomes of the experiment. In the toss of a coin the variable takes values 1 and 0; in the selection of a child it takes values 1 and 0, in the answers of the question it takes the values 1 and 0, in drawing a card it takes values 1, 2, 3, 4, in drawing a ball it takes values 1, 2, 3 etc. This variable may take discrete values or may take any value in a range continuously e.g. the arrival time of a bus at a stop, say, between 9 a.m. and 9.10 a.m. may be any number between the range. Such a variable is called a **random variable**. Actually random variable is a misnomer. It is a function which assigns a real number to the outcome of an experiment. A random variable is denoted by  $X$  and a particular value of  $X$  is denoted by  $x$ . In the toss of a coin  $X$  assigns the value 1 to H and 0 to T, in the selection of a ball  $X$  assigns value 1 to red, 2 to white and 3 to black.

In these cases  $X$  takes discrete values and is called a discrete random variable. But in the case of arrival time of a bus  $X$  takes continuously any value between 9 am. and 9.10 am. and hence

$X$  is a continuous random variable. In this way, we consider  $X$  as a function from sample space  $S$  to the set of real numbers  $R$ . Thus we get the following definition.

(a) Definition

Let  $E$  be an experiment and  $S$  be the sample space associated with it. A function  $X$  assigning to every element  $s$  of  $S$  one and only one real number  $x = X(s)$  of  $R$  is called a random variable.

Since  $X$  is a function whose domain is the set of outcomes of an experiment and whose range is a part or the whole of real line ( $-\infty < x < \infty$ ), it can be shown pictorially as a mapping from the sample space to the real line.

The random variable  $X$  can be discrete or continuous depending upon the nature of its domain.

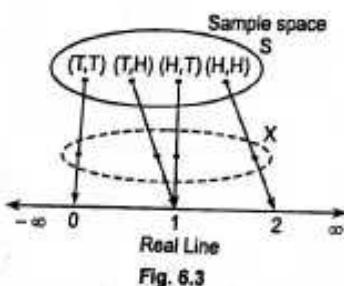
Remarks ...

1. In simple words a variable used to denote the numerical value of the outcome of an experiment is called the random variable, abbreviated as r.v.
2.  $X$  is a function and still we call it a variable.
3. We are not interested in the functional nature of  $X$  but in the values of  $X$ .
4.  $X$  must be single valued i.e. for every  $s$  of  $S$  there corresponds exactly one value of  $X$ . Different elements of  $S$  may lead to the same value of  $X$  (See Example 2). But two values of  $X$  cannot be assigned to the same sample point.
5. We shall denote random variables by capital letters  $X, Y, Z, \dots$ , and shall denote the unknown values of these random variables by small letters  $x, y, z, \dots, x_1, x_2, \dots, y_1, y_2, \dots, z_1, z_2, \dots$  etc. This is an important distinction and students should note it carefully. With this notation it is meaningless to write  $P(x \geq 10)$  say since  $x$  being a value of  $X$  either is or is not  $\geq 10$ . Instead we should write  $P(X \geq 10)$ .

Example 1 : Suppose the experiment  $E$  is to toss a fair coin.

Then  $S = \{H, T\}$ . If  $X$  is the random variable denoting the number of heads then we have  $X(H) = 1$  and  $X(T) = 0$ .

[ See Fig. 6.2 ]



Example 2 : Suppose the experiment  $E$  is to toss two fair coins.

Then  $S = \{(H, H), (H, T), (T, H), (T, T)\}$ . If  $X$  is the random variable denoting the number of heads then  $X(H, H) = 2, X(H, T) = 1, X(T, H) = 1, X(T, T) = 0$ .

[ See Fig. 6.3 ]

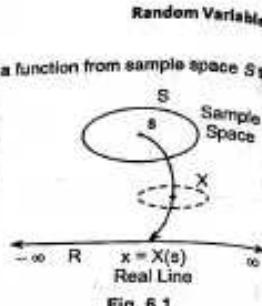


Fig. 6.1

Example 3 : Suppose the experiment is to record the temperature at a place.

If  $X$  denotes the temperature then  $X$  can take any value from  $-273^{\circ}\text{F}$  to  $212^{\circ}\text{F}$  say. [ See Fig. 6.4 ]

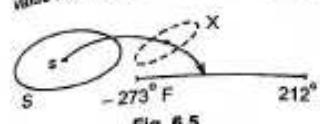


Fig. 6.4

Example 4 : Suppose the experiment is to record the time required to complete a software project. If  $X$  denotes the time then  $X$  can take any value (theoretically) from 0 to  $\infty$ . [ See Fig. 6.5 ]

In examples 1 and 2,  $X$  takes discrete values and in examples 3 and 4,  $X$  takes continuously all values between a specified interval. In the first case  $X$  is called a **discrete random variable**. In the second case it is called **continuous random variable**.

(b) Definition

Let  $X$  be a random variable. If  $X$  takes finite or countably infinite values  $x_0, x_1, x_2, \dots$ , then  $X$  is called a **discrete random variable**.

(c) Definition

Let  $X$  be a random variable. If  $X$  takes uncountably infinite values in a given interval then  $X$  is called a **continuous random variable**.

### 3. Probability Distribution of a Discrete Random Variable

As we know already, with every possible outcome of an experiment there will be associated its probability. We shall be interested in the values of the random variable  $X$  along with their probabilities. If  $x_i$  is the value of  $X$  and  $P(x_i)$  is the probability of  $x_i$  then set of pairs  $\{x_i, P(x_i)\}$  is called the probability distribution of  $X$ .

**Definition :** Let  $X$  be a discrete random variable. Let  $x_1, x_2, \dots, x_n, \dots$  be the possible values of  $X$ . With each possible outcome  $x_i$  we associate a number  $p(x_i) = P(X = x_i)$  called the probability of  $x_i$ . The numbers  $p(x_i)$ ,  $i = 1, 2, \dots, n, \dots$  must satisfy the following conditions :

1.  $p(x_i) \geq 0$  for all  $i$
2.  $\sum_{i=1}^{\infty} p(x_i) = 1$

The function  $p$  is called the probability function or probability mass function (p.m.f) or probability density function (p.d.f.) of the random variable  $X$  and the set of pairs  $\{x_i, p_i\}$  is called the probability distribution of  $X$ .

The probability distribution of a discrete random variable  $X$  taking values  $x_1, x_2, x_3, \dots, x_n, \dots$  with probabilities  $p_1, p_2, p_3, \dots, p_n, \dots$  where  $p_i \geq 0$  and  $\sum p_i = 1$  can be given in tabular form as

$X$	$x_1$	$x_2$	$x_3$	$\dots$	$x_n$	$\dots$
$P(x_i)$	$p_1$	$p_2$	$p_3$	$\dots$	$p_n$	$\dots$

**Example 1 :** State true or false with justification :

(a) A random variable  $X$  takes values 0, 1, 2 and 3 then  $p(X = x) = \frac{x-1}{2}$  can be its probability distribution.

(b) A random variable takes values 0, 1, 2 and  $p(x) = \frac{x+1}{3}$  is its probability distribution.

**Sol. :** As seen above for a probability distribution, two conditions must be satisfied.

(i) Each probability must be equal to or greater than zero but less than one.

(ii) The sum of all probabilities must be equal to unity.

Putting  $x = 0, 1, 2, 3$  in (a), we get

$$P(0) = -\frac{1}{2}, \quad P(1) = 0, \quad P(2) = \frac{1}{2}, \quad P(3) = 1$$

Since, the probability cannot be negative,  $P(X = x) = \frac{x-1}{2}$  cannot be a probability distribution.

Putting  $x = 0, 1, 2, 3$ , in (b), we get

$$P(0) = \frac{1}{3}, \quad P(1) = \frac{2}{3}, \quad P(2) = 1.$$

Although all probabilities are positive, the sum of all the probabilities is 2, (greater than 1). Hence,  $P(X = x) = \frac{x+1}{3}$  also cannot be a probability distribution.

**Example 2 :** From the past experience it was found that the daily demand at an autogarage was as under.

<b>Daily Demand</b>	:	5	6	7
<b>Probability</b>	:	0.25	0.65	0.10

Check if this is a probability distribution. Find also the probability that over a period of two days the number of demands would be 11 or 12.

**Sol. :** Since the sum of all probabilities =  $0.25 + 0.65 + 0.10 = 1$ , it is a probability distribution.

$P(11 \text{ requests over two days})$

$$\begin{aligned} &= P(5 \text{ requests on the first day and } 6 \text{ on the second}) \\ &\quad + P(6 \text{ request on the first day and } 5 \text{ on the second}) \\ &= (0.25 \times 0.65) + (0.65 \times 0.25) \\ &= 0.1625 + 0.1625 = 0.325 \end{aligned}$$

$P(12 \text{ requests over two days})$

$$\begin{aligned} &= P(5 \text{ requests on the first day and } 7 \text{ on the second}) \\ &\quad + P(6 \text{ requests on the first day and } 6 \text{ on the second}) \\ &\quad + P(7 \text{ requests on the first day and } 5 \text{ on the second}) \\ &= (0.25 \times 0.10) + (0.65 \times 0.65) + (0.10 \times 0.25) \\ &= 0.025 + 0.4225 + 0.025 = 0.4725. \end{aligned}$$

**Example 3 :** Find the probability distribution of number of heads ( $X$ ) obtained when a fair coin is tossed 4 times.

**Sol. :** When a coin is tossed 4 times, there are  $2^4 = 16$  outcomes which are listed below.

$Y$	1	2	3	4	5	6
$P(Y = y)$	1/36	3/36	5/36	7/36	9/36	11/36

**Example 7 :** For the above distribution, (i) find the probability that  $X$  is an odd number, (ii) find the probability that  $X$  lies between 3 and 9.

$$\begin{aligned} \text{Sol. : } P(X \text{ is odd}) &= P(X = 3, 5, 7, 9 \text{ or } 11) \\ &= P(X = 3) + P(X = 5) + P(X = 7) + P(X = 9) + P(X = 11) \\ &= \frac{2}{36} + \frac{4}{36} + \frac{6}{36} + \frac{4}{36} + \frac{2}{36} = \frac{18}{36} = \frac{1}{2} \\ P(3 \leq X \leq 9) &= P(X = 3, 4, 5, 6, 7, 8 \text{ or } 9) \\ &= P(X = 3) + P(X = 4) + \dots + P(X = 9) \\ &= \frac{2}{36} + \frac{3}{36} + \dots + \frac{4}{36} = \frac{29}{36}. \end{aligned}$$

**Example 8 :** The probability mass function of a random variable  $X$  is zero except at the points  $X = 0, 1, 2$ . At these points it has the values  $P(0) = 3c^2$ ,  $P(1) = 4c - 10c^2$ ,  $P(2) = 5c - 1$ .

(i) Determine  $c$ , (ii) Find  $P(X < 1)$ ,  $P(1 < X \leq 2)$ ,  $P(0 < X \leq 2)$ . (M.U. 2001)

$$\begin{aligned} \text{Sol. : Since } \sum p_i = 1, \text{ we have, } P(0) + P(1) + P(2) &= 1. \\ \therefore 3c^2 - 10c^2 + 4c + 5c - 1 &= 1 \quad \therefore 3c^2 - 10c^2 + 9c - 2 = 0 \\ (3c - 1)(c - 2)(c - 1) &= 0 \quad \therefore c = 1/3 \end{aligned}$$

(The other values are not admissible. Why?)

$$\begin{aligned} \therefore \text{The probability distribution is} \quad &\begin{array}{c|ccc} X & 0 & 1 & 2 \\ \hline P(X = x) & 1/9 & 2/9 & 2/3 \end{array} \\ \therefore P(X < 1) = P(X = 0) &= \frac{1}{9}; \quad P(1 < X \leq 2) = P(X = 2) = \frac{2}{3}; \\ P(0 < X \leq 2) = P(X = 1) + P(X = 2) &= \frac{2}{9} + \frac{2}{3} = \frac{8}{9}. \end{aligned}$$

**Example 9 :** A random variable  $X$  has the following probability distribution

$$\begin{array}{ll} X & : 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \\ P(X = x) & : 0 \ k \ 2k \ 2k \ 3k \ k^2 \ 2k^2 \ 7k^2 + k \end{array}$$

(i) Find  $k$ , (ii)  $P\left(\frac{1.5 < X < 4.5}{X > 2}\right)$ , (iii) The smallest value of  $\lambda$  for which  $P(X \leq \lambda) > \frac{1}{2}$ .

**Sol. :** (i) Since  $\sum p(x) = 1$ , we get

$$\begin{aligned} 10k^2 + 9k + 1 &= 0 \\ \therefore 10k^2 + 10k - k - 1 &= 0 \quad \therefore 10k(k+1) - 1(k+1) = 0 \\ \therefore (10k-1)(k+1) &= 0 \quad \therefore k = 1/10. \quad k \text{ cannot be } -1. \end{aligned}$$

∴ The probability distribution of  $X$  is

$$\begin{array}{ll} X & : 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \\ P(X = x) & : 0 \ 1/10 \ 2/10 \ 2/10 \ 3/10 \ 1/100 \ 2/100 \ 17/100 \end{array}$$

$$\begin{aligned} \text{(ii)} \quad \text{Now, } P(A/B) &= \frac{P(A \cap B)}{P(B)} \\ \therefore P\left(\frac{1.5 < X < 4.5}{X > 2}\right) &= \frac{P[(1.5 < X < 4.5) \cap (X > 2)]}{P(X > 2)} = \frac{P(2 < X < 4.5)}{P(X > 2)} \\ &= \frac{P(X = 3, 4)}{P(X = 3, 4, 5, 6, 7)} = \frac{5/10}{70/100} = \frac{5}{7}. \end{aligned}$$

Now from the table we find that

$$\begin{aligned} P(X \leq 3) &= P(X = 0) + P(X = 1) + P(X = 2) + P(X = 3) \\ &= 0 + \frac{1}{10} + \frac{2}{10} + \frac{2}{10} = \frac{5}{10} = \frac{1}{2}. \end{aligned}$$

Hence,  $P(X \leq 4) = \frac{8}{10} > \frac{1}{2}$ . Hence,  $\lambda = 4$ .

**Example 10 :** An urn contains 4 white and 3 red balls. Find the probability distribution of the number of red balls in three draws made successively with replacement from the urn. (M.U. 2007)

**Sol. :** We get the following probabilities,

No. of red balls	Probability
0	$\frac{4}{7} \cdot \frac{4}{7} \cdot \frac{4}{7}$
1	$\begin{cases} \frac{3}{7} \cdot \frac{4}{7} \cdot \frac{4}{7} \\ \frac{4}{7} \cdot \frac{3}{7} \cdot \frac{4}{7} \\ \frac{4}{7} \cdot \frac{4}{7} \cdot \frac{3}{7} \end{cases}$
2	$\begin{cases} \frac{3}{7} \cdot \frac{3}{7} \cdot \frac{4}{7} \\ \frac{3}{7} \cdot \frac{4}{7} \cdot \frac{3}{7} \\ \frac{4}{7} \cdot \frac{3}{7} \cdot \frac{3}{7} \end{cases}$
3	$\frac{3}{7} \cdot \frac{3}{7} \cdot \frac{3}{7}$

∴ Probability distribution is

$X$	0	1	2	3	Total
$p(x)$	64/343	144/343	108/343	27/343	1

**Example 11 :** A random variable  $X$  has the following probability function :

$$\begin{array}{ll} X & : 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \\ P(X = x) & : k \ 2k \ 3k \ k^2 \ k^2 + k \ 2k^2 \ 4k^2 \end{array}$$

Find (i)  $k$ , (ii)  $P(X < 5)$ , (iii)  $P(X > 5)$ , (iv)  $P\left(\frac{X < 5}{2 < X \leq 6}\right)$ , (v)  $P\left(\frac{X = 4}{3 \leq X \leq 5}\right)$ .

Sol.: Since  $\sum p(x_i) = 1$ ,

$$k + 2k + 3k + k^2 + k^2 + k + 2k^2 + 4k^2 = 1$$

$$\therefore 8k^2 + 7k - 1 = 0 \quad \therefore (8k - 1)(k + 1) = 0$$

$$\therefore k = 1/8 \quad \text{or} \quad k = -1 \text{ which is impossible (why?)}$$

Thus, we have the following probability distribution.

$X$	: 1	2	3	4	5	6	7
$P(X=x)$	: 1/8	2/8	3/8	1/64	9/64	2/64	4/64

$$\begin{aligned} \text{(i)} \quad P(X < 5) &= P(X=1, 2, 3, 4) \\ &= P(X=1) + P(X=2) + P(X=3) + P(X=4) \\ &= \frac{1}{8} + \frac{2}{8} + \frac{3}{8} + \frac{1}{64} = \frac{49}{64}. \end{aligned}$$

$$\begin{aligned} \text{(ii)} \quad P(X > 5) &= P(X=6, 7) = P(X=6) + P(X=7) \\ &= \frac{2}{64} + \frac{4}{64} = \frac{6}{64} = \frac{3}{32}. \end{aligned}$$

$$\begin{aligned} \text{(iii)} \quad P\left(\frac{X < 5}{2 < X \leq 6}\right) &= \frac{P(X < 5 \cap 2 < X \leq 6)}{P(2 < X \leq 6)} = \frac{P(2 < X < 5)}{P(2 < X \leq 6)} \\ &= \frac{P(X=3, 4)}{P(X=3, 4, 5, 6)} = \frac{25/64}{36/64} = \frac{25}{36}. \end{aligned}$$

$$\begin{aligned} \text{(iv)} \quad P\left(\frac{X=4}{3 \leq X \leq 5}\right) &= \frac{P(X=4 \cap 3 \leq X \leq 5)}{P(3 \leq X \leq 5)} \\ &= \frac{P(X=4)}{P(X=3, 4, 5)} = \frac{1/64}{34/64} = \frac{1}{64}. \end{aligned}$$

**Example 12:** The probability of a man hitting the target is  $1/4$ . How many times must he fire so that the probability of his hitting the target at least once is greater than  $2/3$ ? (M.U. 2016)

Sol.: We are given that the probability of hitting the target  $p = 1/4$ .

$$\text{Probability of not hitting the target, } q = 1 - \frac{1}{4} = \frac{3}{4}.$$

$\therefore$  Probability of not hitting the target in  $n$  trials

$$= \left(\frac{3}{4}\right)^n \cdot \dots \cdot (n \text{ times}) = \left(\frac{3}{4}\right)^n$$

$\therefore$  Probability of hitting the target at least once in  $n$  trials

$$= 1 - \left(\frac{3}{4}\right)^n$$

We want this probability to be greater  $2/3$ .

$$\therefore 1 - \left(\frac{3}{4}\right)^n > \frac{2}{3} \quad \therefore 1 - \left(\frac{2}{3}\right)^n > \left(\frac{3}{4}\right)^n$$

$$\therefore \frac{1}{3} > \left(\frac{3}{4}\right)^n \quad \therefore \left(\frac{3}{4}\right)^n < \frac{1}{3}$$

Taking logarithms of both sides

$$n(\log 3 - \log 4) < -\log 3$$

$$\therefore n(0.4771 - 0.6021) < -\log 3$$

$$\therefore n > \frac{0.4771}{0.1250} = 3.81 \quad \therefore n > 4$$

$\therefore$  He must fire at least 4 times, so that he will hit the target at least once, with probability of success greater  $2/3$ .

### EXERCISE - I

1. If  $P(X=x) = x/25$ ,  $x = 1, 3, 5, 7, 9$ , find  $P(X=1 \text{ or } 3)$  and  $P(4 < X < 8)$ .

[Ans.: (i) 4/25, (ii) 12/25]

2. Verify whether the following functions can be considered as p.m.f. and if so find  $P(X=1 \text{ or } 3)$ . Give reasons.

$$\text{(i)} \quad P(X=x) = \frac{1}{5}, \quad x = 0, 1, 2, 3, 4.$$

$$\text{(ii)} \quad P(X=x) = \frac{x^2+1}{18}, \quad x = 0, 1, 2, 3.$$

$$\text{(iii)} \quad P(X=x) = \frac{x^2-2}{8}, \quad x = 1, 2, 3.$$

$$\text{(iv)} \quad P(X=x) = \frac{2x+1}{18}, \quad x = 0, 1, 2, 3.$$

[Ans.: (i) Yes, 2/5; (ii) Yes, 2/3; (iii) No; (iv) No]

3. If the p.m.f.  $P(X=x)$  of a discrete random variate which assumes values  $x_1, x_2, x_3$  such that  $P(x_1) = 2P(x_2) = 3P(x_3)$ , obtain the probability distribution of  $X$ .

[Ans.: (i)  $P(x_1) = 2/11$ , (ii)  $P(x_2) = 3/11$ , (iii)  $P(x_3) = 6/11$ ]

4. Presuming the daily demand to be independent, find the probability that over a two-days period the number of requests at a service station will be (i) 9, (ii) 10, if the past record show that the demand was 4, 5 or 6 with probabilities 0.50, 0.40 or 0.10 respectively.

(Hint: The event can occur as (i) (4, 5), (5, 4); (ii) (4, 6), (5, 4), (5, 5).)

[Ans.: (i) 0.40, (ii) 0.26]

5. Find the probability distribution and the probability mass function of the number of points obtained when a fair die is tossed.

[Ans.:  $P(X=x) = 1/6$ ,  $x = 1, 2, 3, 4, 5, 6$ ]

6. Find the probability distribution and the p.m.f. of the number of heads obtained when an unbiased coin is tossed three times.

[Ans.:  $P(X=x) = \frac{3C_x}{2^3}$ ,  $x = 0, 1, 2, 3$ ]

7. The probability density function of a random variable  $X$  is

$X$	0	1	2	3	4	5	6
$P(X=x)$	$k$	$3k$	$5k$	$7k$	$9k$	$11k$	$13k$

Find  $P(X < 4)$ ,  $P(3 < X \leq 6)$ .

(M.U. 2001, 05, 10, 15)

8. A random variable  $X$  has the following probability function

$X$	1	2	3	4	5	6	7
$P(X=x)$	$k$	$2k$	$3k$	$k^2$	$k^2+k$	$2k^2$	$4k^2$

Find (i)  $k$ , (ii)  $P(X < 5)$ , (iii)  $P(X > 5)$ , (iv)  $P(0 \leq X \leq 5)$ .

[Ans. : (i)  $k = 1/8$ , (ii)  $49/64$ , (iii)  $3/32$ , (iv)  $29/32$ ]

9. A discrete random variable  $X$  has the following probability distribution

$X$	-2	-1	0	1	2	3
$P(X=x)$	0.1	$k$	0.2	$2k$	0.3	$3k$

Find (i)  $k$ , (ii)  $P(X \geq 2)$ , (iii)  $P(-2 < X < 2)$ .

[Ans. : (i)  $k = 1/15$ , (ii)  $1/2$ , (iii)  $2/5$ ] (M.U. 2009)

10. Given the following probability function of a discrete random variable  $X$

$X$	0	1	2	3	4	5	6	7
$P(X=x)$	0	$c$	$2c$	$2c$	$3c$	$c^2$	$2c^2$	$7c^2 + c$

(i) Find  $c$ , (ii) Find  $P(X \geq 6)$ , (iii)  $P(X < 6)$ , (iv) Find  $k$  if,  $P(X \leq k) > 1/2$ , where  $k$  is a positive integer.  
(v)  $P(1.5 < X < 4.5 / X > 2)$ .

[Ans. : (i)  $c = 0.1$ , (ii)  $0.19$ , (iii)  $0.81$ , (iv)  $k = 4$ , (v)  $5/7$ ] (M.U. 1996, 2003, 05)

11. In the example 9 above, find

(i)  $P(-1 \leq X \leq 1 / -2 \leq X \leq 3)$ , (ii)  $P(X \leq 2 / 0 \leq X \leq 4)$ , (iii)  $P(X \leq 1 / X \leq 2)$ .

[Ans. : (i)  $\frac{1}{2}$ , (ii)  $\frac{19}{26}$ , (iii)  $\frac{15}{24}$ ] (M.U. 2009)

12. A random variable  $X$  takes values  $-2, -1, 0, 1, 2$  such that  $P(X > 0) = P(X = 0) = P(X < 0) = P(X = -2) = P(X = -1)$ ,  $P(X = 1) = P(X = 2)$ . Obtain the probability distribution of  $X$ .

Also find (i)  $P\left(\frac{-1 \leq X \leq 1}{-2 \leq X \leq 0}\right)$ , (ii)  $P\left(\frac{X=1}{0 \leq X \leq 2}\right)$ .

[Ans. :  $X : -2 \quad -1 \quad 0 \quad 1 \quad 2$

$P(X=x) : 1/6 \quad 1/6 \quad 1/3 \quad 1/6 \quad 1/6$

(i)  $4/5$ , (ii)  $1/8$ ] (M.U. 2009)

13. A random variable  $X$  takes values  $0, 1, 2, \dots, n$  with probabilities proportional to  ${}^n C_0, {}^n C_1, {}^n C_2, \dots, {}^n C_n$ . Find the proportionality constant.

(Hint:  $k[{}^n C_0 + {}^n C_1 + {}^n C_2 + \dots + {}^n C_n] = 1 \quad \therefore k \cdot 2^n = 1$ ) [Ans. :  $k = 2^{-n}$ ] (M.U. 2009)

14. A random variable  $X$  assumes four values with probabilities  $(1+3x)/4$ ,  $(1-x)/4$ ,  $(1+2x)/4$  and  $(1-4x)/4$ . For what value of  $x$  do these values represent the probability distribution of  $X$ ?

[Ans. :  $\sum p_i = 1$ . But  $\frac{1+3x}{4} \geq 0$  if  $x \geq -\frac{1}{3}$  and also  $\frac{1-4x}{4} \geq 0$  if  $x \leq \frac{1}{4}$

$$\therefore -\frac{1}{3} \leq x \leq \frac{1}{4}$$

15. The amount of bread  $X$  (in hundred kgs) that a certain bakery is able to sell in a day is a random variable with probability density function given by

$$f_X(x) = \begin{cases} Ax, & 0 < x < 5 \\ A(10-x), & 5 < x < 10 \\ 0, & \text{elsewhere} \end{cases}$$

Find (i)  $A$ , (ii) the probabilities of the events :  $B$ , the amount of bread sold in a day is more than 500 kgs,  $C$  : the amount of bread sold in a day is less than 500 kgs,  $D$  : the amount of bread sold in a day is between 250 kgs and 750 kgs. (iii) Are the events  $B$  and  $C$  exclusive ? (iv) Are the events  $B$  and  $D$  exclusive ? (M.U. 2009)

[Ans. : (i)  $A = 1/25$ , (ii)  $1/2, 1/2, 0.75$ , (iii) Yes, (iv) No]

#### 4. Distribution Function of a Discrete Random Variable $X$

Probability distribution of  $X$  gives us the probability  $p(x)$  that  $X$  will take a particular value  $x$ . Sometimes we need to know the probability that  $X$  will take a value less than or equal to a given value  $x$ . This probability is obtained by adding the probabilities of all values less than or equal to  $x$ .

Suppose,  $X$  is a discrete random variable taking values  $x_1, x_2, \dots, x_n$  with probabilities  $p(x_i)$ ,  $i = 1, 2, \dots, n$  such that

(i)  $p(x_i) \geq 0$  for all  $i$ ,

(ii)  $\sum p(x_i) = 1$  and consider the following table.

$X$	$x_1$	$x_2$	$x_3$	.....	$x_n$	.....
$F(x_i) = P(X = x_i)$	$p(x_1)$	$\sum_{i=1}^2 p(x_i)$	$\sum_{i=1}^3 p(x_i)$	.....	$\sum_{i=1}^n p(x_i)$	.....

The table states that

$$F(x_1) = P(a \leq X < x) = p(x_1)$$

$$F(x_2) = P(X \leq x_2) = p(a \leq X \leq x_1) + p(x_1 \leq X \leq x_2) \\ = p(x_1) + p(x_2)$$

$$F(x_3) = P(X \leq x_3) = p(a \leq X \leq x_1) + p(x_1 \leq X \leq x_2) + p(x_2 \leq X \leq x_3) \\ = p(x_1) + p(x_2) + p(x_3)$$

And so on.

The following graph shows this diagrammatically.

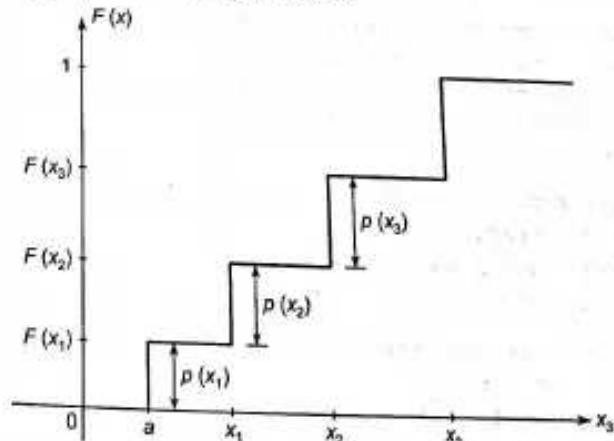


Fig. 6.6 : Graph of Distribution Function.

The function  $F$  is called the distribution function. We have more precise definition as follows.

(a) Definition

Let  $X$  be a discrete random variable taking values  $x_1, x_2, \dots$  such that  $x_1 < x_2 < x_3 \dots$  with probabilities  $p(x_i), p(x_2), \dots$  such that  $p(x_i) \geq 0$  for all  $i$  and  $\sum p(x_i) = 1$ .

Consider  $F$  defined by  $F(x) = P(X \leq x), i = 1, 2, 3, \dots$

$$\text{i.e., } F(x) = p(x_1) + p(x_2) + \dots + p(x_i)$$

then the function  $F$  is called the cumulative distribution function or simply distribution function and the set of pairs  $(x_i, F(x_i))$  is called the cumulative probability distribution.

Note ...

The distribution function is to the probability mass function as cumulative frequency distribution is to frequency distribution.

(b) Important Properties of Distribution function

The distribution function  $F$  of a random variable  $X$  has the following important properties.

$$1. 0 \leq F(x) \leq 1$$

Proof : Since,  $F(x_1) = p(x_1), F(x_2) = p(x_1) + p(x_2)$

$$\dots F(x_n) = p(x_1) + p(x_2) + \dots + p(x_n)$$

and  $0 \leq p(x_i) \leq 1$  for every  $i$  and  $\sum p(x_i) = 1$ , it is clear that  $0 \leq F(x) \leq 1$ .

$$2. F(x) = 0 \text{ for } x < a \text{ and } F(x) = 1 \text{ for } x > b \quad \text{where } a < x_1 < x_2 < \dots < x_n < b.$$

Proof : If  $x < a$  where  $a < x_1$ ,  $p(x) = 0$  and hence,  $F(x) = 0$  for  $x < a$ .

$$\text{If } x > b \text{ then } F(x) = p(x_1) + p(x_2) + \dots + p(x_n) = 1.$$

3.  $F(x)$  is a step function

Proof : By definition,  $F(x_1) = F(X < x_1) = p(x_1)$

$$F(x_2) = F(X < x_2) = p(x_1) + p(x_2)$$

i.e.  $F(X)$  has the same value  $p(x_1)$  for  $x_1 \leq x \leq x_2$ .

and the same value  $p(x_1) + p(x_2)$  for  $x_2 \leq x \leq x_3 \dots$

Hence, the graph of  $F(x)$  is made up of horizontal line segments taking "jumps" at the possible values  $x_i$  of  $X$ . The jump is of magnitude  $p(x_i) = P(X = x_i)$ .

Hence,  $F(x)$  is a step functions.

**Example 1 :** A random variable  $X$  has the probability function given below :

$$f(x) = k \text{ if } x = 0; f(x) = 2k \text{ if } x = 1;$$

$$f(x) = 3k \text{ if } x = 2; f(x) = 0 \text{ otherwise.}$$

(i) Determine the value of  $k$ , (ii) Evaluate  $P(X < 2), P(X \leq 2), P(0 < X < 2)$ , (iii) Obtain the distribution function.

**Sol. :** The probability distribution can be tabulated as

$X$	0	1	2
$p(x)$	$k$	$2k$	$3k$

(i) Since  $\sum p_i = 1$ ,  $k + 2k + 3k = 1 \therefore k = 1/6$ .

$$\begin{aligned} \text{(ii)} \quad P(X < 2) &= P(X = 0) + P(X = 1) = k + 2k = 3/6 = 1/2 \\ P(X \leq 2) &= P(X = 0) + P(X = 1) + P(X = 2) = 6k = 1. \\ P(0 < X < 2) &= P(X = 1) = 2k = 1/3. \end{aligned}$$

(iii) Distribution function of  $X$  is

$X$	0	1	2
$F(x)$	1/6	1/2	1

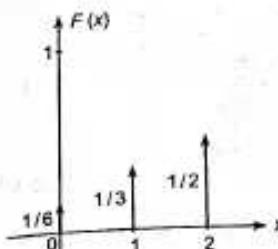


Fig. 6.7 (a)  
Probability Density Function.

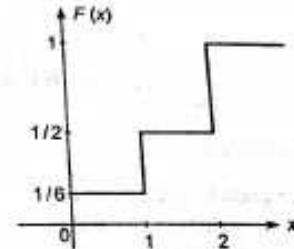


Fig. 6.7 (b)  
Distribution Function.

### EXERCISE - II

1. A random variable takes values 1, 2, 3, 4 such that  $2P(X = 1) = 3P(X = 2) = P(X = 3) = 5P(X = 4)$ . Find the probability distribution and the cumulative distribution function. (M.U. 2004)

[Ans. :	$X$	1	2	3	4
	$P(x)$	15/61	10/61	30/61	6/61
	$F(x)$	15/61	25/61	55/61	1

2. A shipment of 8 computers contains 3 that are defective. If a college makes a random purchase of 2 of these computers, find the probability distribution of the defective computers. Find also distribution function. (M.U. 2005)

[Ans. :	$X$	0	1	2
	$P(x)$	10/28	15/28	3/28
	$F(x)$	10/28	25/28	1

3. The probability density function of a random variable  $X$  is

$X$	:	0	1	2	3	4	5	6
$P(X = x)$	:	$k$	$3k$	$5k$	$7k$	$9k$	$11k$	$13k$

Find  $P(X < 4)$ ,  $P(3 < X \leq 6)$ .

[Ans. :  $k = 1/49, 16/49, 33/49$ ]

### 5. Continuous Random Variable

**Definition :** A random variable is called a **continuous random variable** if it takes all values between an interval  $(a, b)$ .

For example, age, height, weight are continuous random variables.

### 6. Probability Density Function of A Continuous Random Variable

Let  $y = f(x)$  be a continuous function of  $x$  such that the area  $f(x) \delta x$  represents the probability that  $X$  will lie in the interval  $(x, x + \delta x)$ . Symbolically,

$$P(x \leq X \leq x + \delta x) = f_x(x) \delta x$$

where,  $f_x(x)$  denotes the value of  $f(x)$  at  $x$ .

The adjoining figure denotes the curve  $y = f(x)$  and the area under the curve in the interval  $(x, x + \delta x)$ . The function satisfying certain conditions giving the probability that  $x$  will lie between certain limits is called **probability density function**, or simply **density function** of a continuous random variable  $X$  and is abbreviated as **p.d.f.** The curve given by  $y = f(x)$  is called the **probability density curve** or simply **probability curve**. The expression  $f(x) dx$  is usually denoted by  $df(x)$  and is known as **probability differential**.

**Definition :** A continuous function  $y = f(x)$  such that

(i)  $f(x)$  is integrable, (ii)  $f(x) \geq 0$

(iii)  $\int_a^b f(x) dx = 1$  if  $X$  lies in  $[a, b]$  and

(iv)  $\int_a^b f(x) dx = P(\alpha \leq X \leq \beta)$  where  $a < \alpha < \beta < b$

is called **probability density function** of a continuous random variable  $X$ .

Thus, for a continuous random variable  $X$ ,

$$P(\alpha \leq X \leq \beta) = \int_a^b f(x) dx$$

Clearly  $\int_a^b f(x) dx$  represents the area under the curve  $y = f(x)$ , the  $x$ -axis and the ordinates at  $x = \alpha$  and  $x = \beta$ . Further since, the total probability is one, if  $X$  lies in the interval  $[a, b]$  then  $\int_a^b f(x) dx = 1$ . For a continuous random variable  $X$  the range may be finite  $[a, b]$  or infinite  $[-\infty, \infty]$ .

#### Properties of Probability Density Function

The probability density function  $f(x)$  has the following properties.

(i)  $f(x) \geq 0, -\infty < x < \infty$  (i.e. the curve  $y = f(x)$  lies above the  $x$ -axis in the first and second quadrants only)

(ii)  $\int_{-\infty}^{\infty} f(x) dx = 1$  (i.e. the total area under the curve and the  $x$ -axis is one.)

(iii) The probability that  $\alpha \leq X \leq \beta$  is given by  $P(\alpha \leq X \leq \beta) = \int_a^b f(x) dx$ .

#### Notes ...

1. The property (1) and the property (2) can be used to verify whether a given function  $f(x)$  can be a probability density function.

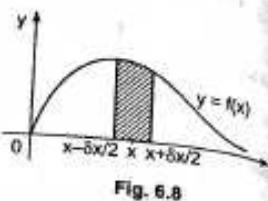


Fig. 6.8

2. You know that for a discrete random variable the probability at  $X = c$  may not be zero. But, in a continuous random variable  $P(X = c)$  is always zero because  $P(X = c) = \int_c^c f(x) dx$  and this definite integral is zero. Hence, for a continuous random variable  $X$ ,

$$P(\alpha \leq X \leq \beta) = P(\alpha < X < \beta) = P(\alpha \leq X \leq \beta) = P(\alpha < X < \beta)$$

In other words we may include or may not include the end-points in the interval.

3. Any function  $f(x)$  of a real variable  $x$  can be a probability density function if it satisfies the first two properties given above viz.  $f(x)$  is non-negative for all values of  $x$  and  $\int_{-\infty}^{\infty} f(x) dx = 1$ .

Sometimes  $\int_{-\infty}^{\infty} f(x) dx$  is not equal to 1 but  $\int_{-\infty}^{\infty} k f(x) dx = 1$  for some value of  $k$ .

In such cases  $k$  is called the **normalising factor** or **normalisation constant**.

**Example 1 :** Find the normalising factor,  $k$  if the following function is a probability density function

$$f(x) = \begin{cases} k(1-x^2) & 0 < x < 1 \\ 0 & \text{otherwise} \end{cases}$$

Also find  $P(0.1 < X < 0.2)$  and  $P(X > 0.5)$ .

Sol.: Since  $0 < x < 1$ ,  $f(x) \geq 0$  for all  $x$ .

$$\text{Now, } \int_0^1 f(x) dx = k \int_0^1 (1-x^2) dx = k \left[ x - \frac{x^3}{3} \right]_0^1 = k \frac{2}{3}$$

But this must be equal to 1.

$$\therefore \frac{2k}{3} = 1 \quad \therefore k = \frac{3}{2}$$

$$\begin{aligned} \text{(i)} \quad P(0.1 < X < 0.2) &= \int_{0.1}^{0.2} \frac{3}{2} (1-x^2) dx = \frac{3}{2} \left[ x - \frac{x^3}{3} \right]_{0.1}^{0.2} \\ &= \frac{3}{2} \left[ \left( 0.2 - \frac{(0.2)^3}{3} \right) - \left( 0.1 - \frac{(0.1)^3}{3} \right) \right] \\ &= \frac{3}{2} [0.0977] = 0.146 \end{aligned}$$

$$\begin{aligned} \text{(ii)} \quad P(X > 0.5) &= \int_{0.5}^1 \frac{3}{2} (1-x^2) dx = \frac{3}{2} \left[ x - \frac{x^3}{3} \right]_{0.5}^1 \\ &= \frac{3}{2} \left[ \left( 1 - \frac{1}{3} \right) - \left( 0.5 - \frac{(0.5)^3}{3} \right) \right] \\ &= \frac{3}{2} [0.667 - 0.458] = 0.313 \end{aligned}$$

**Example 2:** A continuous random variable  $X$  has the following probability law  
 $f(x) = kx^2, 0 \leq x \leq 2$

Determine  $k$  and find the probabilities that (i)  $0.2 \leq X \leq 0.5$ , (ii)  $X \geq 3/4$  given that  $X \geq 1/2$ .  
 Sol. : Since the total probability i.e. the total area is unity

$$\int_0^2 f(x) dx = \int_0^2 kx^2 dx = 1$$

$$k \left[ \frac{x^3}{3} \right]_0^2 = 1 \quad \therefore k \cdot \frac{8}{3} = 1 \quad \therefore k = \frac{3}{8}$$

$$(i) P(0.2 \leq X \leq 0.5) = \frac{3}{8} \int_{0.2}^{0.5} x^2 dx = \frac{3}{8} \left[ \frac{x^3}{3} \right]_{0.2}^{0.5} = \frac{1}{8} [0.5^3 - 0.2^3] = 0.0123$$

(ii) Let  $A = (X \geq 1/2)$ ,  $B = (X \geq 3/4)$

$$\therefore P(A) = P(X \geq 1/2) = \frac{3}{8} \int_{0.5}^2 x^2 dx = \frac{3}{8} \left[ \frac{x^3}{3} \right]_{0.5}^2 = \frac{1}{8} [2^3 - 0.5^3] = 0.984$$

$$P(B) = P(X \geq 3/4) = \frac{3}{8} \int_{0.75}^2 x^2 dx = \frac{3}{8} \left[ \frac{x^3}{3} \right]_{0.75}^2 = \frac{1}{8} [2^3 - 0.75^3] = 0.947$$

$$P(A \cap B) = P(B) = 0.947$$

$$\therefore P(B/A) = \frac{P(A \cap B)}{P(A)} = \frac{0.947}{0.984} = 0.96$$

**Example 3:** Let  $X$  be a continuous random variable with probability distribution

$$p(x) = \begin{cases} \frac{x}{6} + k & \text{if } 0 \leq x \leq 3 \\ 0 & \text{elsewhere} \end{cases}$$

Evaluate  $k$  and find  $P(1 \leq x \leq 2)$ .

Sol. : Since the total probability is one

$$\int_0^3 p(x) dx = \int_0^3 \left( \frac{x}{6} + k \right) dx = \left[ \frac{x^2}{12} + kx \right]_0^3 = \frac{3}{4} + 3k = 1$$

$$\therefore 3\left(\frac{1}{4} + k\right) = 1 \quad \therefore \frac{1}{4} + k = \frac{1}{3} \quad \therefore k = \frac{1}{3} - \frac{1}{4} = \frac{1}{12}$$

$$\therefore p(x) = \begin{cases} \frac{x}{6} + \frac{1}{12} & \text{if } 0 \leq x \leq 3 \\ 0 & \text{elsewhere} \end{cases}$$

**Example 4:** Let  $X$  be a continuous random variable with p.d.f.  $f(x) = kx(1-x), 0 \leq x \leq 1$ . Find  $k$  and determine a number  $b$  such that  $P(X \leq b) = P(X \geq b)$ .  
 Sol. : Since  $\int_a^b f(x) dx = 1$ , we have

$$\therefore P(1 \leq x \leq 2) = \int_1^2 \left( \frac{x}{6} + \frac{1}{12} \right) dx = \left[ \frac{x^2}{12} + \frac{x}{12} \right]_1^2 = \frac{1}{12} [(4+2) - (1+1)] = \frac{1}{12}(4) = \frac{1}{3}$$

**Example 4:** Let  $X$  be a continuous random variable with p.d.f.  $f(x) = kx(1-x), 0 \leq x \leq 1$ . Find  $k$  and determine a number  $b$  such that  $P(X \leq b) = P(X \geq b)$ .  
 (M.U. 2003, 11, 15)

Sol. : Since  $\int_a^b f(x) dx = 1$ , we have

$$k \int_0^1 (x - x^2) dx = 1 \quad \therefore k \left[ \frac{x^2}{2} - \frac{x^3}{3} \right]_0^1 = 1$$

$$\therefore k \left[ \frac{1}{2} - \frac{1}{3} \right] = 1 \quad \therefore k = 6.$$

Since, the total probability is 1 and  $P(x \leq b) = P(x \geq b)$ ,  $P(x \leq b) = 1/2$ .

$$\therefore \int_0^b f(x) dx = \frac{1}{2}$$

$$\therefore 6 \int_0^b (x - x^2) dx = \frac{1}{2} \quad \therefore \left[ \frac{x^2}{2} - \frac{x^3}{3} \right]_0^b = \frac{1}{12}$$

$$\therefore \frac{b^2}{2} - \frac{b^3}{3} = \frac{1}{12} \quad \therefore 6b^2 - 4b^3 = 1 \quad \therefore 4b^3 - 6b^2 + 1 = 0$$

$$\therefore 4b^3 - 2b^2 - 4b^2 + 2b + 2b - 1 = 0$$

$$\therefore (2b-1)(2b^2-2b+1) = 0 \quad \therefore b = 1/2.$$

**Example 5:** The probability that a person will die in the time interval  $(t_1, t_2)$  is given by

$$P(t_1 \leq t \leq t_2) = \int_{t_1}^{t_2} f(t) dt$$

$$\text{where, } f(t) = \begin{cases} 3 \times 10^{-9} (100t - t^2)^2, & 0 < t < 100 \\ 0, & \text{elsewhere.} \end{cases}$$

Find (i) the probability that Mr. X will die between the ages 60 and 70. (ii) the probability that he will die between the ages 60 and 70, given that he has survived upto age 60.  
 (M.U. 2005)

$$\begin{aligned} \text{Sol. : (i) } P(60 \leq t \leq 70) &= \int_{60}^{70} 3 \times 10^{-9} (100t - t^2)^2 dt \\ &= 3 \times 10^{-9} \int_{60}^{70} (100^2 t^2 - 200t^3 + t^4) dt \\ &= 3 \times 10^{-9} \left[ 100^2 \frac{t^3}{3} - 200 \frac{t^4}{4} + \frac{t^5}{5} \right]_{60}^{70} \\ &= 3 \times 10^{-9} [27.89 \times 10^8 - 22.75 \times 10^8] \\ &= 0.1542. \end{aligned}$$

$$(ii) P\left(\frac{60 \leq T \leq 70}{T \geq 60}\right) = \frac{P(60 \leq t \leq 70 \cap t \geq 60)}{P(t \geq 60)} = \frac{P(60 \leq t \leq 70)}{P(60 \leq t \leq 100)}$$

$$= \frac{\int_{60}^{70} f(t) dt}{\int_{60}^{100} f(t) dt} = \frac{0.1542}{0.3174} = 0.4858.$$

**EXERCISE - III**

1. A function is defined as

$$f(x) = \begin{cases} 0 & \text{for } x < 2 \\ \frac{2x+3}{18} & \text{for } 2 \leq x \leq 4 \\ 0 & \text{for } x > 4 \end{cases}$$

Show that  $f(x)$  is a probability density function and find the probability that  $2 < x < 3$ .

(M.U. 2005) [Ans. : 5/18]

2. A random variable
- $X$
- has the probability density function

$$f(x) = \begin{cases} 2e^{-2x} & \text{for } x > 0 \\ 0 & \text{for } x \leq 0 \end{cases}$$

Find  $P(1 \leq X \leq 3)$ ,  $P(X \geq 0.5)$ .

[Ans. : (i) 0.133, (ii) 0.38]

3. A continuous random variable
- $X$
- has the following probability density function

$$f(x) = \begin{cases} kx & 0 \leq x \leq 1 \\ k & 1 \leq x \leq 2 \\ 0 & \text{elsewhere} \end{cases}$$

Find (i) the value of  $k$ , (ii)  $P(x \leq 1.5)$ .[Ans. : (i)  $k = 2/3$ , (ii)  $2/3$ ]

4. A continuous random variable has the following probability density function.

$$f(x) = \begin{cases} (x/4) + k & 0 \leq x \leq 2 \\ 0 & \text{elsewhere} \end{cases}$$

Evaluate  $k$  and  $P(1 \leq X \leq 2)$ .[Ans. :  $k = 1/4$ ,  $5/8$ ]

5. Find the value of
- $k$
- such that the following will be the probability density function. Find also
- $P(x \leq 1.5)$
- .

$$f(x) = \begin{cases} kx & 0 \leq x \leq 1 \\ k & 1 \leq x \leq 2 \\ k(3-x) & 2 \leq x \leq 3 \end{cases}$$

(M.U. 2003) [Ans. :  $k = \frac{1}{2}, \frac{1}{2}$ ]**7. Continuous Distribution Function**

Probability distribution of  $X$  or the probability density function of  $X$  helps us to find the probability that  $X$  will be within a given interval  $[a, b]$  i.e.  $P(a \leq X \leq b) = \int_a^b f(x) dx$ , other conditions being satisfied.

However, sometimes we need to know that probability that  $X$  will be less than a given value  $x$ . For a continuous random variable  $X$ , this probability is obtained by integrating  $f(x)$  from  $-\infty$  (or the lower limit of the interval) to  $x$ . The function so obtained is called **distribution function**.

**Definition :** If  $X$  is a continuous random variable  $X$ , having the probability density function  $f(x)$  then the function

$$F(x) = P(X \leq x) = \int_{-\infty}^x f(t) dt, \quad -\infty < x < \infty$$

is called **distribution function** or **cumulative distribution function** of the random variable  $X$ .**Some Important Properties of Distribution Function  $F(x)$  of a Continuous Random Variable**

1. The function
- $F(x)$
- is defined for every real number
- $x$
- .

2. Since
- $F(x)$
- denotes probability and probability of
- $X$
- lies between 0 and 1,

$$0 \leq F(x) \leq 1.$$

- 3.
- $F(x)$
- is a non-decreasing function which means if
- $x_1 \leq x_2$
- , then
- $F(x_1) \leq F(x_2)$
- .

4. The derivative of
- $F(x)$
- i.e.
- $F'(x)$
- exists at all points (except perhaps at a finite number of points) and is equal to the probability density function
- $f(x)$
- .

$$F'(x) = \frac{d}{dx} F(x) = f(x) \geq 0 \text{ provided the derivative exists.}$$

5. If
- $F(x)$
- is a distribution function of a continuous random variable then

$$P(a \leq X \leq b) = F(b) - F(a).$$

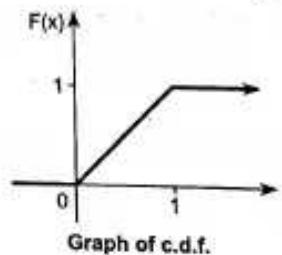
**Example 1 :** A continuous variable  $X$  has the following distribution function

$$F(x) = \begin{cases} 0, & x \leq 0 \\ x, & 0 \leq x \leq 1 \\ 1, & 1 \leq x \end{cases} \quad (1)$$

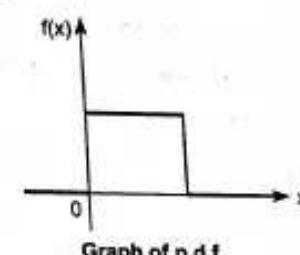
Find the probability density function and draw the graphs of both p.d.f. and c.d.f.

Sol : The p.d.f. is

$$f(x) = F'(x) = \begin{cases} 0 & x < 0 \\ 1 & 0 \leq x \leq 1 \\ 0 & 1 < x \end{cases}$$



Graph of c.d.f.



Graph of p.d.f.

Fig. 6.9

From the graph of  $F(x)$  we see that  $F(x)$  is continuous at all points including  $x = 0$  and  $x = 1$ .  $f(x)$  is obtained by differentiating  $F(x)$ .

**Example 2 :** For the distribution function given below, find p.d.f.

$$F(x) = \begin{cases} 0 & x < 0 \\ 1 - e^{-x/4} & x \geq 0 \end{cases}$$

Also find the probabilities :  $P(X \leq 4)$ ,  $P(X \geq 8)$ ,  $P(4 \leq X \leq 8)$ .

Sol. :  $F(x)$  satisfies all the conditions of a distribution function. If  $f(x)$  is the corresponding probability density function

$$f(x) = F'(x) = \begin{cases} \frac{1}{4} e^{-x/4} & x \geq 0 \\ 0 & x < 0 \end{cases}$$

Now, we have to verify that  $\int_{-\infty}^{\infty} f(x) dx = 1$ .

$$\therefore \int_{-\infty}^0 f(x) dx + \int_0^{\infty} \frac{1}{4} e^{-x/4} dx = 0 + \int_0^{\infty} \frac{1}{4} e^{-x/4} dx = \frac{1}{4} \left[ \frac{e^{-x/4}}{-1/4} \right]_0^{\infty} = -[0 - 1] = 1$$

Hence,  $F(x)$  is a distribution function.

$$\text{Now, } P(X \leq 4) = F(4) = 1 - e^{-1} = 1 - \frac{1}{e} = \frac{e-1}{e}$$

$$P(X \geq 8) = 1 - P(X \leq 8) = 1 - F(8)$$

$$= 1 - [1 - e^{-2}] = e^{-2} = 1/e^2$$

$$P(4 \leq X \leq 8) = F(8) - F(4) = (1 - e^{-2}) - (1 - e^{-1}) = e^{-1} - e^{-2} = \frac{1}{e} - \frac{1}{e^2} = \frac{e-1}{e^2}$$

**Example 3 :** If  $f(x) = \begin{cases} x e^{-x^2/2} & x \geq 0 \\ 0 & x < 0 \end{cases}$

(i) Show that  $f(x)$  is a probability density function. (ii) Find its distribution function.

Sol. : If  $f(x)$  is a p.d.f., we must have  $f(x) \geq 0$  where  $x \geq 0$  and  $\int_0^{\infty} f(x) dx = 1$ .

Clearly  $f(x) = x e^{-x^2/2} \geq 0$  for  $x \geq 0$ .

$$\text{Now, } \int_0^{\infty} x e^{-x^2/2} dx = \int_0^{\infty} e^{-t} dt \quad [t = x^2/2] \\ = -[e^{-t}]_0^{\infty} = -[0 - 1] = 1$$

$\therefore f(x)$  is a probability density function.

Now, its distribution function is given by

$$F(x) = \int_0^x f(t) dt = \int_0^x t e^{-t^2/2} dt = -\left[ e^{-t^2/2} \right]_0^x \quad [\text{As above}] \\ = -\left[ e^{-x^2/2} - 1 \right] = 1 - e^{-x^2/2}, \quad x \geq 0.$$

**EXERCISE - IV**

1. The distribution function of a random variable  $X$  is given by

$$F(x) = \begin{cases} 0 & x < -1 \\ \frac{x+1}{4} & -1 \leq x \leq 3 \\ 1 & x > 3 \end{cases}$$

Find the probability density function. Draw the graphs of both p.d.f. and c.d.f.

2. The c.d.f. of a continuous random variable  $X$  is given by

$$F(x) = \begin{cases} 0 & x < 0 \\ x^2 & 0 \leq x \leq 1 \\ 1 & x > 1 \end{cases}$$

Find the p.d.f. Draw the graphs of both p.d.f. and c.d.f.

$$\text{Also find } P\left(\frac{1}{2} \leq X \leq \frac{4}{5}\right).$$

[Ans. : 0.195]

3. Find the distribution functions corresponding to the following probability density functions.

$$(i) f(x) = \begin{cases} \frac{1}{2} x^2 e^{-x} & 0 \leq x < \infty \\ 0 & \text{otherwise} \end{cases} \quad (ii) f(x) = \begin{cases} x & 0 \leq x \leq 1 \\ 2-x & 1 \leq x \leq 2 \\ 0 & \text{otherwise} \end{cases}$$

$$(iii) f(x) = \begin{cases} \lambda(x-1)^4 & 1 \leq x \leq 3, \lambda > 0 \\ 0 & \text{otherwise} \end{cases}$$

$$[\text{Ans. : (i)} \quad F(x) = \begin{cases} 1 - e^{-x} \left(1 + x + \frac{x^2}{2}\right), & x \geq 0 \\ 0, & \text{otherwise} \end{cases}$$

$$(ii) F(x) = \begin{cases} 0 & x < 0 \\ x^2/2 & 0 \leq x \leq 1 \\ 2x - 0.5x^2 - 1 & 1 \leq x \leq 2 \\ 1 & x > 2 \end{cases}$$

$$(iii) \lambda = \frac{5}{32}; \quad F(x) = \begin{cases} 0 & x \leq 1 \\ \frac{(x-1)^5}{32} & 1 \leq x \leq 3 \\ 1 & x \geq 3 \end{cases}$$

4. A continuous random variable  $X$  has the following probability density function

$$f(x) = \frac{a}{x^5}, \quad 2 \leq x \leq 10$$

Determine the constant  $a$ , distribution function of  $X$  and find the probability of the event  $4 \leq x \leq 7$ .

$$[\text{Ans. : (i)} \quad a = \frac{2500}{39}, \quad (\text{ii}) \quad \frac{625}{39} \left[ \frac{1}{16} - \frac{1}{x^4} \right], \quad (\text{iii}) \quad 0.056]$$

5. The distribution function of a random variable  $X$  is given by
- $$F(x) = \begin{cases} 1 - (1+x)e^{-x}, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

Find the probability density function and find  $P(0 \leq X \leq 1)$ .

$$[ \text{Ans. : (i) } f(x) = xe^{-x}, \text{ (ii) } P(0 \leq X \leq 1) = F(1) - F(0) = \frac{e^{-2}}{e} ]$$

### 8. Expectation

Suppose two coins are tossed twenty times. Let  $X$  be the number of heads obtained in a toss  $X$  then, takes values 0, 1 and 2. Suppose further that no heads, one head and two heads were obtained 4, 10, 6 times respectively. Then, the average number of heads per toss

$$= \frac{4(0) + 10(1) + 6(2)}{6 + 10 + 4} = 1.1$$

This is the average value and is not necessarily a possible outcome of the toss.

The ratios 4/20, 10/20, 6/20 of 0, 1, 2 heads to the total number of tosses are the relative frequencies of  $X = 0, 1, 2$ . If the experiment is repeated very large number of times, we know that, these relative frequencies tend to the probabilities 1/4, 1/2, 1/4 of 0, 1, 2 heads because in the toss of two coins we have the following.

Sample space :	HH	$\underbrace{HT, TH}_{1/2}$	TT
Probability :	1/4	1/2	1/4

The average calculated with probabilities in place of relative frequencies above is called expected value or mathematical expectation and is denoted by  $E(X)$ . Thus,

$$E(X) = \frac{1}{4}(0) + \frac{1}{2}(1) + \frac{1}{4}(2) = 1$$

$$\begin{aligned} E(X) &= \text{sum of the products of the values and their probabilities} \\ &= p_1 x_1 + p_2 x_2 + p_3 x_3 + \dots \end{aligned}$$

This means, a person who throws two coins over and over again will get one head per toss on the average. This suggests us that the expected value of  $X$  can be obtained by multiplying the values of  $X$  by their respective probabilities and taking the sum. This leads us to the following definition of expectation of a discrete random variable  $X$ .

### 9. Expectation of a Random Variable

(a) Definition : If a discrete random variable  $X$  assumes values  $x_1, x_2, \dots, x_n, \dots$  with probabilities  $p_1, p_2, \dots, p_n, \dots$  respectively then the mathematical expectation of  $X$  denoted by  $E(X)$  (if it exists) is defined by

$$E(X) = p_1 x_1 + p_2 x_2 + \dots + p_n x_n + \dots$$

i.e.

$$E(X) = \sum p_i x_i \quad \text{where } \sum p_i = 1.$$

If  $\sum p_i x_i$  is absolutely convergent.

This value is also referred to as mean value of  $X$ . It is also denoted by  $\mu_1$ .  $\therefore \mu_1 = E(X)$ .

Notation : In this chapter we shall slightly deviate from our previous notation. Instead of denoting  $P(X = x)$  by  $p(x)$  we shall denote it simply by  $p$ . This will be found more convenient while dealing with expectations.

(b) Definition : Let  $X$  be a continuous random variable with probability density function  $f(x)$ . Then the mathematical expectation of  $X$ , denoted by  $E(X)$  (if it exists), is defined by

$$E(X) = \int_{-\infty}^{\infty} x \cdot f(x) dx$$

where,  $\int_{-\infty}^{\infty} f(x) dx = 1$

if the integral is absolutely convergent.

#### Notes ...

- If  $X$  assumes only a finite number of values then  $E(X) = \sum p_i x_i$  and can be considered as "weighted average" of the values  $x_1, x_2, \dots, x_n$  with weights  $p_1, p_2, \dots, p_n$ .
- If all values  $x_1, x_2, \dots, x_n$  are equiprobable i.e.  $p_1 = p_2 = \dots = p_n = 1/n$  then  $E(X) = (1/n) \sum x_i$  and can be seen to be simple arithmetic mean of the  $n$  values  $x_1, x_2, \dots, x_n$ .
- One should guard oneself from being misled by the term 'expectation'.  $E(X)$  does not give us the value of  $X$ , we can expect in a single trial. In the Example 4 below  $E(X) = 7/2$  is not even a possible value of  $X$  when a die is tossed.

$E(X)$  denotes mathematical expectation of  $X$  in the sense that if we toss a die for a fairly large number of times, observe the frequencies of the outcomes 1, 2, 3, 4, 5, 6 then the average of these values will be closer to  $7/2$  the more often the die were tossed.

- $E(X)$  is expressed in the same units as  $X$ .

#### 5. Expectation of a constant is constant

$$(i) \quad E(c) = \sum p_i c = c \sum p_i = c \quad [\because \sum p_i = 1]$$

$$(ii) \quad E(c) = \int_{-\infty}^{\infty} c f(x) dx = c \int_{-\infty}^{\infty} f(x) dx = c \quad [\because \int_{-\infty}^{\infty} f(x) dx = 1]$$

Example 1 : A fair coin is tossed 3 times. A person received  $\text{₹ } X^2$  if he gets  $X$  heads. Find his expectation.

Sol. : When a coin is tossed three times, the sample space is

HHH, HHT, HTH, HTT, THH, THT, TTH, TTT

The probability distribution of  $X$  is

$$\begin{array}{ll} X & : 0 \quad 1 \quad 2 \quad 3 \\ P(X=x) & : 1/8 \quad 3/8 \quad 3/8 \quad 1/8 \end{array}$$

Now,  $X^2$  takes the following values

$$\begin{array}{ll} X^2 & : 0 \quad 1 \quad 2 \quad 3 \\ P(X^2) & : 1/8 \quad 3/8 \quad 3/8 \quad 1/8 \end{array}$$

$$\begin{aligned} E(X^2) &= \sum p_i x_i^2 = \frac{1}{8} \times 0 + \frac{3}{8} \times 1 + \frac{3}{8} \times 4 + \frac{1}{8} \times 9 \\ &= \frac{3+12+9}{8} = \frac{24}{8} = 3 \text{ Rs.} \end{aligned}$$

Example 2 : There are 10 counters in a bag, 6 of which are worth 5 rupees each while the remaining 4 are of equal but unknown value. If the expectation of drawing a single counter at random is 4 rupees, find the unknown value.

(M.U. 2015)

Sol.: Let  $x$  be the value of the remaining 4 counters.

$$P(\text{of counter worth of } \text{₹} 5) = \frac{6}{10}$$

$$P(\text{of counter of unknown value}) = \frac{4}{10}$$

$$E(X) = \sum p_i x_i \quad \therefore 4 = \frac{6}{10} \cdot 5 + \frac{4}{10} \cdot x$$

$$\therefore 40 = 30 + 4x \quad \therefore 4x = 10 \quad \therefore x = \text{₹} 2.5.$$

**Example 3:** A fair coin is tossed till a head appears. What is the expectation of the number of tosses required? (M.U. 1996, 2010)

Sol.: Let  $X$  denote the order of the toss at which we get the first head. We have

Event	H	TH	TTH	TTTH	.....
$X$	1	2	3	4	.....
$P(X=x)$	$\frac{1}{2}$	$\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$	$\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$	$\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{16}$	.....

$$\therefore E(X) = \sum p_i x_i = 1\left(\frac{1}{2}\right) + 2\left(\frac{1}{4}\right) + 3\left(\frac{1}{8}\right) + 4\left(\frac{1}{16}\right) + \dots$$

$$\text{Let } S = \frac{1}{2} + 2 \cdot \frac{1}{4} + 3 \cdot \frac{1}{8} + 4 \cdot \frac{1}{16} + \dots$$

$$\frac{1}{2}S = \frac{1}{4} + 2 \cdot \frac{1}{8} + 3 \cdot \frac{1}{16} + \dots$$

$$\therefore S - \frac{1}{2}S = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots$$

$$\therefore \frac{1}{2}S = \frac{1}{2} \cdot \frac{1}{1-(1/2)} = 1 \quad \left[ \text{G.P. } S_n = \frac{a}{1-r} \right]$$

$$\therefore E(X) = 2.$$

**Example 4:** Find the expectation of (i) the sum, (ii) the product of the number of points on the throw of  $n$  dice.

(M.U. 2004, 06)

Sol.: Let  $X_i$  denote the number of points on the  $i$ th dice.

Then if  $S$  denotes the sum of the points of  $n$  dice then  $S = \sum_{i=1}^n X_i$ .

$$\text{Now, } E(X_i) = \sum p_i x_i = \frac{1}{6} + 1 + \frac{1}{6} \cdot 2 + \frac{1}{6} \cdot 3 + \dots + \frac{1}{6} \cdot 6$$

$$\therefore E(X_i) = \frac{1}{6}(1+2+3+4+5+6) = \frac{21}{6} = \frac{7}{2}$$

$$\therefore S = \sum_{i=1}^n X_i = n \cdot \frac{7}{2} = \frac{7n}{2}$$

If  $\pi$  denotes the product of the points

$$E(\pi) = E(X_1) \cdot E(X_2) \dots E(X_n) = \left(\frac{7}{2}\right) \cdot \left(\frac{7}{2}\right) \dots \left(\frac{7}{2}\right) = \left(\frac{7}{2}\right)^n.$$

**Example 5:** A box contains  $n$  tickets numbered 1, 2, ...,  $n$ . If  $m$  tickets are drawn at random from the box. What is the expectation of the sum of the numbers on the tickets drawn? (M.U. 2001)

Sol.: Let  $X_i$  denote the number on the  $i$ th ticket drawn.

$$\text{Then } S = X_1 + X_2 + \dots + X_m$$

$$\text{Now, } E(X_i) = \sum p_i x_i = \frac{1}{n} + \frac{1}{n} + \frac{1}{n} + \dots + \frac{1}{n} + n$$

$$= \frac{1}{n}(1+2+\dots+n) = \frac{1}{n} \cdot \frac{n(n+1)}{2} = \frac{n+1}{2}$$

$$\therefore E(S) = \sum_{i=1}^m E(X_i) = \frac{m(n+1)}{2}.$$

**Example 6:** Three urns contain respectively 3 green and 2 white balls, 5 green and 6 white balls, 2 green and 4 white balls. One ball is drawn from each urn. Find the expected number of white ball drawn. (M.U. 2007, 09)

Sol.: If  $X$  denotes the number of white balls drawn from an urn then the expectation of  $X$  is as follows:

$$E(X) = p_1 x_1 + p_2 x_2$$

$x$  takes two values.  $X = 1$  if white ball is drawn and  $X = 0$  if green ball is drawn.

$$\therefore \text{From first urn: } E(X_1) = 1 \cdot \frac{2}{5} + 0 \cdot \frac{3}{5} = \frac{2}{5}$$

$$\text{From second urn: } E(X_2) = 1 \cdot \frac{6}{11} + 0 \cdot \frac{5}{11} = \frac{6}{11}$$

$$E(X_3) = 1 \cdot \frac{4}{6} + 0 \cdot \frac{2}{6} = \frac{2}{3}$$

$$\therefore \text{The required expectation} = E(X_1) + E(X_2) + E(X_3)$$

$$= \frac{2}{5} + \frac{6}{11} + \frac{2}{3} = \frac{266}{165} = 1.61$$

**Example 7:** A box contains  $2^n$  tickets of which  ${}^n C_r$  tickets bear the number  $r$  ( $r = 0, 1, 2, \dots, n$ ). A group of  $m$  tickets is drawn. What is the expectation of the sum of their numbers?

Sol.: Let  $X_1, X_2, \dots, X_m$  be the variables denoting the number on the first, second, ...,  $m$ th ticket.

If  $S$  is the sum of the numbers on the tickets drawn then

$$S = \sum X_i \text{ and } E(S) = \sum E(X_i)$$

Now,  $X_i$  is a random variable which can take any one of the values 0, 1, 2, ...,  $n$  with probabilities  ${}^n C_0 / 2^n, {}^n C_1 / 2^n, \dots, {}^n C_n / 2^n$ .

$$\therefore E(X_i) = \sum p_i x_i$$

$$= \frac{1}{2^n} [0 \cdot {}^n C_0 + 1 \cdot {}^n C_1 + 2 \cdot {}^n C_2 + 3 \cdot {}^n C_3 + \dots + n \cdot {}^n C_n]$$

$$= \frac{1}{2^n} [1 + 2 \cdot \frac{n(n-1)}{2!} + 3 \cdot \frac{n(n-1)(n-2)}{3!} + \dots + n+1]$$

$$= \frac{n}{2^n} [1 + (n-1) + \frac{(n-1)(n-2)}{2!} + \dots + 1]$$

$$\therefore E(X_i) = \frac{n}{2^n} [1 + 1]^{n-1} = \frac{n}{2^n} \cdot 2^{n-1} = \frac{n}{2}.$$

$$\therefore E(S) = \sum E(X_i) = m \cdot \frac{n}{2} = \frac{mn}{2}.$$

**Cov. 1:** If two tickets are drawn then putting  $m = 2$ , we get

$$E(\text{Sum}) = 2 \cdot \frac{n}{2} = n.$$

**Example 8:** A box contains 'a' white balls and 'b' black balls. 'c' balls are drawn from the box at random. Find the expected value of the number of white balls.

**Sol.:** Let  $X_i$  be the variable denoting the result of the  $i$ th draw,

Let  $X_i = 1$  if  $i$ th ball drawn is white and  $X_i = 0$  if  $i$ th ball drawn is black.

Since, 'c' balls are drawn the sum of the white ball will be

$$S = X_1 + X_2 + \dots + X_c = \sum_{i=1}^c X_i$$

$$\text{Now, } P(X_i = 1) = P(\text{drawing a white ball}) = \frac{a}{a+b}$$

$$P(X_i = 0) = P(\text{drawing a black ball}) = \frac{b}{a+b}$$

$$E(X_i) = 1 \cdot P(X_i = 1) + 0 \cdot P(X_i = 0)$$

$$= 1 \cdot \frac{a}{a+b} + 0 \cdot \frac{b}{a+b} = \frac{a}{a+b}$$

$$\therefore E(S) = E(X_1) + E(X_2) + \dots + E(X_c)$$

$$= c \cdot \frac{a}{a+b} = \frac{ac}{a+b}.$$

**Example 9:** A die is thrown until a five is obtained, find the expectation of the number of throws.

**Sol.:** Probability of getting 5 in the first toss =  $1/6$ ,

Probability of getting 5 in the second =  $(5/6) \cdot (1/6)$ ,

Probability of getting 5 in third =  $(5/6) \cdot (5/6) \cdot (1/6)$  and so on,  
and  $X$  takes values 1, 2, 3, ...

$$E(X) = 1(1/6) + 2(5/6)(1/6) + 3(5/6)^2(1/6) + \dots$$

$$= (1/6)[1 + 2x + 3x^2 + \dots] \quad \text{where, } x = 5/6$$

$$= (1/6)(1-x)^{-2} = (1/6)[1 - (5/6)]^{-2}$$

$$= 6.$$

**Example 10:** A and B throw a fair die for a stake of ₹ 44, which is won by the player who throws 6 first. If A starts first, find their expectations.

**Sol.:** A can win the game, in the first throw or in the third throw or in the fifth throw and so on.

$$P(A \text{ winning}) = \frac{1}{6} + \left(\frac{5}{6}\right)\left(\frac{5}{6}\right) \cdot \frac{1}{6} + \left(\frac{5}{6}\right)\left(\frac{5}{6}\right)\left(\frac{5}{6}\right)\left(\frac{5}{6}\right) \cdot \frac{1}{6} + \dots$$

(M.U. 2009)  
(M.U. 2005)

$$\therefore P(A \text{ winning}) = \frac{1}{6} \left[ 1 + \left(\frac{25}{36}\right) + \left(\frac{25}{36}\right)^2 + \dots \right] = \frac{1}{6} \cdot \frac{1}{1 - (25/36)} = \frac{6}{11}.$$

$$P(B \text{ winning}) = 1 - P(A \text{ winning}) = \frac{5}{11}$$

$$\therefore \text{Expectation of } A = p \cdot x = \frac{6}{11} \cdot 44 = ₹ 24$$

$$\therefore \text{Expectation of } B = p \cdot x = \frac{5}{11} \cdot 44 = ₹ 20.$$

**Example 11:** A, B, C, D cut a pack of cards successfully in the order mentioned. The person who cuts a spade first wins ₹ 175. Find their expectations.

$$\text{Sol. : Probability of cutting a spade} = \frac{13}{52} = \frac{1}{4}.$$

Let  $A$  denote the success of  $A$  and  $\bar{A}$  denote failure of  $A$  and so on.

Probability of  $A$ 's success

$$\begin{aligned} &= P(A) + P(\bar{A} \bar{B} \bar{C} \bar{D} A) + P(\bar{A} \bar{B} \bar{C} \bar{D} \bar{A} \bar{B}) + \dots \\ &= \frac{1}{4} + \left(\frac{3}{4} \cdot \frac{3}{4} \cdot \frac{3}{4} \cdot \frac{3}{4} \cdot \frac{1}{4}\right) + \left(\frac{3}{4} \cdot \frac{3}{4} \cdot \frac{3}{4} \cdot \frac{3}{4} \cdot \frac{3}{4} \cdot \frac{3}{4} \cdot \frac{3}{4} \cdot \frac{1}{4}\right) + \dots \\ &= \frac{1}{4} + \frac{81}{256} \cdot \frac{1}{4} + \left(\frac{81}{256}\right)^2 \cdot \frac{1}{4} + \dots = \frac{1}{4} \cdot \frac{1}{1 - (81/256)} \\ &= \frac{1}{4} \cdot \frac{256}{256 - 81} = \frac{1}{4} \cdot \frac{256}{175} = \frac{64}{175}. \end{aligned}$$

Probability of  $B$ 's success

$$\begin{aligned} &= P(\bar{A} B) + P(\bar{A} \bar{B} \bar{C} \bar{D} + \bar{A} B) + \dots \\ &= \frac{3}{4} \cdot \frac{1}{4} + \left(\frac{3}{4} \cdot \frac{3}{4} \cdot \frac{3}{4} \cdot \frac{3}{4}\right) \left(\frac{3}{4} \cdot \frac{1}{4}\right) + \dots = \frac{3}{16} \left[ 1 + \frac{81}{256} + \dots \right] \\ &= \frac{3}{16} \left[ \frac{1}{1 - (81/256)} \right] = \frac{3}{16} \left[ \frac{256}{175} \right] = \frac{48}{175}. \end{aligned}$$

Probability of  $C$ 's success

$$= \frac{3}{4} \cdot \frac{3}{4} \cdot \frac{1}{4} + \dots = \frac{9}{64} \left[ \frac{1}{1 - (81/256)} \right] = \frac{9}{64} \cdot \frac{256}{256 - 81} = \frac{36}{175}.$$

Probability of  $D$ 's success

$$= 1 - [P(A) + P(B) + P(C)] = 1 - \left[ \frac{64}{175} + \frac{48}{175} + \frac{36}{175} \right] = \frac{27}{175}.$$

Now, the probabilities of  $A, B, C, D$

$$\therefore E(A) = p \cdot x = \frac{64}{175} \times 175 = ₹ 64, \quad E(B) = p \cdot x = \frac{48}{175} \times 175 = ₹ 48,$$

$$E(C) = p \cdot x = \frac{36}{175} \times 175 = ₹ 36, \quad E(D) = p \cdot x = \frac{27}{175} \times 175 = ₹ 27.$$

**Example 12 :** Find the expectation of number of failures preceding the first success in an infinite series of independent trials with constant probabilities  $p$  and  $q$  of success and failure respectively.

Sol. : We have the following probability distribution

$$\begin{array}{ll} X & : 0 \quad 1 \quad 2 \quad 3 \quad \dots \\ P(X=x) & : p \quad qp \quad q^2p \quad q^3p \quad \dots \end{array}$$

Since, we may get success in the first trial where the number of failures  $X=0$  and the probability is  $p$ ; we may get success in the second trial when the number of failures  $X=1$  and the probability is  $qp$  and so on.

$$\therefore E(X) = \sum p_i x_i = p(0) + qp(1) + q^2p(2) + q^3p(3) + \dots$$

$$= qp[1 + 2q + 3q^2 + \dots] = qp(1-q)^{-2} = \frac{qp}{p^2} = \frac{q}{p}.$$

**Example 13 :** The daily consumption of electric power (in million kwh) is a random variable with probability distribution function

$$f(x) = \begin{cases} kx e^{-x/3} & \text{for } x > 0 \\ 0 & \text{for } x \leq 0 \end{cases}$$

Find the value of  $k$ , the expectation of  $x$  and the probability that on a given day the electric consumption is more than expected value.

(M.U. 2003, 04, 11)

Sol. : We must have

$$\int_{-\infty}^{\infty} f(x) dx = 1 \text{ i.e. } k \int_0^{\infty} x e^{-x/3} dx = 1$$

$$\therefore k \left[ \left( x \left( \frac{e^{-x/3}}{-1/3} \right) - (1) \left( \frac{e^{-x/3}}{1/9} \right) \right) \right]_0^{\infty} = 1$$

$$\therefore k[0 + 9] = 1 \quad \therefore 9k = 1 \quad \therefore k = 1/9$$

$$E(X) = \int_{-\infty}^{\infty} x f(x) dx = \frac{1}{9} \int_0^{\infty} x^2 \cdot e^{-x/3} \cdot dx$$

$$= \frac{1}{9} \left[ x^2 \left( \frac{e^{-x/3}}{-1/3} \right) - (2x) \left( \frac{e^{-x/3}}{1/9} \right) + 2 \left( \frac{e^{-x/3}}{-1/27} \right) \right]_0^{\infty}$$

$$= \frac{1}{9} [0 - 0 + 0 + 54] = 6$$

$$\therefore P(X > 6) = \frac{1}{9} \int_6^{\infty} x \cdot e^{-x/3} \cdot dx$$

$$= \frac{1}{9} \left[ \left( x \left( \frac{e^{-x/3}}{-1/3} \right) - (1) \left( \frac{e^{-x/3}}{1/9} \right) \right) \right]_6^{\infty}$$

$$= \frac{1}{9} [(0 - 0) - (-18e^{-2} - 9e^{-2})]$$

$$= 3e^{-2} = 0.406$$

**Example 14 :** Find  $k$  and then  $E(X)$  if  $X$  has the p.d.f.

$$f(x) = \begin{cases} kx(2-x), & 0 \leq x \leq 2, k > 0 \\ 0, & \text{elsewhere} \end{cases}$$

$$\text{Sol. : Now } \int_0^2 kx(2-x) dx = k \int_0^2 2x - x^2 dx = k \left[ x^2 - \frac{1}{3} x^3 \right]_0^2 = k \cdot \frac{4}{3}$$

$$\therefore k \cdot \frac{4}{3} = 1 \quad \therefore k = \frac{3}{4}$$

By definition

$$E(X) = \int_0^2 x f(x) dx = \int_0^2 x \cdot \frac{3}{4} x(2-x) dx = \frac{3}{4} \int_0^2 (2x^2 - x^3) dx$$

$$\therefore E(X) = \frac{3}{4} \left[ \frac{2x^3}{3} - \frac{x^4}{4} \right]_0^2 = \frac{3}{4} \left[ \frac{16}{3} - \frac{16}{4} \right] = \frac{3}{4} \cdot \frac{16}{12} = 1.$$

**Example 15 :** Find  $k$  and then  $E(X)$  for the p.d.f.

$$f(x) = \begin{cases} k(x-x^2), & 0 \leq x \leq 1, k > 0 \\ 0, & \text{elsewhere} \end{cases}$$

$$\text{Sol. : Now } k \int_0^1 (x-x^2) dx = k \cdot \left[ \frac{x^2}{2} - \frac{x^3}{3} \right]_0^1 = k \left[ \frac{1}{2} - \frac{1}{3} \right] = k \cdot \frac{1}{6}$$

$$\text{But } k \cdot \frac{1}{6} = 1 \quad \therefore k = 6$$

By definition

$$E(X) = \int_0^1 x f(x) dx = \int_0^1 x \cdot 6(x-x^2) dx = 6 \left[ \frac{x^3}{3} - \frac{x^4}{4} \right]_0^1 = \frac{6}{12} = \frac{1}{2}.$$

### EXERCISE - V

- From an urn containing 3 red balls and 2 white balls, a man is to draw 2 balls at random without replacement. He gets ₹ 20 for each red ball and ₹ 10 for each white ball he draws. Find his expectation. [Ans. : ₹ 32]
- Two urns contain respectively 5 white and 3 black balls; 2 white and 3 black balls. One ball is drawn from each urn. Find the expected number of white balls drawn. [Ans. : 41/40]
- A and B toss a fair coin alternately. One who gets a head first wins ₹ 12. A starts. Find their mathematical expectations. [Ans. : ₹ 8, 4]
- A, B, and C toss a fair coin. The first one to throw a head wins the game and gets ₹ 28. If A starts, find their mathematical expectations. [Ans. : ₹ 16, 8, 4]
- A, B and C draw a card in that order from a well shuffled pack of 52 cards. The first to draw a diamond wins ₹ 740. If A starts, find their expectations. [Ans. : ₹ 320, 240, 180]
- Two unbiased dice are thrown. Find the expectation of the sum. (M.U. 2007) [Ans. : 7]

7. A man with  $n$  keys in his pocket wants to open the door of his case by trying the keys independently and randomly one by one. Find the mean and the variance of the number of trials required to open the door if unsuccessful keys are kept aside.  
 [Ans. : (i)  $(n+1)/2$ , (ii)  $(n^2-1)/12$ ] (M.U. 1999)
8. A player throwing an ordinary die is to receive  $\text{₹ } 1/2^n$  where  $n$  denotes the number of throws required to get first 3. Find his expectation.  
 (M.U. 2001, 04) [Ans. :  $\text{₹ } 1/2$ ]
9. Three fair coins are tossed. Find the expectation and the variance of number of heads.  
 (M.U. 2004) [Ans. :  $E(X) = 1.5$ ,  $\text{Var}(X) = 0.75$ ]
10. From a box containing  $n$  tickets bearing numbers 1, 2, 3, ...,  $n$  a ticket is drawn. If  $X$  denotes the number on the ticket drawn, find the mean and variance of  $X$ .  
 [Ans. :  $E(X) = (n+1)/2$ ,  $\text{Var}(X) = (n^2-1)/12$ ]
11. In a game of chance a man is allowed to throw a fair coin indefinitely. He receives rupees 1, 2, 3, ... if he throws a head at the 1st, 2nd, 3rd, ... trial respectively. If the entry fee to participate in the game is  $\text{₹ } 2$ , find the expected value of his net gain.  
 [Ans. : Zero]
12. A person draws 3 balls from a bag containing 3 white, 4 red and 5 black balls. He is offered  $\text{₹ } 10$ ,  $\text{₹ } 5$  and  $\text{₹ } 2$  if he draws 3 balls of the same colour, 2 balls of the same colour and 1 ball of each colour respectively. Find his expectation.  
 [Ans. :  $P_1 = \frac{3}{44}$ ,  $P_2 = \frac{29}{44}$ ,  $P_3 = \frac{12}{44}$ ;  $\text{₹ } 4.52$ ] (M.U. 2004)
13. A continuous random variable  $X$  has the density function  $f(x) = k(1+x)$  where  $2 \leq x \leq 5$ . Find  $k$ ,  $P(x \leq 4)$  and  $E(X)$ .  
 (M.U. 2005) [Ans. :  $k = \frac{2}{27}$ ;  $\frac{18}{27}$ ;  $\frac{11}{3}$ ]

## Random Variables

3. It should be noted that,  $E(X^2) \neq [E(X)]^2$  and  $E(1/X) \neq 1/E(X)$
4. Putting  $a = 1$ ,  $E(X^n) = \sum p_i x_i^n$  and  $E(X^n) = \int_{-\infty}^{\infty} x^n f(x) dx$   
 in particular  $E(X^2) = \sum p_i x_i^2$  and  $E(X^2) = \int_{-\infty}^{\infty} x^2 f(x) dx$   
 $E(X^2)$  is denoted by  $\mu_2'$   
 $\therefore \mu_2' = \sum p_i x_i^2$  or  $\mu_2' = \int_{-\infty}^{\infty} x^2 f(x) dx$

## 11. Mean and Variance

If we know the probability density function, discrete or continuous, we can find the mean and variance of the random variable as follows.

$$\mu_1' = \text{Mean} = E(X) = \sum p_i x_i \quad \text{or} \quad \mu_1' = \int_{-\infty}^{\infty} x f(x) dx$$

$$\text{We then find} \quad \mu_2' = E(X^2) = \sum p_i x_i^2 \quad \text{or} \quad \mu_2' = \int_{-\infty}^{\infty} x^2 f(x) dx$$

$$\begin{aligned} \text{Now,} \quad \text{Var}(X) &= E(X - \bar{X})^2 = E[X - E(X)]^2 \\ &= E[X^2 - 2XE(X) + [E(X)]^2] \\ &= E(X^2) - 2E(X) \cdot E(X) + [E(X)]^2 \end{aligned}$$

$$\text{Var}(X) = E(X^2) - [E(X)]^2$$

$$E(X^2) = \mu_2' \text{ and } E(X) = \mu_1'$$

$$\text{Var}(X) = \mu_2' - \mu_1'^2$$

## Type I : Examples on Mean and Variance of a Discrete Probability Distribution

**Example 1 :** If  $X$  denotes the smaller of the two numbers that appear when a pair of dice is thrown, find the probability distribution of  $X$ , and also the mean and variance of  $X$ . (M.U. 2004)  
**Sol. :** Refer to the table of Ex. 4, page 6-5.

We see that the number 1 appears as smaller (including equality) of the two numbers in 11 cases out of 36, the number 2 appears in 9 cases, 3 in 7 cases and so on.

The probability distribution of  $X$  is as given below.

$X$	: 1	2	3	4	5	6
$P(X = x)$	: $1/36$	$9/36$	$7/36$	$5/36$	$3/36$	$1/36$
$E(X) = \sum p_i x_i$	= $\frac{1}{36}(1) + \frac{9}{36}(2) + \frac{7}{36}(3) + \frac{5}{36}(4) + \frac{3}{36}(5) + \frac{1}{36}(6) = 2.5278$					
$E(X^2) = \sum p_i x_i^2$	= $\frac{1}{36}(1^2) + \frac{9}{36}(2^2) + \frac{7}{36}(3^2) + \frac{5}{36}(4^2) + \frac{3}{36}(5^2) + \frac{1}{36}(6^2)$					
	= $\frac{301}{36} = 8.3611$					
	$\therefore V(X) = E(X^2) - [E(X)]^2 = 8.3611 - (2.5278)^2 = 1.97$					

## Notes ...

1. If  $g(X) = aX^n$ , then  $E[g(X)] = E[aX^n] = \sum p_i a x_i^n = a \sum p_i x_i^n = a E(X^n)$

And

$$E[g(X)] = E[aX^n] = \int_{-\infty}^{\infty} ax^n f(x) dx = a \int_{-\infty}^{\infty} x^n f(x) dx = a E(X^n)$$

$$\text{e.g. } E(aX) = a E(X)$$

$$\text{e.g. } E(aX^2) = a E(X^2), E(aX^3) = a E(X^3)$$

2. If  $g(X) = aX + b$ , then  $E[g(X)] = E[aX + b] = a E(X) + b$ .

**Example 2 :** A discrete random variable has the probability density function given below.

$X$	-2	-1	0	1	2	3
$P(X=x)$	0.2	$k$	0.1	$2k$	0.1	$2k$

Find  $k$ , the mean and variance.  
Solution : We must have  $\sum p_i = 1$ .

$$\therefore 5k + 0.4 = 1 \quad \therefore 5k = 0.6 \quad \therefore k = \frac{0.6}{5} = \frac{3}{25}$$

Hence, the probability distribution is

$X$	-2	-1	0	1	2	3
$P(X=x)$	2/10	3/25	1/10	6/25	1/10	6/25

Now, Mean =  $E(X) = \sum p_i x_i = -\frac{4}{10} - \frac{3}{25} + 0 + \frac{6}{25} + \frac{2}{10} + \frac{18}{25} = \frac{60}{250} = \frac{6}{25}$

$$E(X^2) = \sum p_i x_i^2 = \frac{2}{10}(4) + \frac{3}{25}(1) + 0 + \frac{6}{25}(1) + \frac{1}{10}(4) + \frac{8}{25}(9) = \frac{73}{250}$$

$$\therefore \text{Variance} = \sigma^2 = E(X^2) - [E(X)]^2 = \frac{73}{250} - \frac{36}{625} = \frac{293}{625}$$

**Example 3 :** Find the value of  $k$  from the following data.

$X$	0	10	15
$P(x)$	$\frac{k-6}{5}$	$\frac{2}{k}$	$\frac{14}{5k}$

Also find the distribution function and the expectation of the distribution.  
Sol. : Since  $\sum p_i = 1$ ,

$$\frac{k-6}{5} + \frac{2}{k} + \frac{14}{5k} = 1 \quad \therefore k^2 - 11k + 14 = 0$$

$$\therefore (k-8)(k-3) = 0 \quad \therefore k = 8 \text{ or } 3$$

But when  $k = 3$ ,  $P(x=0) = \frac{3-6}{5} = -\frac{3}{5}$  which is impossible.  $\therefore k = 8$ .

The p.d.f. and distribution function are

$X$	0	10	15
$P(x)$	2/5	1/4	7/20
$F(x)$	2/5	13/20	1
$\therefore E(X) = \sum p_i x_i = \frac{2}{5}(0) + \frac{1}{4}(10) + \frac{7}{20}(15) = \frac{5}{2} + \frac{21}{4} = \frac{31}{4}$			

**Example 4 :** If the mean of the following distribution is 16 find  $m$ ,  $n$  and variance

$X$	8	12	16	20	24
$P(X=x)$	1/8	$m$	$n$	1/4	1/12

Sol. : Since  $\sum p_i = 1$ ,

$$\frac{1}{8} + m + n + \frac{1}{4} + \frac{1}{12} = 1 \quad \therefore m + n = \frac{13}{24}$$

(M.U. 2006, 10)

Since mean = 16,  $\sum p_i x_i = 16$

$$\begin{aligned} 1 + 12m + 16n + 5 + 2 &= 16 \\ 12m + 16n + 8 &= 16 \quad \therefore 3m + 4n = 2 \end{aligned}$$

Multiply (1) by 3 and subtract from (2),

$$\begin{aligned} 3m + 4n = 2 &; \quad 3m + 3n = \frac{13}{8} \quad \therefore n = \frac{3}{8} \\ \therefore m + n = \frac{13}{24} \text{ gives } m + \frac{3}{8} = \frac{13}{24} &; \quad m = \frac{4}{24} = \frac{1}{6} \end{aligned}$$

To find variance, consider

$$E(X^2) = \sum p_i x_i^2 = \frac{1}{8}(64) + \frac{1}{6}(144) + \frac{3}{8}(256) + \frac{1}{4}(400) + \frac{1}{12}(576) = 276$$

$$\text{Var}(X) = E(X^2) - [E(X)]^2 = 276 - 16^2 = 20.$$

**Example 5 :** A woman with  $n$  keys with her, wants to open the door of her house by trying keys independently and randomly one by one. Find the mean and the variance of the number of trials required to open the door, if unsuccessful keys are kept aside.

(M.U. 2016)

Sol. : If unsuccessful keys are kept aside, she will get success in the first trial, or second trial or third trial and so on, the random variable  $X$  of the successful trial will take values 1, 2, 3, ...,  $n$ .

$$\therefore P(\text{Success in the first trial}) = \frac{1}{n}$$

$$P(\text{Failure in the first trial}) = 1 - \frac{1}{n}$$

If there is failure in the first trial, the key is eliminated. There are now  $(n-1)$  keys.

$$\therefore P(\text{Success in the second trial}) = \frac{1}{n-1}$$

$$\therefore P(\text{Failure in the first trial and success in the second trial})$$

$$= \left(1 - \frac{1}{n}\right) \left(\frac{1}{n-1}\right) = \frac{n-1}{n} \cdot \frac{1}{n-1} = \frac{1}{n}$$

$$\therefore P(\text{Failure in the first trial, failure in the second trial and success in the third trial})$$

$$= \left(1 - \frac{1}{n}\right) \left(1 - \frac{1}{n-1}\right) \left(\frac{1}{n-2}\right)$$

$$= \frac{(n-1)}{n} \cdot \frac{(n-2)}{(n-1)} \cdot \frac{1}{(n-2)} = \frac{1}{n}$$

Thus, the probability of success at any trial remains constant =  $\frac{1}{n}$

Thus, the probability distribution of  $X$  is

$X$	1	2	3	4	...	$n$
$P(X=x)$	$\frac{1}{n}$	$\frac{1}{n}$	$\frac{1}{n}$	$\frac{1}{n}$	$\dots$	$\frac{1}{n}$

$$\therefore E(X) = \sum x p(x) = \frac{1}{n} \cdot 1 + \frac{1}{n} \cdot 2 + \frac{1}{n} \cdot 3 + \dots + \frac{1}{n} \cdot n$$

$$= \frac{1}{n} (1 + 2 + 3 + \dots + n) = \frac{1}{n} \cdot \frac{n(n+1)}{2} = \frac{n+1}{2}$$

$$\begin{aligned} E(X) &= \frac{n+1}{2} \quad \left[ \because 1+2+\dots+n = \frac{n(n+1)}{2} \right] \\ E(X^2) &= \sum p(x)x^2 = \frac{1}{n} \cdot 1^2 + \frac{1}{n} \cdot 2^2 + \frac{1}{n} \cdot 3^2 + \dots + \frac{1}{n} \cdot n^2 \\ &= \frac{1}{n} (1^2 + 2^2 + 3^2 + \dots + n^2) = \frac{1}{n} \cdot \frac{n(n+1)(2n+1)}{6} \\ &= \frac{(n+1)(2n+1)}{6} \quad \left[ \because 1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6} \right] \\ V(X) &= E(X^2) - [E(X)]^2 = \frac{(n+1)(2n+1)}{6} - \frac{(n+1)^2}{4} \\ &= \frac{2(2n^2 + 3n + 1) - 3(n^2 + 2n + 1)}{12} = \frac{n^2 - 1}{12}. \end{aligned}$$

#### Type II : Examples on Mean and Variance of a Continuous Probability Distribution

**Example 1 :** A continuous random variable  $X$  has the p.d.f. defined by  $f(x) = A + Bx, 0 \leq x \leq 1$ . If the mean of the distribution is  $1/3$ , find  $A$  and  $B$ .

Sol. : Since  $f(x)$  is a probability distribution  $\int_{-\infty}^{\infty} f(x) dx = 1$

$$\text{By data } \int_0^1 (A + Bx) dx = 1 \quad \therefore \left[ AX + \frac{Bx^2}{2} \right]_0^1 = 1 \quad \therefore A + \frac{B}{2} = 1 \quad \text{.....(i)}$$

$$\text{Since the mean is } \frac{1}{3}, \quad \int_0^1 x f(x) dx = \frac{1}{3} \quad \therefore \int_0^1 (A + Bx) x dx = \frac{1}{3}$$

$$\therefore \int_0^1 (Ax + Bx^2) dx = \frac{1}{3} \quad \therefore \left[ Ax^2 + \frac{Bx^3}{3} \right]_0^1 = \frac{1}{3}$$

$$\therefore \frac{A}{2} + \frac{B}{3} = \frac{1}{3} \quad \therefore 3A + 2B = 2 \quad \text{.....(ii)}$$

Solving the equations (i) and (ii), we get  $A = 2, B = -2$ .

$\therefore$  The p.d.f. is  $f(x) = 2 - 2x, 0 \leq x \leq 1$

**Example 2 :** The distribution function of a r.v.  $X$  is given by  $F_X(x) = 1 - (1+x)e^{-x}, x \geq 0$ . Find the mean and variance.

Solution : We have

$$f_X(x) = \frac{dF_X(x)}{dx} = (1+x)e^{-x} - e^{-x} = x e^{-x}, \quad x \geq 0$$

$$\begin{aligned} \therefore \text{Mean } \bar{X} &= \int_0^{\infty} x \cdot f_X(x) dx = \int_0^{\infty} x^2 e^{-x} dx \\ &= \left[ x^2 (-e^{-x}) - 2x(e^{-x}) + 2(1) \cdot (-e^{-x}) \right]_0^{\infty} = 2 \end{aligned}$$

$$E(X^2) = \int_0^{\infty} x^2 f_X(x) dx = \int_0^{\infty} x^3 e^{-x} dx$$

#### Applied Mathematics - IV

(6-36)

Random Variables

$$E(X^2) = \left[ x^3 (-e^{-x}) - 3x^2 (e^{-x}) + 6x(-e^{-x}) - 6(e^{-x}) \right]_0^{\infty} = 6$$

$$V(X) = E(X^2) - [E(X)]^2 = 6 - 4 = 2.$$

**Example 3 :** A continuous random variable  $X$  has the p.d.f.  $f(x) = kx^2 e^{-x}, x \geq 0$ . Find  $k$ , mean and variance.

(M.U. 2004)

Solution : We must have  $\int_0^{\infty} kx^2 e^{-x} dx = 1$

$$\therefore k \left[ x^2 (-e^{-x}) - \int -e^{-x} 2x dx \right]_0^{\infty} = 1$$

$$\therefore k \left[ -x^2 e^{-x} + 2x(-e^{-x}) - \int -2e^{-x} dx \right]_0^{\infty} = 1$$

[ Integrating by parts ]

$$k \left[ -x^2 e^{-x} - 2x e^{-x} - 2e^{-x} \right]_0^{\infty} = 1$$

$$k [0 - (-0 - 0 - 2)] = 1 \quad \therefore 2k = 1 \quad \therefore k = \frac{1}{2}.$$

$$\text{Now, mean } \bar{X} = \int_0^{\infty} x f(x) dx = \int_0^{\infty} \frac{1}{2} x^3 e^{-x} dx$$

$$= \frac{1}{2} \left[ x^3 (-e^{-x}) - (3x^2)(e^{-x}) + (6x)(-e^{-x}) - (6)(e^{-x}) \right]_0^{\infty}$$

( By the generalised rule of integration by parts. )

$$\int u v dx = u v_1 - u' v_2 + u'' v_3 - u''' v_4 + \dots$$

where dashes denote the derivatives and suffixes denote the integrals. )

$$\therefore \bar{X} = \frac{1}{2} [0 - (-6)] = \frac{1}{2} \cdot 6 = 3$$

$$\text{Now, } \mu_2' = \frac{1}{2} \int_0^{\infty} x^2 f(x) dx = \frac{1}{2} \int_0^{\infty} x^2 \cdot x^2 e^{-x} dx$$

$$= \frac{1}{4} \int_0^{\infty} x^4 \cdot e^{-x} dx$$

$$= \frac{1}{2} \left[ x^4 (-e^{-x}) - (4x^3)(e^{-x}) + (12x^2)(-e^{-x}) - (24x)(e^{-x}) + 24(-e^{-x}) \right]_0^{\infty}$$

$$= \frac{1}{2} [0 - (-24)] = \frac{24}{2} = 12$$

$$\therefore \text{Variance} = \mu_2' - \mu_1'^2 = 12 - 9 = 3.$$

**Example 4 :** Find the value of  $k$ , if the function

$$f(x) = kx^2(1-x^3), \quad 0 \leq x \leq 1$$

$$= 0 \quad \text{otherwise}$$

is a probability density function. Also find  $P(0 \leq x \leq 1/2)$  and the mean and variance.

Sol. : We have  $\int_0^1 kx^2(1-x^3) dx = 1 \quad \therefore \int_0^1 k(x^2 - x^5) dx = 1$

$$\therefore k \left[ \frac{x^3}{3} - \frac{x^6}{6} \right]_0^1 = 1 \quad \therefore k \left[ \frac{1}{3} - \frac{1}{6} \right] = 1 \quad \therefore k \cdot \frac{1}{6} = 1 \quad \therefore k = 6.$$

$$\text{Now, } P(0 \leq x \leq 2) = 6 \int_0^{1/2} (x^2 - x^5) dx = 6 \left[ \frac{x^3}{3} - \frac{x^6}{6} \right]_0^{1/2} = 6 \left[ \frac{1}{6 \cdot 3} - \frac{1}{64 \cdot 6} \right] = \frac{15}{64}$$

$$\begin{aligned} \text{Mean } \bar{x} &= \mu_1' = \int_0^1 x f(x) dx = 6 \int_0^1 x \cdot x^2 (1-x^3) dx = 6 \int_0^1 (x^3 - x^6) dx \\ &= 6 \left[ \frac{x^4}{4} - \frac{x^7}{7} \right]_0^1 = 6 \left[ \frac{1}{4} - \frac{1}{7} \right] = \frac{18}{28} = \frac{9}{14} \end{aligned}$$

$$\begin{aligned} \mu_2' &= \int_0^1 x^2 f(x) dx = 6 \int_0^1 x^2 [x^2 (1-x^3)] dx = 6 \int_0^1 (x^4 - x^7) dx \\ &= 6 \left[ \frac{x^5}{5} - \frac{x^8}{8} \right]_0^1 = 6 \left[ \frac{1}{5} - \frac{1}{8} \right] = \frac{18}{40} = \frac{9}{20} \end{aligned}$$

$$\text{Variance} = \mu_2' - \mu_1'^2 = \frac{9}{20} - \frac{91}{196} = \frac{441 - 405}{980} = \frac{36}{980} = \frac{9}{245}.$$

**Example 5 :** A continuous random variable  $X$  has the following probability density function

$$f(x) = \begin{cases} kx & 0 \leq x \leq 2 \\ 2k & 2 \leq x \leq 4 \\ 6k - kx & 4 \leq x \leq 6 \end{cases}$$

Find  $k$ ,  $P(1 \leq x \leq 3)$  and the mean.

Sol. : For p.d.f. we must have  $\int_{-\infty}^{\infty} f(x) dx = 1$ .

$$\therefore \int_0^2 kx dx + \int_2^4 2k dx + \int_4^6 (6k - kx) dx = 1$$

$$\therefore k \left[ \frac{x^2}{2} \right]_0^2 + 2k[x]_2^4 + k \left[ 6x - \frac{x^2}{2} \right]_4^6 = 1$$

$$\frac{k}{2}[4-0] + 2k[4-2] + k[(36-18)-(24-8)] = 1$$

$$2k+4k+6k=1 \quad \therefore 12k=1 \quad \therefore k=\frac{1}{12}$$

$$\therefore P(1 \leq x \leq 3) = \int_1^2 \frac{x}{12} dx + \int_2^3 \frac{1}{6} dx = \frac{1}{12} \left[ \frac{x^2}{2} \right]_1^2 + \frac{1}{6} [x]_2^3 = \frac{1}{6} + \frac{1}{6} = \frac{1}{3}.$$

$$\text{Mean } \bar{x} = \mu_1' = \int_{-\infty}^{\infty} x f(x) dx$$

$$= \frac{1}{12} \int_0^2 x \cdot x dx + \frac{1}{6} \int_2^4 x dx + \frac{1}{12} \int_4^6 x (6-x) dx$$

$$\begin{aligned} \text{Mean } \bar{x} &= \frac{1}{12} \left[ \frac{x^3}{3} \right]_0^2 + \frac{1}{6} \left[ \frac{x^2}{2} \right]_2^4 + \frac{1}{12} \left[ 3x^2 - \frac{x^3}{3} \right]_4^6 \\ &= \frac{8}{36} + \frac{1}{12} [16-4] + \frac{1}{12} \left[ \left( 108 - \frac{216}{3} \right) - \left( 48 - \frac{64}{3} \right) \right] \\ &= \frac{2}{9} + 1 + \frac{1}{12} + \frac{28}{3} = \frac{383}{36}. \end{aligned}$$

**Example 6 :** If the distribution function of a random variable is given by

$$F(x) = \begin{cases} 1 - 4/x^2, & x > 2 \\ 0, & x \leq 2 \end{cases}$$

find (i)  $P(x < 3)$ , (ii)  $P(4 < x < 5)$ , (iii) mean and the variance.

Sol. : The probability density function  $f(x)$  is given by

$$f(x) = F'(x) = \begin{cases} 8/x^3, & x > 2 \\ 0, & x \leq 2 \end{cases}$$

$$(i) \quad P(x < 3) = \int_2^3 \frac{8}{x^3} dx = \left[ -\frac{8}{2x^2} \right]_2^3 = \left[ -\frac{4}{x^2} \right]_2^3 = -4 \left[ \frac{1}{9} - \frac{1}{4} \right] = \frac{5}{9}.$$

$$(ii) \quad P(4 < x < 5) = \int_4^5 \frac{8}{x^3} dx = \left[ -\frac{4}{x^2} \right]_4^5 = -4 \left[ \frac{1}{25} - \frac{1}{16} \right] = 0.09$$

$$(iii) \quad \mu_1' = \int_2^{\infty} x \cdot \frac{8}{x^3} dx = \int_2^{\infty} \frac{8}{x^2} dx = 8 \left[ -\frac{1}{x} \right]_2^{\infty} = -8 \left[ 0 - \frac{1}{2} \right] = 4.$$

$$\mu_2' = \int_2^{\infty} x^2 \cdot \frac{8}{x^3} dx = 8 \int_2^{\infty} \frac{1}{x} dx = 8 [\log x]_2^{\infty} = \infty$$

$\therefore \text{Var.}(x) = \mu_2' - \mu_1'^2$   $\therefore \text{Var.}(x)$  does not exist.

**Example 7 :** A continuous random variable has probability density function

$$f(x) = 6(x-x^2), \quad 0 \leq x \leq 1$$

Find (i) mean, (ii) variance.

(M.U. 1997, 2001, 03, 14)

Sol. : (i)  $\mu_1' = \int_0^1 x \cdot 6(x-x^2) dx = 6 \int_0^1 (x^2 - x^3) dx$

$$= 6 \left[ \frac{x^3}{3} - \frac{x^4}{4} \right]_0^1 = 6 \left( \frac{1}{3} - \frac{1}{4} \right) = \frac{1}{2}$$

(ii)  $\mu_2' = \int_0^1 x^2 \cdot 6(x-x^2) dx = 6 \int_0^1 (x^3 - x^4) dx$

$$\therefore \mu_2' = 6 \left[ \frac{x^4}{4} - \frac{x^5}{5} \right]_0^1 = 6 \left[ \frac{1}{4} - \frac{1}{5} \right] = \frac{6}{20} = \frac{3}{10}$$

$$\therefore \text{Var.}(x) = \mu_2' - \mu_1'^2 = \frac{3}{10} - \frac{1}{4} = \frac{1}{20}$$

## EXERCISE - VI

Type - I  
1. The probability distribution of a random variable  $X$  is given by

$$\begin{array}{ccccccc} X & : & -2 & -1 & 0 & 1 & 2 & 3 \\ P(X=x) & : & 0.1 & k & 0.2 & 2k & 0.3 & k \end{array}$$

Find  $k$ , the mean and variance. [Ans.: (i)  $k=0.1$ , (ii)  $\bar{X}=0.8$ , (iii)  $\text{Var. } 2.16$ ]

2. If  $X$  denotes the larger of the two numbers that appear when a pair of dice is thrown, find its probability distribution of  $X$ , and also the mean and variance of  $X$ .

$$\begin{array}{ccccccc} X & : & 1 & 2 & 3 & 4 & 5 & 6 \\ P(X=x) & : & 1/36 & 3/36 & 5/36 & 7/36 & 9/36 & 11/36 \end{array}$$

Mean = 4.47, Var. = 1.97]

3. Given the following distribution

$$\begin{array}{ccccccc} X & : & -3 & -2 & -1 & 0 & 1 & 2 \\ P(X=x) & : & 0.01 & 0.1 & 0.2 & 0.3 & 0.2 & 0.15 \end{array}$$

Find (i)  $P(X \geq 1)$ , (ii)  $P(X < 0)$ , (iii)  $E(X)$ , (iv)  $V(X)$ . [Ans.: (i) 0.35, (ii) 0.35, (iii) 0.05, (iv) 1.8475]

4. Find the value of  $k$  from the following data.

$$\begin{array}{cccc} X & : & 0 & 10 & 15 \\ P(X=x) & : & (k-6)/5 & 2/k & 14/5k \end{array}$$

Also find the distribution function and expectation of  $X$ . [Ans.:  $k=8$  or 3, 3 is impossible since  $P(X=0)=-\frac{3}{5}$  for  $k=3$ ]

$$\begin{array}{cccc} X & : & 0 & 10 & 15 \\ F(x) & : & 2/5 & 13/20 & 1 \end{array} \quad E(X)=31/4$$

5. Find the mean and variance of  $X$  in Ex. 1 of Exercise I, page 6-9. [Ans.: 33/5, 136/25]

6. Find the mean and variance of  $X$  in Ex. 2 (ii) of Exercise I, page 6-9. [Ans.: 7/3, 14/9]

7. A random variable  $X$  has the probability law  $P(X=x)=1/n$ ,  $x=1, 2, \dots, n$ . Find  $E(X)$  and  $V(X)$ . [Ans.: (i)  $(n+1)/2$ , (ii)  $(n^2-1)/12$ ]

8. A random variable  $X$  has the probability distribution

$$\begin{array}{ccccccc} X & : & -2 & -1 & 0 & 1 & 2 & 3 \\ P(X=x) & : & 0.1 & k & 0.2 & 2k & 0.3 & k \end{array}$$

Find  $k$  and then mean and variance of  $X$ . [Ans.:  $k=0.1$ , 0.8, 2.16]

9. Find the mean and the variance of the following distribution

$$\begin{array}{ccccc} X & : & 1 & 3 & 4 & 5 \\ P(X=x) & : & 0.4 & 0.1 & 0.2 & 0.3 \end{array}$$

[Ans.: (i)  $\bar{X}=3$ , (ii)  $\text{Var. } 3$ ]

10. A random variable  $X$  has the probability distribution  $P(X=0)=P(X=2)=p$ ,  $P(X=1)=1-2p$  and  $0 \leq p \leq 2/3$ .

For what value of  $p$  is the  $\text{Var. } (X)$  maximum?

[Ans.:  $p=2/3$ ]

Type - II

1. Find the mean and the variance of the following distribution

$$f(x) = \begin{cases} 1-x, & 0 < x < 1 \\ x-1, & 1 < x < 2 \end{cases}$$

(M.U. 2006) [Ans.: (i)  $\bar{X}=1$ , (ii)  $\text{Var. } 1/2$ ]

2. If the probability density function is given by

$$f(x) = \begin{cases} kx^2(1-x^2), & 0 \leq x \leq 1 \\ 0, & \text{elsewhere} \end{cases}$$

(i) Find  $k$ , (ii)  $P(0 < X < 1/2)$ , (iii)  $\bar{X}$ , (iv)  $\sigma^2$ .

[Ans.: (i)  $k=6$ , (ii)  $15/64$ , (iii)  $9/14$ , (iv)  $9/245$ ]

3. If the probability density of a random variable is given by

$$f(x) = \begin{cases} kx, & 0 \leq x \leq 2 \\ 2k, & 2 \leq x \leq 4 \\ 6k - kx, & 4 \leq x \leq 6 \end{cases}$$

Find (i)  $k$ , (ii)  $P(1 \leq X \leq 3)$ , (iii)  $\bar{X}$ . (M.U. 2002, 03, 05) [Ans.: (i)  $1/6$ , (ii)  $7/18$ , (iii)  $7/4$ ]

4. Find the mean and the variance of

$$f(x) = \begin{cases} x, & 0 \leq x \leq 1 \\ 2-x, & 1 \leq x \leq 2 \end{cases}$$

(M.U. 2006) [Ans.: 1.5/2]

5. If the probability density of a random variable is given by

$$(a) f(x) = \begin{cases} kx e^{-x/3}, & x > 0 \\ 0, & x \leq 0 \end{cases} \quad (M.U. 2005) \quad (b) f(x) = \begin{cases} kx^2 e^{-x}, & x > 0 \\ 0, & x \leq 0 \end{cases} \quad (M.U. 2007)$$

(i) Find  $k$ , (ii)  $\bar{X}$ , (iii)  $\sigma^2$ . [Ans.: (a) (i)  $1/9$ , (ii)  $6$ , (iii)  $18$ ; (b) (i)  $1/2$ , (ii)  $3$ , (iii)  $3$ ]

6. A continuous random variable  $X$  has p.d.f.  $f(x)=kx^2 e^{-x}$ ,  $x \geq 0$ . Find  $k$ , mean and variance. (M.U. 2004) [Ans.: (i)  $1/2$ , (ii)  $3$ , (iii)  $3$ ]

7. If the probability density of a random variable is given by

$$f(x) = \begin{cases} kx e^{-x/3}, & x > 0 \\ 0, & x \leq 0 \end{cases}$$

(i) Find  $k$ , (ii)  $\bar{X}$ , (iii)  $\sigma^2$ .

(M.U. 2005) [Ans.: (i)  $1/9$ , (ii)  $6$ , (iii)  $18$ ]

8. A continuous random variable has probability density function

$$f(x) = \begin{cases} 2e^{-2x} & \text{for } x > 0 \\ 0 & \text{for } x \leq 0 \end{cases}$$

Find (i)  $E(X)$ , (ii)  $E(X^2)$ , (iii)  $\text{Var. } (X)$ , (iv) S.D. of  $X$ .

(M.U. 2005)

[Ans.: (i)  $\frac{1}{2}$ , (ii)  $\frac{1}{2}$ , (iii)  $\frac{1}{4}$ , (iv)  $\frac{1}{2}$ ]

9. The length of time (in minutes) a lady speaks on telephone is found to be a random variable with probability density function

$$f(x) = \begin{cases} Ae^{-x/5} & \text{for } x \geq 0 \\ 0 & \text{elsewhere} \end{cases}$$

Find  $A$  and the probability that she will speak for (i) more than 10 minutes, (ii) less than 5 minutes, (iii) between 5 and 10 minutes.

$$[ \text{Ans. : (i) } A = \frac{1}{5}, \text{ (ii) } \frac{1}{a^2}, \text{ (iii) } \frac{(a-1)}{a}, \text{ (iv) } \frac{(a-1)}{a^2} ] \quad (\text{M.U. 2004})$$

10. The probability density function of a random variable is given by

$$f(x) = ke^{-x/a}, \quad 0 < x < \infty$$

Find the mean and standard deviation of  $X$ .

(M.U. 2002) [ Ans. : (i)  $\sigma$ , (ii)  $\sigma$  ]

11. A random variable  $X$  has the p.d.f.  $f(x) = \frac{k}{1+x^2}, -\infty < x < \infty$ .

Determine  $k$  and the distribution function. Evaluate (i)  $P(X \geq 0)$ , (ii) Mean, (iii) Variance.

$$[ \text{Ans. : } k = \frac{1}{\pi}, \quad F(x) = \frac{1}{\pi} \left[ \tan^{-1} x + \frac{\pi}{2} \right], \quad P(X \geq 0) = \frac{1}{2}, \quad \bar{X} = 0, \text{ variance does not exist.} ] \quad (\text{M.U. 2004})$$

12. If  $f(x) = \begin{cases} xe^{-x^2/2}, & x \geq 0 \\ 0, & x < 0 \end{cases}$

prove that (i)  $f(x)$  is a probability density function and (ii) obtain distribution function  $F(x)$ .

$$[ \text{Ans. : (i) } \int_0^\infty xe^{-x^2/2} dx = \int_0^\infty e^{-t} dt = 1 \text{ where } t = \frac{x^2}{2}; \text{ (ii) } F(x) = 1 - e^{-x^2/2} ] \quad (\text{M.U. 1996})$$

13. A continuous random variable  $X$  takes values between 2 and 5. Its density function is  $f(x) = k(1+x)$ . Find  $k$  and  $P(X < 4)$ .

(M.U. 1996) [ Ans. :  $k = 2/27, 16/27$  ]

14. The distribution function of a continuous random variable  $X$  is given by

$$F(x) = 1 - (1+x) e^{-x}, \quad x \geq 0.$$

- Find the density function, mean and variance.

[ Ans. :  $f(x) = xe^{-x}, \quad x \geq 0$ ; (i)  $\bar{X}$ , (ii)  $V(X)$  ]

15. A continuous random variable  $X$  has a probability density function  $f(x) = 3x^2, 0 \leq x \leq 1$ . Find  $a$  and  $b$  such that (i)  $P(X \leq a) = P(X \geq b)$ , (ii)  $P(X > b) = 0.005$ .

$$[ \text{Ans. : (i) } a = \sqrt[3]{1/2}, \text{ (ii) } b = \sqrt[3]{0.005} ]$$

16. If  $f(x)$  is probability density function of a continuous random variate, find  $k$ , mean and variance.

$$f(x) = \begin{cases} kx^2 & 0 \leq x \leq 1 \\ (2-x)^2 & 1 \leq x \leq 2 \end{cases} \quad (\text{M.U. 2002}) \quad [ \text{Ans. : } k = 2, \quad \bar{X} = \frac{11}{12}, \quad V(X) = 0.826 ]$$

17. A continuous random variable  $X$  has the probability density function given by

$$f(x) = \begin{cases} 2ax+b & 0 \leq x \leq 2 \\ 0 & \text{otherwise} \end{cases}$$

If the mean of the distribution is 3, find the constants  $a$  and  $b$ .

(M.U. 1996)

$$[ \text{Ans. : } a = \frac{3}{2}, \quad b = -\frac{5}{2} ]$$

18. If  $X$  is a continuous random variate with probability density function given by

$$f(x) = \begin{cases} k(x-x^2) & 0 \leq x \leq 1 \\ 0 & \text{otherwise} \end{cases}$$

Find (i)  $k$ , (ii) mean, (iii) variance, (iv) median.

(M.U. 1998)

19. The probability density function of a random variable is given by

$$f(x) = \begin{cases} 0 & x < 2 \\ \frac{2x+3}{18} & 2 \leq x \leq 4 \\ 0 & x > 4 \end{cases}$$

Find the mean and variance.

(M.U. 2001, 02) [ Ans. :  $\bar{X} = \frac{83}{27}, \quad V(X) = 0.333$  ]

20. Prove that  $f(x) = \begin{cases} 1-|1-x| & 0 \leq x \leq 2 \\ 0 & \text{elsewhere} \end{cases}$

is a probability density function. Find its mean and variance.

(M.U. 1998)

[ Ans. :  $\bar{X} = 12, \quad V(X) = \frac{1}{2}$  ]

21. A continuous random variable  $X$  has the following probability density function

$$f(x) = \begin{cases} x^3 & 0 \leq x \leq 1 \\ (2-x)^3 & 1 \leq x \leq 2 \\ 0 & \text{otherwise} \end{cases}$$

Find  $P(0.5 \leq x \leq 1.5)$  and the mean of the distribution.

(M.U. 1998) [ Ans. :  $\frac{15}{32}, \quad \bar{X} = \frac{1}{2}$  ]

22. The probability density function of a continuous random variable  $X$  is given by

$$f(x) = kx(2-x), \quad 0 \leq x \leq 2.$$

Find  $k$ , mean and variance.

(M.U. 1997, 99) [ Ans. :  $k = \frac{3}{4}, \quad \bar{X} = 1, \quad V(X) = \frac{1}{5}$  ]

## 12. Moments

The term moment has been borrowed from Mechanics in which it is used to measure the capacity of a force to produce rotation of a body. In statistics moments are used to describe characteristics of a distribution. In fact we have already used two moments of the first and second order to define the mean and the standard deviation of a distribution. The mean is the representative figure of a distribution and standard deviation measures the spread of the items around the mean. But if we want further information about the distribution it is provided by the moments of higher order. Moments are defined about any value or about the mean.

The  $r$ -th moment of a variable  $X$  about any point  $A$ , denoted by  $\mu_r'$  is given by

$$\mu_r' = \frac{1}{N} \sum f_i (x_i - A)^r \quad \text{where } N = \sum f_i$$

$$\mu_r' = \frac{1}{N} \sum f_i d_i^r$$

where  $d_i = x_i - A$ .

They are called raw moments.

In other words, the  $r$ -th moment of  $X$  about  $A$  is the arithmetic mean of the  $r$ -th power of deviations of  $X$  from  $A$ .The  $r$ -th moment of  $X$  about the mean  $\bar{X}$  denoted by  $\mu_r$  is given

$$\mu_r = \frac{1}{N} \sum f_i (x_i - \bar{X})^r$$

$$\mu_r = \frac{1}{N} \sum f_i z_i^r \quad \text{where } z_i = x_i - \bar{X}$$

They are called central moments.

In words, the  $r$ -th moment of  $X$  about the mean  $\bar{X}$  is the arithmetic mean of the  $r$ -th power of the deviations of  $X$  from the mean  $\bar{X}$ .

## Particular Cases

1. Zeroth moment about
- $A$
- or the mean is unity.

$$\mu_0' = \frac{1}{N} \sum f_i (x_i - A)^0 = \frac{1}{N} \sum f_i = 1$$

$$\text{Also } \mu_0 = \frac{1}{N} \sum f_i (x_i - \bar{X})^0 = \frac{1}{N} \sum f_i = 1.$$

2. The first moment about the mean
- $\bar{X}$
- is always zero.

$$\begin{aligned} \mu_1 &= \frac{1}{N} \sum f_i (x_i - \bar{X}) = \frac{1}{N} \sum f_i x_i - \bar{X} \cdot \frac{1}{N} \sum f_i \\ &= \bar{X} - \bar{X} = 0. \end{aligned}$$

3. The second moment about the mean is the variance.

$$\mu_2 = \frac{1}{N} \sum f_i (x_i - \bar{X})^2 = \sigma^2 \text{ by definition of } \sigma.$$

4. The relation between
- $\mu_1'$
- and
- $\bar{X}$
- .

$$\text{By definition } \mu_1' = \frac{1}{N} \sum f_i (x_i - A) = \frac{1}{N} \sum f_i x_i - \frac{A}{N} \sum f_i = \bar{X} - A$$

$$\bar{X} = A + \mu_1'$$

In short we have the following fundamental results. You are advised to memorise them.

$$\mu_0' = 1, \mu_0 = 1, \mu_1 = 0, \mu_2 = \sigma^2 \text{ and } \bar{X} = A + \mu_1'.$$

(a) Moments about mean in terms of moments about any point : Moments about the mean can be expressed in terms of moments about any point as follows.

$$\text{We have } \mu_r = \frac{1}{N} \sum f_i (x_i - \bar{X})^r = \frac{1}{N} \sum f_i (x_i - A + A - \bar{X})^r.$$

Putting  $x_i - A = d_i$ ,

$$\mu_r = \frac{1}{N} \sum f_i (d_i + A - \bar{X})^r.$$

But as seen above  $\bar{X} - A = \mu_1'$ 

$$\begin{aligned} \therefore \mu_r &= \frac{1}{N} \sum f_i (d_i + \mu_1')^r \\ &= \frac{1}{N} \sum f_i [d_i^r + r C_1 d_i^{r-1} \mu_1' + r C_2 d_i^{r-2} \mu_1'^2 + \dots + (-1)^r \mu_1'^r] \\ &\therefore \mu_r = \mu_r' - r C_1 \mu_{r-1}' \mu_1' + r C_2 \mu_{r-2}' \mu_1'^2 - r C_3 \mu_{r-3}' \mu_1'^3 + \dots + (-1)^r \mu_1'^r \quad \dots \dots \dots (A) \end{aligned}$$

In particular, putting  $r = 1, 2, 3, \dots$ 

$$\mu_1 = \mu_1' - \mu_0' \mu_1' = \mu_1' - \mu_1' = 0 \quad [\because \mu_0' = 1]$$

$$\mu_2 = \mu_2' - 2\mu_1' \mu_1' + \mu_0' \mu_1'^2 = \mu_2' - \mu_1'^2$$

$$\mu_3 = \mu_3' - 3\mu_2' \mu_1' + 3\mu_1' \mu_1'^2 - \mu_0' \mu_1'^3$$

$$= \mu_3' - 3\mu_2' \mu_1' + 2\mu_1'^3$$

$$\mu_4 = \mu_4' - 4\mu_3' \mu_1' + 6\mu_2' \mu_1'^2 - 4\mu_1' \mu_1'^3 + \mu_0' \mu_1'^4$$

$$= \mu_4' - 4\mu_3' \mu_1' + 6\mu_2' \mu_1'^2 - 3\mu_1'^4.$$

You are advised to memorise these results also.

(b) Conversely we derive below moments about any point in terms of central moments,

$$\mu_r' = \frac{1}{N} \sum f_i (x_i - A)^r = \frac{1}{N} \sum f_i (x_i - \bar{X} + \bar{X} - A)^r$$

Putting  $x_i - \bar{X} = z_i$ 

$$\mu_r' = \frac{1}{N} \sum f_i (z_i + \bar{X} - A)^r$$

But  $\bar{X} - A = \mu_1'$ 

$$\therefore \mu_r' = \frac{1}{N} \sum f_i (z_i + \mu_1')^r$$

$$\begin{aligned} \therefore \mu_r' &= \frac{1}{N} \sum f_i [z_i^r + r C_1 z_i^{r-1} \mu_1' + r C_2 z_i^{r-2} \mu_1'^2 + \dots + \mu_1'^r] \\ &= \mu_r + r C_1 \mu_{r-1}' \mu_1' + r C_2 \mu_{r-2}' \mu_1'^2 + r C_3 \mu_{r-3}' \mu_1'^3 + \dots + \mu_1'^r. \end{aligned}$$

In particular, putting  $r = 1, 2, 3, \dots$ 

$$\mu_1' = \mu_1 + \mu_0 \mu_1' = 0 + \mu_1' = \mu_1'$$

$$\mu_2' = \mu_2 + 2\mu_1 \mu_1' + \mu_0 \mu_1'^2 = \mu_2 + \mu_1'^2 \quad [\because \mu_1 = 0, \text{ and } \mu_0 = 1]$$

$$\mu_3' = \mu_3 + 3\mu_2 \mu_1' + 3\mu_1 \mu_1'^2 + \mu_0 \mu_1'^3$$

$$= \mu_3 + 3\mu_2 \mu_1' + \mu_1'^3$$

$$\mu_4' = \mu_4 + 4\mu_3 \mu_1' + 6\mu_2 \mu_1'^2 + 4\mu_1 \mu_1'^3 + \mu_0 \mu_1'^4$$

$$= \mu_4 + 4\mu_3 \mu_1' + 6\mu_2 \mu_1'^2 + \mu_1'^4$$

You are advised to memorise these results also.

### 13. Moment Generating Function

(a) Definition (Discrete Random Variable) : The moment generating function (m.g.f.) of discrete random variate  $X$  about  $a$  denoted by  $M_a(t)$  is defined by

$$M_a(t) = E[e^{t(x-a)}] \quad \therefore \quad M_a(t) = \sum p_i e^{t(x_i-a)}$$

The m.g.f. is a function of the real parameter  $t$ . The subscript  $a$  shows the point about which the m.g.f. is taken.

Expanding the exponential in (1), we get

$$\begin{aligned} M_a(t) &= \sum p_i \left[ 1 + \frac{t}{1!}(x_i - a) + \frac{t^2}{2!}(x_i - a)^2 + \frac{t^3}{3!}(x_i - a)^3 + \dots \right] \\ &= \sum p_i + \frac{t}{1!} \sum p_i (x_i - a) + \frac{t^2}{2!} \sum p_i (x_i - a)^2 + \frac{t^3}{3!} \sum p_i (x_i - a)^3 + \dots \end{aligned}$$

But  $\sum p_i (x_i - a)^r$  is the  $r$ -th moment of  $X$  about  $a$  i.e.,  $\mu'_r$ . Hence, we have

$$M_a(t) = 1 + \mu'_1 \cdot \frac{t}{1!} + \mu'_2 \cdot \frac{t^2}{2!} + \mu'_3 \cdot \frac{t^3}{3!} + \dots + \mu'_r \cdot \frac{t^r}{r!} + \dots$$

Thus, the coefficient of  $(t^r/r!)$  is the  $r$ -th moment of  $X$  about  $a$  i.e.,  $\mu'_r$ . In this way  $M_a(t)$  generates moments. This is the reason why the function  $M_a(t)$  is called the **moment generating function**.

(b) The moment generating function about the origin is denoted by  $M_0(t)$ . Thus, for a discrete random variable

$$M_0(t) = \sum p_i e^{tx_i}$$

If we take the logarithm of both sides and denote it by  $L(t)$ , then

$$L(t) = \log M_0(t) = \log \sum p_i e^{tx_i}$$

Differentiating both sides w.r.t.  $x$ ,

$$L'(t) = \frac{\sum p_i x_i e^{tx_i}}{\sum p_i e^{tx_i}}$$

Putting  $t = 0$ , we get

$$L'(0) = \frac{\sum p_i x_i}{\sum p_i} = \sum p_i x_i = \mu_1 \quad [\because \sum p_i = 1]$$

Differentiating again w.r.t.  $t$

$$L''(t) = \frac{\sum p_i e^{tx_i} \cdot \sum p_i e^{tx_i} \cdot x_i^2 - \sum p_i e^{tx_i} x_i \cdot \sum p_i e^{tx_i} \cdot x_i}{(\sum p_i e^{tx_i})^2}$$

Putting  $t = 0$ , we get

$$L''(0) = \frac{\sum p_i \sum p_i x_i^2 - (\sum p_i x_i)^2}{(\sum p_i)^2}$$

$$\therefore L''(0) = \sum p_i x_i^2 - (\sum p_i x_i)^2 = \mu_2 - \mu_1^2 = \mu_2 \quad [\because \sum p_i = 1]$$

Thus, the mean =  $L'(0) = \mu_1$  and variance =  $L''(0) = \mu_2$ .

(c) Definition (Continuous Random Variable) : The moment generating function (m.g.f.) of a continuous random variate  $X$  about  $a$  denoted  $M_a(t)$  is defined by

$$M_a(t) = E[e^{t(x-a)}]$$

where  $f(x)$  is the p.d.f. of  $X$ .

Expanding the exponential in (3), we get,

$$\begin{aligned} M_a(t) &= \int_{-\infty}^{\infty} f(x) \left[ 1 + \frac{t}{1!}(x-a) + \frac{t^2}{2!}(x-a)^2 + \frac{t^3}{3!}(x-a)^3 + \dots \right] dx \\ &= \int_{-\infty}^{\infty} f(x) dx + \frac{t}{1!} \int_{-\infty}^{\infty} (x-a)f(x) dx \\ &\quad + \frac{t^2}{2!} \int_{-\infty}^{\infty} (x-a)^2 f(x) dx + \frac{t^3}{3!} \int_{-\infty}^{\infty} (x-a)^3 f(x) dx + \dots \end{aligned} \quad (3a)$$

But  $\int_{-\infty}^{\infty} (x-a)^r f(x) dx$  is the  $r$ -th moment  $\mu_r$  of  $X$  about  $a$ . Hence,

$$M_a(t) = 1 + \mu_1 \cdot \frac{t}{1!} + \mu_2 \cdot \frac{t^2}{2!} + \mu_3 \cdot \frac{t^3}{3!} + \dots + \mu_r \cdot \frac{t^r}{r!} + \dots \quad (4)$$

Thus, the coefficient of  $(t^r/r!)$  is the  $r$ -th moment of  $X$  about  $a$ .

(d) To find moments of various orders from m.g.f. : It is clear from (2) and (4) that the moment of order  $r$  is the coefficient of  $(t^r/r!)$  in the expansion of m.g.f. Hence, one way of obtaining various moments is to obtain expansion of the m.g.f. of  $X$  and find the coefficient of  $(t^r/r!)$  in the expansion.

However, in practice many a time obtaining the expansion of m.g.f. is not convenient. In such cases we differentiate m.g.f. w.r.t.  $t$  for  $r$  times and equate it to zero to get  $\mu_r$ .

Thus, differentiating  $M_a(t)$  from (2) (or from 4), successively, we get;

$$\frac{d}{dt} [M_a(t)] = \mu_1' + \mu_2' t + \mu_3' \frac{t^2}{2!} + \dots$$

$$\text{Putting } t = 0, \quad \frac{d}{dt} [M_a(t)]_{t=0} = \mu_1'$$

$$\frac{d^2}{dt^2} [M_a(t)] = \mu_2' + \mu_3' t + \mu_4' \frac{t^2}{2!} + \dots$$

$$\text{Putting } t = 0, \quad \frac{d^2}{dt^2} [M_a(t)]_{t=0} = \mu_2'$$

$$\text{In general, } \frac{d^r}{dt^r} [M_a(t)]_{t=0} = \mu_r'$$

(e) Moment generating function about origin : Putting  $a = 0$  in (1), we get,

$$M_0 = \sum p_i e^{tx_i}$$

Putting  $a = 0$  in (3), we get,

$$M_0(t) = \int_{-\infty}^{\infty} e^{tx} f(x) dx$$

Putting  $a = 0$  in (1a), we get since  $\sum p_i x_i^r = \mu_r'$  about the origin.

$$M_0(t) = 1 + \mu_1 t + \mu_2 \frac{t^2}{2!} + \dots + \mu_r \frac{t^r}{r!} + \dots = \sum \mu_r \frac{t^r}{r!}$$

Note ...

It is assumed that the r.h.s. of (5) and (6) is absolutely convergent.

(f) Moment generating function of the sum of two independent random variables : The moment generating function of sum of two independent random variables is equal to the product of the m.g.f.s of the two variates."

Proof : Let  $X, Y$  be two independent random variables then the m.g.f. of their sum  $X+Y$  about the origin is given by

$$\begin{aligned} M_{X+Y}(t) &= E[e^{t(X+Y)}] = E[e^{tX} \cdot e^{tY}] \\ &= E(e^{tX}) \cdot E(e^{tY}) \quad [\because X \text{ and } Y \text{ are independent}] \end{aligned}$$

$$\therefore M_{X+Y}(t) = M_X(t) \cdot M_Y(t)$$

Generalisation : If  $X_1, X_2, \dots, X_n$  are  $n$  independent random variables, then the m.g.f. of their sum is equal to the product of their m.g.f.s

$$M_{X_1+X_2+\dots+X_n}(t) = M_{X_1}(t) \cdot M_{X_2}(t) \dots M_{X_n}(t)$$

(g) Uniqueness of Moment Generating Function : This is a very important property of m.g.f. It states that the m.g.f. of a distribution, if it exists, uniquely determines the distribution. In other words it means that for a given probability distribution there is one and only one m.g.f. and corresponding a given m.g.f. there is one and only one probability distribution. Thus, if m.g.f. of  $X$  and m.g.f. of  $Y$  are equal then  $X$  and  $Y$  must be identical.

**Example 1 :** A random variable  $X$  has probability density function  $1/(2^x)$ ,  $x = 1, 2, 3, \dots$ . Find the m.g.f. and hence, find the mean and variance.

Sol. : Since,  $P(X=x) = \frac{1}{2^x}$ ,  $x = 1, 2, 3, \dots$

$$M_0(t) = E(e^{tx}) = \sum p_i e^{tx}$$

$$\begin{aligned} &= \sum \frac{1}{2^x} e^{tx} = \sum \left( \frac{e^t}{2} \right)^x = \frac{e^t}{2} + \left( \frac{e^t}{2} \right)^2 + \left( \frac{e^t}{2} \right)^3 + \dots \\ &= \frac{e^t}{2} \left[ 1 + \left( \frac{e^t}{2} \right) + \left( \frac{e^t}{2} \right)^2 + \dots \right] = \frac{e^t}{2} \left[ 1 + \frac{e^t}{2} \right]^{-1} \\ &= \frac{e^t}{2} \cdot \frac{1}{1 - (e^t/2)} = \frac{e^t}{2} \cdot \frac{2}{2 - e^t} = \frac{e^t}{2 - e^t} \\ \therefore \mu_1' &= \left[ \frac{d}{dt} M_0(t) \right]_{t=0} = \left[ \frac{(2-e^t)e^t - e^t(-e^t)}{(2-e^t)^2} \right]_{t=0} = 2 \left[ \frac{e^t}{(2-e^t)^2} \right]_{t=0} = 2 \\ \therefore \mu_2' &= \left[ \frac{d^2}{dt^2} M_0(t) \right]_{t=0} = 2 \cdot \left[ \frac{(2-e^t)^2 \cdot e^t - e^t \cdot 2(2-e^t) \cdot (-e^t)}{(2-e^t)^4} \right]_{t=0} \end{aligned}$$

$$\mu_2' = 2 \cdot \left[ \frac{(2-e^t) \cdot e^t + 2e^{2t}}{(2-e^t)^3} \right]_{t=0} = \frac{2(1+2)}{1} = 6$$

$$\mu_2 = \mu_2' - \mu_1'^2 = 6 - 4 = 2,$$

$$\text{Mean} = \text{Variance} = 2.$$

**Example 2 :** If  $X$  denotes the outcome when a fair die is tossed, find M.G.F. of  $X$  and hence, find the mean and variance of  $X$ . (M.U. 2005)

Sol. : We have, here  $X$  taking values 1, 2, 3, 4, 5, 6 each with probability  $1/6$ .

$$M_0(t) = E(e^{tx}) = \sum p_i e^{tx}$$

$$= \frac{1}{6} e^t + \frac{1}{6} e^{2t} + \frac{1}{6} e^{3t} + \dots + \frac{1}{6} e^{6t}$$

$$= \frac{1}{6} (e^t + e^{2t} + \dots + e^{6t})$$

$$\therefore \mu_1' = \left[ \frac{d}{dt} M_0(t) \right]_{t=0} = \frac{1}{6} [e^t + 2e^{2t} + \dots + 6e^{6t}]_{t=0}$$

$$= \frac{1}{6} [1 + 2 + \dots + 6] = \frac{21}{6} = \frac{7}{2}$$

$$\therefore \mu_2' = \left[ \frac{d^2}{dt^2} M_0(t) \right]_{t=0} = \frac{1}{6} [e^t + 4e^{2t} + 9e^{3t} + \dots + 36e^{6t}]_{t=0}$$

$$= \frac{1}{6} [1 + 4 + 9 + \dots + 36] = \frac{91}{6}$$

$$\therefore \mu_2 = \mu_2' - \mu_1'^2 = \frac{91}{6} - \frac{49}{4} = \frac{35}{12}$$

$$\therefore \text{Mean} = \frac{7}{2} \text{ and Variance} = \frac{35}{12}.$$

**Example 3 :** Find the m.g.f. of a random variable  $X$  if the  $n$ -th moment about the origin is given by  $\mu_r' = r!$ .

Sol. : By definition,  $\mu_r' = E(x^r) = r!$

$$\therefore E(x) = 1, E(x^2) = 2!, E(x^3) = 3!, \dots$$

$$\text{Now, } M_0(t) = E(e^{tx}) = E \left[ 1 + tx + \frac{t^2 x^2}{2!} + \frac{t^3 x^3}{3!} + \dots \right]$$

$$= E(1) + tE(x) + \frac{t^2}{2!} E(x^2) + \frac{t^3}{3!} E(x^3) + \dots$$

Putting the values of  $E(x)$ ,  $E(x^2)$ , ..., from (1)

$$\therefore M_0(t) = 1 + t + \frac{t^2}{2!} + \frac{t^3}{3!} + \dots$$

$$= 1 + t + t^2 + t^3 + \dots = (1-t)^{-1} = \frac{1}{1-t}.$$

**Example 4 :** Find the m.g.f. of the random variable  $X$  whose p.m.f. is given by

$$\begin{array}{ccccc} X & : & -2 & 3 & 1 \\ P(X=x) & : & 1/3 & 1/2 & 1/6 \end{array}$$

Also find the first two moments about the origin.

(M.U. 2004)

Sol. : By definition

$$M_0(t) = E(e^{tX}) = \sum P_i e^{tX_i} = \frac{1}{3} e^{-2t} + \frac{1}{2} e^{3t} + \frac{1}{6} e^t$$

$$\text{Now, } \mu_1' = \left[ \frac{d}{dt} M_0(t) \right]_{t=0} = \left[ -\frac{2}{3} e^{-2t} + \frac{3}{2} e^{3t} + \frac{1}{6} e^t \right]_{t=0} = -\frac{2}{3} + \frac{3}{2} + \frac{1}{6} = \frac{6}{6} = 1$$

$$\mu_2' = \left[ \frac{d^2}{dt^2} M_0(t) \right]_{t=0} = \left[ \frac{4}{3} e^{-2t} + \frac{9}{2} e^{3t} + \frac{1}{6} e^t \right]_{t=0} = \frac{4}{3} + \frac{9}{2} + \frac{1}{6} = \frac{36}{6} = 6.$$

**Example 5 :** A continuous random variable  $X$  has the probability distribution  $f(x) = \frac{4}{81} x(9-x^2)$

when  $0 \leq x \leq 3$  and  $f(x) = 0$  otherwise.

Find the first four moments about the origin and the mean.

(M.U. 2004)

Sol. : Moments about the origin

$$\mu_1' = E(X) = \frac{4}{81} \int_0^3 x \cdot x \cdot (9-x^2) dx = \frac{4}{81} \int_0^3 (9x^2 - x^4) dx$$

$$= \frac{4}{81} \left[ 3x^3 - \frac{x^5}{5} \right]_0^3 = \frac{4}{81} \left[ 81 - \frac{243}{5} \right] = \frac{4}{81} \cdot \frac{162}{5} = \frac{8}{5}$$

$$\mu_2' = E(X^2) = \frac{4}{81} \int_0^3 x^2 (9-x^2) dx = \frac{4}{81} \left[ \frac{9x^4}{4} - \frac{x^6}{6} \right]_0^3$$

$$= \frac{4}{81} \left[ \frac{729}{4} - \frac{729}{6} \right] = \frac{4}{81} \cdot 729 \cdot \frac{1}{12} = 3$$

$$\mu_3' = E(X^3) = \frac{4}{81} \int_0^3 x^3 (9-x^2) dx = \frac{4}{81} \left[ \frac{9x^5}{5} - \frac{x^7}{7} \right]_0^3$$

$$= \frac{4}{81} \left[ \frac{9 \times 243}{5} - \frac{9 \times 243}{7} \right] = \frac{216}{35}$$

$$\mu_4' = E(X^4) = \frac{4}{81} \int_0^3 x^4 (9-x^2) dx = \frac{4}{81} \left[ \frac{9x^6}{6} - \frac{x^8}{8} \right]_0^3$$

$$= \frac{4}{81} \left[ \frac{81 \times 81}{6} - \frac{81 \times 81}{8} \right] = \frac{27}{2}$$

The moments about the mean

$$\mu_1 = 0$$

$$\mu_2 = \mu_2' - \mu_1^2 = 3 - \left( \frac{8}{5} \right)^2 = \frac{11}{25}$$

$$\mu_3 = \mu_3' - 3\mu_2' \mu_1 + 2\mu_1^3 = \frac{216}{35} - 3 \cdot \frac{8}{5} + 2 \left( \frac{8}{5} \right)^3 = -\frac{32}{875}$$

$$\mu_4 = \mu_4' - 4\mu_3' \mu_1 + 6\mu_2' \mu_1^2 - 3\mu_1^4 = \frac{27}{2} - 4 \cdot \frac{216}{35} \cdot \frac{8}{5} + 6 \cdot \frac{8}{5} \cdot \left( \frac{8}{5} \right)^2 - 3 \left( \frac{8}{5} \right)^4 = \frac{3693}{8750}$$

**Example 6 :** If a random variable has the moment generating function  $M_t = \frac{3}{3-t}$ , obtain the mean and the standard deviation.

Sol. : We have

$$\text{Now, } M_0(t) = \frac{3}{3-t} = \frac{3}{3[1-(t/3)]} = \left( 1 - \frac{t}{3} \right)^{-1} = 1 + \frac{t}{3} + \frac{t^2}{9} + \frac{t^3}{27} + \dots$$

$$\text{Mean} = E(X) = \text{Coefficient of } \frac{t}{3} = \frac{1}{3}$$

$$\mu_2' = E(X^2) = \text{Coefficient of } \frac{t^2}{9} = \frac{2}{9}$$

$$\therefore \text{Var}(X) = \mu_2' - \mu_1^2 = \frac{2}{9} - \frac{1}{9} = \frac{1}{9}. \quad \therefore \text{S.D.} = \frac{1}{3}.$$

### EXERCISE - VII

1. A random variable takes values  $X = 0, 1$  with probabilities  $q$  and  $p$  respectively, such that  $q + p = 1$ . Find the moment generating function of  $X$  and show that all moments about the origin are equal to  $p$ .

$$[\text{Ans. : } M_0(t) = qe^0 + pe^t = 1 + (e^t - 1)p = 1 + \left( t + \frac{t^2}{2!} + \frac{t^3}{3!} + \dots \right) \cdot p \quad \therefore \mu_r' = p]$$

2. A random variable  $X$  has the m.g.f. given by  $M_0(t) = \frac{2}{2-t}$ . Find the standard deviation of  $X$ .

$$[\text{Ans. : } \sigma = 1/2]$$

3. A random variable  $X$  has the probability distribution

$$P(X=x) = \frac{1}{8} {}^3C_x, \quad x = 0, 1, 2, 3.$$

Find the moment generating function of  $X$  and then find mean and variance. (M.U. 2003)

$$[\text{Ans. : (I) } \frac{1}{8}(1+e^t), \text{ (II) } \frac{3}{2}, \frac{3}{4}]$$

4. A random variable  $X$  has p.d.f.  $f(x) = 1, \quad 0 < x < 1$ .

Find m.g.f. and  $\mu_r'$ .

$$[\text{Ans. : } \mu_r' = \frac{1}{r+1}]$$

5. A random variable  $X$  has the following probability distribution.

$$\begin{array}{cccc} X & : & 0 & 1 & 2 & 3 \\ P(X=x) & : & 1/6 & 1/3 & 1/3 & 1/6 \end{array}$$

- Compute (i) Moment generating function about the origin, (ii) first four raw moments, (iii) first four central moments.
- [Ans. : (i)  $\frac{1}{6} + \frac{1}{3}e^t + \frac{1}{3}e^{2t} + \frac{1}{6}e^{3t}$ , (ii)  $\frac{3}{2}, \frac{19}{6}, \frac{15}{2}, \frac{115}{6}$ , (iii)  $0, \frac{11}{12}, 0, 1729$ .]
6. A random variable  $X$  has the following probability distribution.
- $$\begin{array}{c|ccc} X = x & 0 & 1 & 2 \\ \hline P(X=x) & 1/3 & 1/3 & 1/3 \end{array}$$
- Find (i) the moment generating function, (ii) the first four raw moments, (iii) the first four central moments.
- [Ans. : (i)  $\frac{1}{3}(1 + e^t + e^{2t})$ , (ii)  $1, \frac{5}{3}, \frac{9}{3}, \frac{17}{3}$ , (iii)  $0, \frac{2}{3}, 0, \frac{2}{3}$ .]
7. A random variable  $X$  has the following density function
- $$f(x) = \begin{cases} ke^{-kx}, & x > 0, k > 0 \\ 0, & x \leq 0 \end{cases}$$
- Find the m.g.f. and hence, its mean and variance.
- [Ans. :  $M_0(t) = \frac{k}{k-t}; t \neq 2, \mu_1 = \frac{1}{k}, \mu_2 = \frac{1}{k^2}$ ]
8. Find the m.g.f. of the random variable having the following probability density function. Also find the mean and variance.
- (i)  $f(x) = \begin{cases} 1/2, & -1 \leq x < 1 \\ 0, & \text{elsewhere} \end{cases}$  (ii)  $f(x) = \begin{cases} e^{-(x-5)}, & x \geq 5 \\ 0, & \text{elsewhere} \end{cases}$
- [Ans. : (i)  $\frac{(e^t - e^{-t})}{2t}, 0, \frac{1}{3}$ ; (ii)  $\frac{e^{5t}}{1-t}, 6, 1$ ]

**EXERCISE - VIII****Theory**

- Define the following terms giving suitable illustrations.
  - Random Variable.
  - Discrete Random Variable.
  - Continuous Random Variable.
  - Probability Distribution of a random variable.
  - Distribution Function of a discrete random variable.
- State the properties of probability density function must satisfy.
- State some important properties of a distribution function.
- State the relation between probability mass function and distribution function of a random variable. Give an example.
- Explain the following terms .
  - Discrete Random Variable.
  - Probability distribution of a random variable.

(M.U. 1998)

- Define mathematical expectation.
- Define expectation of a function of a random variable  $X$ .
  - when  $X$  is a discrete r.v., (b) when  $X$  is a continuous r.v.
- Explain the following terms :
  - Expectation of a random variable.
  - Variance of a random variable.
- Define Moment Generating Function of a random variable  $X$  about  $a$  and explain how you will get moments from it.
- Define  $r$ th moment about any point and find the first four moments about the mean.
- Derive the formulae for  $r$ th moment about any point and  $r$ th moment about the mean.
- If  $L(t) = \log M(t)$  where  $M(t)$  is the m.g.f. of a discrete random variable, then prove that mean =  $L'(0)$  and variance =  $L''(0)$ .

(M.U. 1998)

(M.U. 1999)

(M.U. 2006)





## Some Standard Distributions

### 1. Introduction

In this chapter we shall study some standard probability distributions. Study of such theoretical distributions is the foundation for the development of further topics. The first two distributions are discrete while the third is continuous.

### 2. Binomial Distribution

This was discovered by James Bernoulli's in 1700 and it expresses probabilities of events of dichotomous (dicho + tomy = two parts) nature i.e., which results in only two ways, success or failure.

(a) To Derive Binomial Distribution : Consider an experiment which results in either success or failure. Let it be repeated  $n$  times, the probability  $p$  of success remaining constant every time and let  $q = 1 - p$ , the probability of failure.

The probability of  $x$  successes and hence  $(n-x)$  failures in a trial in a particular order say,  $SSS \dots (x \text{ times}) \times FFF \dots (n-x \text{ times})$ , as given by the multiplication theorem on probability, is

$$= ppp \dots (x \text{ times}) \times qqq \dots (n-x \text{ times}) \\ = p^x q^{n-x}$$

But  $x$  successes can occur in  ${}^n C_x$  ways and the probability of each of these ways is the same viz.  $p^x q^{n-x}$ . Hence, the probability of  $x$  successes in any order by the addition theorem is  ${}^n C_x p^x q^{n-x}$ .

Hence,  $P(x) = {}^n C_x p^x q^{n-x}, x = 0, 1, 2, \dots, n$ .

This is Binomial distribution.

(b) Definition : A random variable is said to follow Binomial distribution if probability of  $x$  is given by

$$P(X=x) = {}^n C_x p^x q^{n-x}, \quad x = 0, 1, 2, 3, \dots, n \quad \text{and} \quad q = 1 - p$$

The two constants  $n$  and  $p$  are called the parameters of the distribution.

(The meanings of 'success' and 'failure' are quite arbitrary. We may call 'a fatal accident' or 'getting infected by a disease' or 'premature delivery' a success!).

Remarks ...

1. The sum of the probabilities is 1.

$$\sum_{x=0}^n P(x) = \sum_{x=0}^n {}^n C_x p^x q^{n-x} = {}^n C_0 q^n + {}^n C_1 q^{n-1} p + {}^n C_2 q^{n-2} p^2 + \dots + p^n \\ = (q+p)^n = 1$$

(M.U. 1998)

2. Let the experiment of  $n$  trials be repeated  $N$  times. Then we expect  $x$  successes to occur  $N \cdot {}^n C_x p^x q^{n-x}$  times. This is called frequency function. The expected frequencies of 0, 1, 2, ...,  $n$  successes are the successive terms of the binomial expansion  $N(q+p)^n$ .

3. If  $x$  is a binomial variate with parameters  $n$  and  $p$ , it is denoted as  $b(x, n, p)$ .

4. The distribution is called "Binomial Distribution" because the probabilities  ${}^n C_x p^x q^{n-x}$ ,  $x = 0, 1, 2, \dots, n$  are the successive terms of the expansion of the binomial expression  $(q+p)^n$ .

(c) When do we get binomial distribution ?

As is clear from the previous discussion, we get a binomial distribution when the following conditions are satisfied :

- (i) A trial is repeated  $n$  times where  $n$  is a finite number.
- (ii) Each trial results only in two ways-success or failure.
- (iii) These possibilities are mutually exclusive, exhaustive but not necessarily equally likely.
- (iv) If  $p$  and  $q$  are the probabilities of success and failure then  $p+q=1$ .
- (v) The events are independent, i.e., the probability  $p$  of success in each trial remains constant in all trials.

(d) Uses : Naturally, we can use binomial distribution when these conditions are satisfied. Thus, in problems involving (i) the tossing of a coin-heads or tails, (ii) the result of an examination-success or failure, (iii) the result of an election-success or failure, (iv) the result of inspection of an article-defective or non-defective, (v) habit of a person-smoker or non-smoker etc. binomial distribution can be used if other conditions are also satisfied.

(e) Mean and Variance : The first two moments about the origin are obtained as follows.

(M.U. 2003, 05)

$$\mu_1' = E(X) = \sum p_i x_i = \sum_{x=0}^n {}^n C_x p^x q^{n-x} \cdot x \\ = {}^n C_0 p^0 q^n + 0 \cdot {}^n C_1 p q^{n-1} + 1 \cdot {}^n C_2 p^2 q^{n-2} + 2 + \dots + p^n \cdot n \\ = npq^{n-1} + \frac{n(n-1)}{2!} \cdot p^2 q^{n-2} + 2 + \dots + p^n \cdot n \\ = np \left[ q^{n-1} + (n-1) q^{n-2} \cdot p + \frac{(n-1)(n-2)}{2!} q^{n-3} p^3 + \dots + p^{n-1} \right] \\ = np[q+p]^{n-1} = np, \quad [\because p+q=1]$$

$$\mu_2' = E(X^2) = \sum p \cdot x^2 = \sum {}^n C_x p^x q^{n-x} \cdot x^2$$

But  $x^2$  can be written as  $x^2 = x + x(x-1)$

$$\therefore \mu_2' = \sum [x + x(x-1)] {}^n C_x p^x q^{n-x} \\ = \sum x {}^n C_x p^x q^{n-x} + \sum x(x-1) {}^n C_x p^x q^{n-x}$$

But the first term on the r.h.s. is  $np$  as shown above.

$$\therefore \mu_2' = np + [0 \cdot {}^n C_0 p^0 q^n + 0 \cdot {}^n C_1 p^1 q^{n-1} + 2 \cdot 1 \cdot {}^n C_2 p^2 q^{n-2} + 3 \cdot 2 \cdot {}^n C_3 p^3 q^{n-3} + \dots] \\ = np + 2 \cdot \frac{n(n-1)}{2!} p^2 q^{n-2} + 3 \cdot 2 \cdot \frac{n(n-1)(n-2)}{3!} p^3 q^{n-3} \\ + 4 \cdot 3 \cdot \frac{n(n-1)(n-2)(n-3)}{4!} p^4 q^{n-4} + \dots$$

$$\begin{aligned} \therefore \mu_2' &= np + n(n-1)p^2q^{n-2} + n(n-1)(n-2)p^3q^{n-3} \\ &\quad + \frac{n(n-1)(n-2)(n-3)}{2!} p^4q^{n-4} + \dots \\ &= np + n(n-1)p^2 \left[ q^{n-2} + (n-2)pq^{n-3} + \frac{(n-2)(n-3)}{2!} p^2q^{n-4} + \dots \right] \\ &= np + n(n-1)p^2(q+p)^{n-2} = np + n(n-1)p^2 \\ &= np[1 + (n-1)p] = np[1 - p + np] \\ &= np[q + np] = npq + n^2p^2 \\ \therefore \mu_2 &= \mu_2' - \mu_1'^2 = npq \end{aligned}$$

∴ Mean =  $np$  and Variance =  $npq$

(f) Moment Generating Function about origin : By definition m.g.f. about origin is

$$\begin{aligned} M_0(t) &= E(e^{tX}) = \sum p_i e^{tx_i} \quad [\text{See (2A), page 6-44}] \quad (\text{M.U. 2015}) \\ &= \sum {}^n C_x p^x q^{n-x} e^{tx} = \sum {}^n C_x q^{n-x} \cdot (pe^t)^x \\ &= (q + pe^t)^n \end{aligned}$$

[Note that  $\sum {}^n C_x a^{n-x} b^x = {}^n C_0 a^n + {}^n C_1 a^{n-1} b + {}^n C_2 a^{n-2} b^2 + \dots = (a+b)^n$ .]

Differentiating  $M_0(t)$  and putting  $t=0$ , we get the required moments.

$$\text{Now, } \frac{d}{dt}[M_0(t)] = n(q+pe^t)^{n-1} pe^t = np[e'(q+pe^t)^{n-1}]$$

$$\therefore \left[ \frac{d}{dt} M_0(t) \right]_{t=0} = np(q+p) = np$$

$$\begin{aligned} \frac{d^2}{dt^2}[M_0(t)] &= np[e'(n-1)(q+pe^t)^{n-2} pe^t + e'(q+pe^t)^{n-1}] \\ &= nppe'(q+pe^t)^{n-2} [e'(n-1)p + (q+pe^t)] \end{aligned}$$

$$\begin{aligned} \therefore \left[ \frac{d^2}{dt^2} M_0(t) \right]_{t=0} &= np(q+p)[(n-1)p + (q+p)] \\ &= np(np-p+1) = np(np+q) = npq + n^2p^2 \end{aligned}$$

$$\therefore \mu_2 = \mu_2' - \mu_1'^2 = npq.$$

#### (g) Additive property of Binomial Distribution :

(1) If  $X_1$  is a Binomial variate with parameter  $n_1$  and  $p_1$  and  $X_2$  is another Binomial variate with parameter  $n_2$  and  $p_2$  then  $X_1 + X_2$  in general is not a Binomial variate.

Proof : Since  $X_1, X_2$  are Binomial with parameters  $n_1, p_1$  and  $n_2, p_2$

$$M_{X_1}(t) = (q_1 + p_1 e^t)^{n_1}; \quad M_{X_2}(t) = (q_2 + p_2 e^t)^{n_2}$$

Since,  $X$  and  $Y$  are independent

$$M_{X_1+X_2}(t) = M_{X_1}(t) \cdot M_{X_2}(t) = (q_1 + p_1 e^t)^{n_1} \cdot (q_2 + p_2 e^t)^{n_2}$$

But this cannot be expressed in the form  $(q + pe^t)^n$ . Hence,  $X_1 + X_2$  is not a Binomial variate. Thus, the sum of two independent Binomial variates is not a Binomial variate. In other words, Binomial distribution does not possess additive property. (However if  $p_1 = p_2$ , we get the additive property).

(2) If  $X_1$  and  $X_2$  are two Binomial variates with parameters  $n_1, p$  and  $n_2, p$  then  $X_1 + X_2$  is a Binomial variate with parameters  $(n_1 + n_2), p$ .

We have,  $M_{X_1}(t) = (q + pe^t)^{n_1}, M_{X_2}(t) = (q + pe^t)^{n_2}$

$$\begin{aligned} \therefore M_{X_1+X_2}(t) &= M_{X_1}(t) \cdot M_{X_2}(t) \\ &= (q + pe^t)^{n_1} \cdot (q + pe^t)^{n_2} \\ &= (q + pe^t)^{n_1+n_2} \end{aligned}$$

∴  $X_1 + X_2$  is a Binomial variate with parameters  $(n_1 + n_2), p$ .

Example 1 : Find the mean of the probability distribution of the number of heads obtained in three flips of a balanced coin.

Sol. : We have  $p = 1/2, n = 3$

$$\therefore \text{Mean} = E(X) = np = 3 \times \frac{1}{2} = 1.5$$

Example 2 : What is the expectation of heads if an unbiased coin is tossed 12 times ?

Sol. : Since the expectation of  $x$  in a binomial distribution is given by  $E(X) = np$  and  $n = 12, p = 1/2$ . We could expect  $12 \times (1/2)$  i.e. 6 heads.

Example 3 : If  $X$  is Binomially distributed with  $E(X) = 2$  and  $\text{Var}(X) = 4/3$ , find the probability distribution of  $X$ . (M.U. 2004, 16, 17)

Sol. : We have  $E(X) = np = 2$  and  $\text{Var}(X) = npq = 4/3$ .

$$\therefore \frac{npq}{np} = \frac{4/3}{2} \quad \therefore q = \frac{2}{3} \quad \therefore p = 1 - q = \frac{1}{3}$$

$$\text{But } np = 2, \quad \therefore n \cdot \frac{1}{3} = 2 \quad \therefore n = 6$$

Hence, the distribution is

$$P(X=x) = {}^n C_x p^x q^{n-x} = {}^6 C_x \left(\frac{1}{3}\right)^x \left(\frac{2}{3}\right)^{6-x}$$

Putting  $x = 0, 1, 2, \dots, 6$ , we get the following probability distribution of  $X$ .

$x$	0	1	2	3	4	5	6
$P(X=x)$	64/729	192/729	240/729	160/729	60/729	12/729	1/729

Example 4 : Prove that for all Binomial distributions with the same parameter  $n$ , the variance is maximum when  $p = 1/2$ .

Sol. : We have for Binomial distribution

$$P(x) = {}^n C_x p^x q^{n-x}$$

And the variance is given by  
 $V = npq$  where,  $q = 1 - p$   
 $\therefore V = np(1-p) = np - np^2$

$$\text{For maxima, } \frac{dV}{dp} = 0 \text{ and } \frac{d^2V}{dp^2} = -np$$

Now,  $\frac{dV}{dp} = n - 2np$  and  $\frac{d^2V}{dp^2} = -2n$ , always -ve.

$$\therefore \frac{dV}{dp} = 0 \text{ gives } n - 2np = 0 \quad \therefore n(1 - 2p) = 0$$

$$\therefore n \neq 0 \quad \therefore 1 - 2p = 0 \quad \therefore p = \frac{1}{2}$$

Hence, the variance is maximum when  $p = \frac{1}{2}$ .

**Example 5:** The mean and variance of a Binomial distribution are 4 and 4/3. Find the distribution and the probability of atleast one success. (M.U. 2010)

Sol.: We have  $E(X) = np = 4$ ,  $V(X) = npq = 4/3$

$$\therefore \frac{npq}{np} = \frac{4/3}{4} = \frac{1}{3} \quad \therefore q = \frac{1}{3} \quad \therefore p = \frac{2}{3}$$

$$\therefore np = 4 \quad \therefore n \cdot \frac{2}{3} = 4 \quad \therefore n = 6.$$

The distribution is

$$P(X=x) = {}^nC_x p^x q^{n-x} = {}^6C_x \left(\frac{2}{3}\right)^x \left(\frac{1}{3}\right)^{6-x}$$

x	0	1	2	3	4	5	6
P(X=x)	$\frac{1}{729}$	$\frac{12}{729}$	$\frac{60}{729}$	$\frac{160}{729}$	$\frac{240}{729}$	$\frac{192}{729}$	$\frac{64}{729}$

$$P(\text{atleast one success}) = 1 - P(0 \text{ success}) = 1 - \frac{1}{729} = \frac{728}{729}.$$

(Compare Ex. 3 with Ex. 5.)

**Example 6:** Find the Binomial distribution if the mean is 4 and variance is 3. (M.U. 2005)

Sol.: We have mean =  $np = 4$  and variance =  $npq = 3$ .

$$\begin{aligned} \therefore \frac{np}{npq} &= \frac{4}{3} \quad \therefore \frac{1}{q} = \frac{4}{3} \quad \therefore q = \frac{3}{4} \quad \therefore p = 1 - q = 1 - \frac{3}{4} = \frac{1}{4} \\ \therefore n &= 4 \quad \therefore n \cdot \frac{1}{4} = 4 \quad \therefore n = 16 \end{aligned}$$

$$\therefore P(X=x) = {}^nC_x p^x q^{n-x} = {}^{16}C_x \left(\frac{1}{4}\right)^x \left(\frac{3}{4}\right)^{16-x}$$

**Example 7:** The probability that a man aged 60 will live upto 70 is 0.65. What is the probability that out of 10 such men now at 60 at least 7 will live upto 70? (M.U. 2003, 07)

Sol.:  $P(\text{man will live upto 70}) = 0.65$

$P(\text{man will not live upto 70}) = 0.35$ .

We have  $n = 10$ ,  $p = 0.65$ ,  $q = 0.35$ .

$$\therefore P(X=x) = {}^{10}C_x (0.65)^x (0.35)^{10-x}$$

$$\begin{aligned} P(\text{at least 7 will survive}) &= P(X=7) + P(X=8) + P(X=9) + P(X=10) \\ &= \sum_{x=7}^{10} {}^{10}C_x (0.65)^x (0.35)^{10-x} \end{aligned}$$

**Example 8:** In a Binomial distribution the mean is 5 and the standard deviation is 3\*. Find the fallacy if any in this statement. (M.U. 1996)

Sol.: For a Binomial distribution the mean =  $np = 5$  and variance =  $npq = 9$ .

$$\therefore \frac{np}{npq} = \frac{5}{9} \quad \therefore \frac{1}{q} = \frac{5}{9} \quad \therefore q = \frac{9}{5} = 1.8$$

This is the probability of failure and probability of an event cannot be greater than 1.

Hence, the statement is wrong.

**Example 9:** With usual notation find  $p$  of Binomial distribution if  $n = 6$ ,  $9P(X=4) = P(X=2)$ . (M.U. 2001, 04)

Sol.: We have  $P(X=x) = {}^nC_x p^x q^{n-x} = {}^6C_x p^x q^{6-x}$

Since,  $9P(X=4) = P(X=2)$

$$\therefore 9{}^6C_4 p^4 q^{6-4} = {}^6C_2 p^2 q^{6-2}$$

$$\therefore {}^6C_4 = {}^6C_2, \quad 9p^2 = q^2 = (1-p)^2$$

$$\therefore 9p^2 = 1 - 2p + p^2 \quad \therefore 8p^2 + 2p - 1 = 0$$

$$\therefore (4p-1)(2p+1) = 0 \quad \therefore p = \frac{1}{4} \text{ or } p = -\frac{1}{2}$$

$$\therefore p = \frac{1}{4} \text{ and } q = \frac{3}{4}.$$

**Example 10:** If  $X$  is Binomially distributed with parameters  $n$  and  $p$ , show that  $E\left(\frac{X}{n} - p\right)^2 = \frac{pq}{n}$ . (M.U. 2009)

Sol.: We have

$$\begin{aligned} E\left(\frac{X}{n} - p\right)^2 &= E\left(\frac{X^2}{n^2} - \frac{2X}{n}p + p^2\right) \\ &= E\left(\frac{X^2}{n^2}\right) - E\left(\frac{2X}{n}p\right) + E(p^2) \\ &= \frac{1}{n^2} E(X^2) - \frac{2p}{n} E(X) + p^2 E(1) \end{aligned} \quad (1)$$

For Binomial distribution  $E(X) = np$  and  $\text{Var}(X) = npq$   
 $\therefore E(X^2) = \text{Var}(X) + [E(X)]^2 = npq + n^2 p^2$  and  $E(X) = np$

$\therefore$  From (1),

$$\begin{aligned} E\left(\frac{X}{n} - p\right)^2 &= \frac{1}{n^2} (npq + n^2 p^2) - \frac{2p}{n} \cdot np + p^2 \\ &= \frac{pq}{n} + p^2 - 2p^2 + p^2 = \frac{pq}{n}. \end{aligned}$$

**Example 11 :** What is the mean and variance of the Binomial Distribution  
 $(0.3 + 0.7)^{10}$ ,  $q = 0.3$ ?

Sol. : Here,  $p = 0.7$ ,  $q = 0.3$ ,  $n = 10$ .

$$\therefore \text{Mean} = np = 10 \times 0.7 = 7$$

$$\therefore \text{Variance} = npq = 10 \times 0.3 \times 0.7 = 2.1.$$

**Example 12 :** A factory turns out an article by mass production methods. From the experience it is found that 20 articles on an average are rejected out of every batch of 100. Find the mean and the variance of the number of rejected articles.  
(M.U. 1997)

Sol. : The number of rejected articles in a batch is a Binomial variate with  $n = 100$  and  $p = \frac{20}{100} = 0.2$ .

Hence, the mean of the distribution  $= np = 100 \times \frac{2}{10} = 20$ .

$$\text{Variance} = \sqrt{npq} = \sqrt{100 \times 0.2 \times 0.8} = \sqrt{16} = 4.$$

**Example 13 :** The ratio of the probability of 3 successes in 5 independent trials to the probability of 2 successes in 5 independent trials is  $1/4$ . What is the probability of 4 successes in 6 independent trials?  
(M.U. 2005, 10)

Sol. : For a Binomial distribution  $P(X=x) = {}^n C_x p^x q^{n-x}$

$$\text{When } n = 5, x = 3, \quad P(X=3) = {}^5 C_3 p^3 q^2$$

$$\text{When } n = 5, x = 2, \quad P(X=2) = {}^5 C_2 p^2 q^3$$

The ratio of these probabilities is  $1/4$ .

$$\therefore \frac{P(X=3)}{P(X=2)} = \frac{{}^5 C_3 p^3 q^2}{{}^5 C_2 p^2 q^3} = \frac{1}{4}$$

Since,  ${}^5 C_3 = {}^5 C_2$ , we get

$$\frac{p}{q} = \frac{1}{4} \quad \therefore \frac{p}{1-p} = \frac{1}{4} \quad \therefore 4p = 1-p$$

$$\therefore 5p = 1 \quad \therefore p = \frac{1}{5} \quad \therefore q = 1-p = \frac{4}{5}$$

$$\therefore P(X=x) = {}^n C_x \left(\frac{1}{5}\right)^x \left(\frac{4}{5}\right)^{n-x}$$

$$\text{When } n = 6 \text{ and } x = 4, \quad P(X=4) = {}^6 C_4 \left(\frac{1}{5}\right)^4 \cdot \left(\frac{4}{5}\right)^2.$$

**Example 14 :** A biased coin is tossed  $n$  times. Prove that the probability of getting even number of heads is  $0.5 [1 + (q-p)^n]$ .

Sol. : Let  $P(\text{head}) = p \quad \therefore q = 1-p$ .

(M.U. 2004)

$$\therefore P(\text{even head}) = P(0, 2, 4, 6, \dots \text{heads})$$

$$= {}^n C_0 p^0 q^n + {}^n C_2 p^2 q^{n-2} + {}^n C_4 p^4 q^{n-4} + \dots$$

$$\text{Now, } (p+q)^n = {}^n C_0 p^0 q^n + {}^n C_1 p^1 q^{n-1} + \dots + 1^n = 1$$

$$\text{and } (q-p)^n = {}^n C_0 q^n p^0 - {}^n C_1 q^{n-1} p + {}^n C_2 q^{n-2} p^2 - \dots$$

$$\text{By addition } 2[{}^n C_0 p^0 q^n + {}^n C_2 p^2 q^{n-2} + \dots] = 1 + (q-p)^n$$

$$\therefore \text{Required Probability} = \frac{1}{2} [1 + (q-p)^n].$$

**Example 15 :** If  $m$  things are distributed among 'a' men and 'b' women, show that the probability that the number of things received by men is odd is

$$\frac{1}{2} \left[ \frac{(b+a)^m - (b-a)^m}{(b+a)^m} \right]$$

(M.U. 2004, 05)

Sol. : There are 'a' men and 'b' women. Hence, the probability that a man will be selected for giving that thing is  $P = \frac{a}{a+b}$ .

The probability that a woman will be selected for giving that thing is  $q = \frac{b}{a+b}$  where  $p+q=1$ .

Now, the probability of giving  $r$  things to men  $= {}^m C_r p^r q^{m-r}$ ,  $r = 1, 2, 3, \dots$

Since, men are to get odd number of things,  $r = 1, 3, 5, \dots$

$$\therefore P(\text{men receiving odd number of things}) = P(1) + P(3) + P(5) + \dots$$

$$= {}^m C_1 p^1 q^{m-1} + {}^m C_3 p^3 q^{m-3} + \dots$$

$$= \frac{1}{2} [(q+p)^m - (q-p)^m]$$

(Even powers in  $(q+p)^m$  are cancelled by  $(q-p)^m$  and odd powers are added.)

$$\text{But } q+p=1 \text{ and } q-p = \frac{b}{a+b} - \frac{a}{a+b} = \frac{b-a}{b+a}$$

$$\therefore \text{Required Probability} = \frac{1}{2} \left[ 1 - \frac{(b-a)^m}{(b+a)^m} \right] = \frac{1}{2} \left[ \frac{(b+a)^m - (b-a)^m}{(b+a)^m} \right].$$

**Example 16 :** A communication system consists of  $n$  components, each of which functions independently with probability  $p$ . The total system will be able to function effectively if at least one-half of its components are functioning. For what value of  $p$  is a 5-component system more likely to operate effectively than a 3-component system?  
(M.U. 2004, 09)

Sol. : Here, we have a Binomial distribution with parameters  $n$  and  $p$ .

$$\therefore P(X=x) = {}^n C_x p^x q^{n-x}, \quad x = 0, 1, 2, \dots, n$$

$$\begin{aligned} P(\text{5 component system will work effectively}) &= P(X = 3, \text{ or } 4 \text{ or } 5) \\ &= P(X = 3) + P(X = 4) + P(X = 5) \\ &= \sum_{x=3}^5 {}^n C_x p^x q^{n-x} \quad [\because n = 5] \end{aligned}$$

$$\begin{aligned} P(\text{3-component system will work effectively}) &= P(X = 2 \text{ or } 3) \\ &= \sum_{x=2}^3 {}^n C_x p^x q^{n-x} \quad [\because n = 3] \end{aligned}$$

5-component system will work more effectively than 3-component system if

$$\begin{aligned} \sum_{x=3}^5 {}^n C_x p^x q^{n-x} &\geq \sum_{x=2}^3 {}^n C_x p^x q^{n-x} \\ (5C_3 p^3 q^2 + 5C_4 p^4 q + 5C_5 p^5) &\geq (3C_2 p^2 q + 3C_3 p^3) \\ (10p^3(1-p)^2 + 5p^4(1-p) + p^5) &\geq 1(3p^2(1-p) + p^3) \\ 10p^3 - 20p^4 + 10p^5 + 5p^4 - 5p^5 + p^5 - 3p^2 + 3p^3 - p^3 &\geq 0 \\ 6p^5 - 15p^4 + 12p^3 - 3p^2 &\geq 0 \\ 3p^2(2p^3 - 5p^2 + 4p - 1) &\geq 0 \quad \therefore 3p^2(p-1)^2(2p-1) \geq 0 \\ 2p-1 \geq 0 \quad [\because p^2 \geq 0, (p-1)^2 \geq 0] & \\ \therefore p \geq \frac{1}{2} & \text{ is the required value.} \end{aligned}$$

**Example 17 :** It has been claimed that in 60% of all solar heat installations, the utility bill is reduced by atleast one third. Accordingly what are the probabilities that the utility bill will be reduced by atleast one third in (i) four of five installations, (ii) atleast four of five installations.

Sol. : For a Binomial distribution  $P(X=x) = {}^n C_x p^x q^{n-x}$

We have  $n = 5, x = 4, p = 0.6, q = 0.4$ .

$$(i) \therefore P(X=4) = {}^5 C_4 (0.6)^4 (0.4)^1 = 0.259$$

$$\begin{aligned} (ii) P(\text{atleast 4 of 5 installations}) &= P(X \geq 4) = P(X = 4 \text{ or } 5) \\ &= P(X = 4) + P(X = 5) \\ &= {}^5 C_4 (0.6)^4 (0.4)^1 + {}^5 C_5 (0.6)^5 (0.4)^0 \\ &= 0.259 + 0.078 = 0.337. \end{aligned}$$

**Example 18 :** The incidence of an occupational disease in an industry is such that the workers have 20% chance of suffering from it. What is the probability that out of 6 workers chosen at random 4 or more will be suffering from the disease?

Sol. : We have  $p = 20\% = \frac{20}{100} = 0.2, q = 1-p = 0.8, n = 6$  (M.U. 2005)

$$\begin{aligned} P(X=x) &= {}^n C_x p^x q^{n-x} = {}^6 C_x \left(\frac{1}{5}\right)^x \left(\frac{4}{5}\right)^{6-x} \\ \therefore P(X \geq 4) &= P(X = 4) + P(X = 5) + P(X = 6) \\ &= {}^6 C_4 \left(\frac{1}{5}\right)^4 \left(\frac{4}{5}\right)^2 + {}^6 C_5 \left(\frac{1}{5}\right)^5 \left(\frac{4}{5}\right)^1 + {}^6 C_6 \left(\frac{1}{5}\right)^6 \left(\frac{4}{5}\right)^0 \end{aligned}$$

$$\therefore P(X \geq 4) = \frac{1}{5^6} [15 \cdot 4^2 + 6 \cdot 4 + 1] = \frac{205}{5^6} = \frac{41}{3125}$$

**Example 19 :** The probability that a bomb dropped from a plane will strike the target is  $1/5$ . If six such bombs are dropped, find the probability that (i) exactly two bombs hit the target, (ii) at least two will hit the target.

Sol. : We have  $p = \frac{1}{5}, q = \frac{4}{5}, n = 6$ .

$$\begin{aligned} \text{By Binomial distribution, } P(X=x) &= {}^n C_x p^x q^{n-x} = {}^6 C_x \left(\frac{1}{5}\right)^x \left(\frac{4}{5}\right)^{6-x} \\ \therefore P(2) &= {}^6 C_2 \left(\frac{1}{5}\right)^2 \left(\frac{4}{5}\right)^4 = \frac{6 \cdot 5}{2} \cdot \frac{1}{25} \cdot \frac{256}{625} = \frac{1536}{6250} = 0.24576. \\ P(\text{at least two}) &= 1 - [P(1)] \\ \text{Now, } P(1) &= {}^6 C_1 \left(\frac{1}{5}\right)^1 \left(\frac{4}{5}\right)^5 = 6 \cdot \frac{1}{5} \cdot \frac{1024}{3125} = \frac{6144}{15625} = 0.3932 \\ \therefore P(\text{at least two}) &= 1 - 0.3932 = 0.6068. \end{aligned}$$

**Example 20 :** The probability that at any moment one telephone line out of 10 will be busy is 0.2.

- (i) What is the probability that 5 lines are busy?
- (ii) Find the expected number of busy lines and also find the probability of this number.
- (iii) What is the probability that all lines are busy?

Sol. : We have,  $p = 0.2, q = 0.8, n = 10$ .

By Binomial distribution,  $P(X=x) = {}^n C_x p^x q^{n-x}$

$$\therefore P(X=x) = {}^{10} C_x (0.2)^x (0.8)^{10-x}$$

$$(i) \therefore P(X=5) = {}^{10} C_5 (0.2)^5 (0.8)^5$$

$$(ii) \text{ Expected number of busy lines} = \text{mean} = np = 10 \times \frac{2}{10} = 2.$$

$$P(X=2) = {}^{10} C_2 (0.2)^2 (0.8)^8$$

$$(iii) \text{ Probability of all lines busy} = P(X=10) = {}^{10} C_{10} (0.2)^{10} (0.8)^0 = 0.2^{10}.$$

**Example 21 :** In a precision bombing attack there is a 50% chance that any one bomb will strike the target. Two direct hits are required to destroy the target completely. How many bombs must be dropped to give at least 99% chance of destroying the target?

(M.U. 2003, 04)

Sol. : We have  $p = 1/2$  and  $q = 1/2$ .

The probability distribution of  $X$ , the number of bombs hitting the target is

$$P(X=x) = {}^n C_x \left(\frac{1}{2}\right)^x \left(\frac{1}{2}\right)^{n-x}$$

For completely destroying the target  $X$  must be greater than or equal to 2.

$$\therefore P(X \geq 2) \geq 0.99$$

$$[1 - P(X \leq 1)] \geq 0.99$$

$$[1 - P(X=0) - P(X=1)] \geq 0.99$$

$$\text{But } P(X=0) = {}^n C_0 \left(\frac{1}{2}\right)^0 \left(\frac{1}{2}\right)^n = \left(\frac{1}{2}\right)^n; \quad P(X=1) = {}^n C_1 \left(\frac{1}{2}\right)^1 \left(\frac{1}{2}\right)^{n-1} = n \left(\frac{1}{2}\right)^n$$

$$\therefore \left[1 - \left(\frac{1}{2}\right)^n - n \left(\frac{1}{2}\right)^n\right] \geq \frac{99}{100} \quad \therefore -\left(\frac{1}{2}\right)^n - n \left(\frac{1}{2}\right)^n \geq -0.01$$

$$\therefore \left(\frac{1}{2}\right)^n + n \left(\frac{1}{2}\right)^n \leq \frac{1}{100} \quad \therefore 1+n \leq \frac{2^n}{100} \quad \therefore 2^n \geq 100 + 100 \cdot n$$

We know that  $2^1, 2^2, \dots, 2^{10}, 2^{11}$  are 2, 4, ..., 1024, 2048.

Thus, by trial and error, we find that  $n \geq 11$ .

Hence, minimum 11 bombs are required to destroy the target.

**Example 22 :** Seven dice are thrown 729 times. How many times do you expect at least four dice to show three or five?

Sol. : Probability of getting (3 or 5) in a single toss =  $\frac{1}{6} + \frac{1}{6} = \frac{1}{3}$ . (M.U. 2004, 15, 16)

This is a binomial distribution with  $n = 7$ ,  $p = 1/3$ ,  $q = 2/3$ .

**Example 23 :** Out of 1000 families of 3 Children each, how many would you expect to have 2 boys and 1 girl?

Sol. : Here  $P(\text{Boy}) = p = \frac{1}{2}$ ,  $P(\text{Girl}) = q = \frac{1}{2}$ ,  $n = 3$ ,  $r = 2$ .

$$\therefore P(2 \text{ boys and 1 girl}) = {}^3 C_2 \left(\frac{1}{2}\right)^2 \left(\frac{1}{2}\right)^1 = \frac{3}{8}$$

$$\therefore \text{Expected number of families} = Np = 1000 \times \frac{3}{8} = 375$$

**Example 24 :** If hens of a certain breed lay eggs on 5 days a week on an average; find on how many days during a season of 100 days, a poultry keeper with 5 hens of this breed, will expect receive at least 4 eggs?

Sol. : Probability of an hen laying an egg,  $p = 5/7$  and probability of not laying an egg,  $q = 1-p = 2/7$ .

$$P(X=x) = {}^n C_x p^x q^{n-x} \text{ and } n = 5, p = \frac{5}{7}, q = \frac{2}{7}$$

$$\therefore P(X \geq 4) = P(X=4) + P(X=5)$$

$$= {}^5 C_4 \left(\frac{5}{7}\right)^4 \left(\frac{2}{7}\right)^1 + {}^5 C_5 \left(\frac{5}{7}\right)^5 \left(\frac{2}{7}\right)^0 = 0.5578.$$

$$\text{Expectation} = Np = 100 \times 0.5578 = 55.78 = 56.$$

**Example 25 :** Let  $X, Y$  be two independent binomial variates with parameters  $(n_1 = 6, p = 1/2)$  and  $(n_2 = 4, p = 1/2)$  respectively. Evaluate  $P(X+Y) = 3$ . (M.U. 2004)

Sol. : By the additive property of Binomial variates  $Z = X+Y$  is a Binomial variate with parameters  $n = n_1 + n_2 = 6+4 = 10$  and  $p = 1/2$ .

$$\therefore P(Z) = {}^n C_x p^x q^{n-x}$$

$$\therefore P(Z=3) = {}^{10} C_3 \left(\frac{1}{2}\right)^3 \left(\frac{1}{2}\right)^7 = \frac{15}{128} = 0.1172.$$

**Example 26 :** In the above example, find  $P(X+Y) \geq 3$ . (M.U. 2004)

Sol. : We want,

$$P(Z \geq 3) = 1 - [P(Z=0) + P(Z=1) + P(Z=2)]$$

$$= 1 - \left[ {}^{10} C_0 \left(\frac{1}{2}\right)^0 \left(\frac{1}{2}\right)^{10} + {}^{10} C_1 \left(\frac{1}{2}\right)^1 \left(\frac{1}{2}\right)^9 + {}^{10} C_2 \left(\frac{1}{2}\right)^2 \left(\frac{1}{2}\right)^8 \right]$$

$$= 1 - \left[ \left({}^{10} C_0 + {}^{10} C_1 + {}^{10} C_2\right) \left(\frac{1}{2}\right)^{10} \right]$$

$$= 0.945.$$

**Example 27 :** If  $X$  and  $Y$  are two independent Binomial variates with parameters  $(3, 1/3)$  and  $(5, 1/3)$  respectively. Find  $P(X+Y \geq 1)$ .

Sol. : As above  $Z = X+Y$  is a Binomial variate with parameters  $n = n_1 + n_2 = 3+5 = 8$  and  $p = 1/3$ .

$$P(Z) = {}^n C_x p^x q^{n-x} = {}^8 C_2 (1/3)^2 (2/3)^6$$

$$P(Z=0) = {}^8 C_0 (1/3)^0 (2/3)^8 = (2/3)^8$$

$$P(Z \geq 1) = 1 - P(Z=0) = 1 - (2/3)^8.$$

**Example 28 :** Three fair coins are tossed 3000 times. Find the frequencies of the distribution of heads and tails and tabulate the result. Also calculate the mean and standard deviation of the distribution.

Sol. : We have  $p = \frac{1}{2}$ ,  $q = \frac{1}{2}$ ,  $n = 3$ .

Let  $X$  be the number of heads obtained when the three coins are tossed.

$$\therefore P(X=x) = {}^n C_x p^x q^{n-x} = {}^3 C_x \left(\frac{1}{2}\right)^x \left(\frac{1}{2}\right)^{3-x}$$

Putting  $X = 0, 1, 2, 3$  we get

$$\begin{aligned} P(X=0) &= {}^3C_0 \left(\frac{1}{2}\right)^0 \left(\frac{1}{2}\right)^3 = \frac{1}{8}; & P(X=1) &= {}^3C_1 \left(\frac{1}{2}\right)^1 \left(\frac{1}{2}\right)^2 = \frac{3}{8}; \\ P(X=2) &= {}^3C_2 \left(\frac{1}{2}\right)^2 \left(\frac{1}{2}\right)^1 = \frac{3}{8}; & P(X=3) &= {}^3C_3 \left(\frac{1}{2}\right)^3 \left(\frac{1}{2}\right)^0 = \frac{1}{8}. \end{aligned}$$

$\therefore$  Expected frequency =  $Np$

To obtain frequencies, we multiply these probabilities by 3000.

$X$	0	1	2	3	Total
$f$	375	1125	1125	375	3000

Also Mean =  $np = 3000 \times \frac{1}{2} = 1500$

$$S.D. = \sqrt{npq} = \sqrt{3700 \times \frac{1}{2} \times \frac{1}{2}} = 27.39$$

**Example 29 :** Seven coins are tossed and the number of heads obtained is noted. The experiment is repeated 128 times and the following distribution is obtained.

No. of heads : 0, 1, 2, 3, 4, 5, 6, 7 Total

Frequency : 7, 6, 19, 35, 30, 23, 7, 1 128

(M.U. 1998, 2005, 06)

Fit a Binomial distribution if (i) the coins are unbiased, (ii) if the nature of the coins is not known.

Sol. : To fit a distribution to given data means to find the constants of the distribution which will adequately describe the given situation.

(i) When the coins are unbiased

$$p = \frac{1}{2}, q = \frac{1}{2} \text{ and by data } n = 7 \quad \therefore P(X=x) = {}^7C_x \left(\frac{1}{2}\right)^x \left(\frac{1}{2}\right)^{7-x}$$

Putting  $x = 0, 1, 2, 3, \dots, 7$ , we get

$$P(0) = \frac{1}{2^7}, \quad P(1) = \frac{7}{2^7}, \quad P(2) = \frac{21}{2^7}, \dots$$

Expected frequency =  $Np$  and  $N = 128$ .

Multiplying the above probabilities by 128 i.e. by  $2^7$  we get the expected frequencies as 1, 7, 21, 35, 35, 21, 7, 1.

(ii) When the nature of the coins is not known.

$$\text{We have } \bar{X} = \frac{\sum f_i x_i}{N} = \frac{0 \times 7 + 1 \times 6 + 2 \times 19 + \dots + 7 \times 1}{128} = \frac{433}{128} = 3.38$$

But  $\bar{X} = np$

$$\therefore p = \frac{\bar{X}}{n} = \frac{3.38}{7} = 0.48 \quad \therefore q = 1 - p = 0.52$$

$$\therefore P(X=x) = {}^7C_x (0.48)^x (0.52)^{7-x}$$

Putting  $x = 0, 1, 2, 3, \dots, 7$  we get

$$P(0) = 0.01, \quad P(1) = 0.066, \quad P(2) = 0.184, \dots$$

Multiply these probabilities by 128 we get the expected frequencies as  
1, 8, 23, 36, 33, 18, 6, 3.  
(Last term = 128 - sum of other terms).

**Example 29 :** Fit a Binomial distribution to the following data.

$X$	0	1	2	3	4	5	6
$f$	5	18	28	12	7	6	4

(M.U. 2004, 05, 16)

Sol. : We have  $n = 6$

$$\begin{aligned} N &= 5 + 18 + 28 + 12 + 7 + 6 + 4 = 80 \\ \sum f_i x_i &= 5 \times 0 + 18 \times 1 + 28 \times 2 + 12 \times 3 + 7 \times 4 + 6 \times 5 + 4 \times 6 \\ &= 0 + 18 + 56 + 36 + 28 + 30 + 24 = 192 \end{aligned}$$

$$\therefore \bar{X} = \frac{\sum f_i x_i}{N} = \frac{192}{80} = 2.4$$

$$\text{But } \bar{X} = np \quad \therefore p = \frac{\bar{X}}{n} = \frac{2.4}{6} = 0.4$$

$$\therefore q = 1 - p = 1 - 0.4 = 0.6$$

$$\therefore P(x) = {}^nC_x p^n q^{n-x} = {}^6C_x (0.4)^x (0.6)^{6-x}$$

Putting  $x = 0, 1, 2, 3, 4, 5, 6$ , we get

$$\begin{aligned} P(0) &= {}^6C_0 (0.4)^0 (0.6)^6 = 0.0466; & P(1) &= {}^6C_1 (0.4)^1 (0.6)^5 = 0.1866; \\ P(2) &= {}^6C_2 (0.4)^2 (0.6)^4 = 0.3110; & P(3) &= {}^6C_3 (0.4)^3 (0.6)^3 = 0.2765; \\ P(4) &= {}^6C_4 (0.4)^4 (0.6)^2 = 0.1382; & P(5) &= {}^6C_5 (0.4)^5 (0.6)^1 = 0.0389; \\ P(6) &= {}^6C_6 (0.4)^6 (0.6)^0 = 0.0041. \end{aligned}$$

Multiplying these probabilities by  $N = 80$ , we get the expected frequencies as

$X$	0	1	2	3	4	5	6
$f$	4	15	25	22	11	3	0

(The frequencies are to be rounded).

**Example 30 :** Twelve dice were thrown 4096 times and the number of appearance of 6 each time was noted.

No. of successes : 0 1 2 3 4 5 6 and above

Frequency : 447 1145 1181 786 380 115 32

Fit a Binomial distribution when the dice are unbiased.

(M.U. 2016)

Sol. : We have the probability of getting 6 in a throw of one die  $p = \frac{1}{6}$

The probability of not getting 6 is  $q = 1 - \frac{1}{6} = \frac{5}{6}$ .

The number of trials,  $n = 12$ .

The number of repetitions,  $N = 4096$ .

$$\text{Now, } P(X=x) = {}^{12}C_x p^x q^{12-x} = {}^{12}C_x \left(\frac{1}{6}\right)^x \left(\frac{5}{6}\right)^{12-x}$$

Putting  $X = 0, 1, 2, 3, 4, 5, \dots$

$$P(0) = {}^{12}C_0 \left(\frac{1}{6}\right)^0 \left(\frac{5}{6}\right)^{12} = 0.1122; \quad P(1) = {}^{12}C_1 \left(\frac{1}{6}\right)^1 \left(\frac{5}{6}\right)^{11} = 0.2692;$$

$$P(2) = {}^{12}C_2 \left(\frac{1}{6}\right)^2 \left(\frac{5}{6}\right)^{10} = 0.2961; \quad P(3) = {}^{12}C_3 \left(\frac{1}{6}\right)^3 \left(\frac{5}{6}\right)^9 = 0.1974;$$

$$P(4) = {}^{12}C_4 \left(\frac{1}{6}\right)^4 \left(\frac{5}{6}\right)^8 = 0.0888; \quad P(5) = {}^{12}C_5 \left(\frac{1}{6}\right)^5 \left(\frac{5}{6}\right)^7 = 0.0284;$$

$$P(6 \text{ and above}) = 1 - (0.1122 + 0.2692 + \dots + 0.0284) = 0.0079$$

Expected frequency =  $Np = 4096p$

No. of successes	0	1	2	3	4	5	6 and above
Frequency	480	1103	1213	808	364	116	32

### EXERCISE - I

- (A) 1. Find the fallacy if any in the following statements.

- (a) "The mean of a Binomial distribution is 6 and standard deviation is 4." (M.U. 1998)  
 (b) "The mean of a Binomial distribution is 9 and its standard deviation is 4."

[Ans. : (a) False,  $q = 8/3$  is impossible, (b) False,  $q = 16/9$ , is impossible]

2. The mean and variance of a Binomial variate are 3 and 1.2. Find ' $n$ ', ' $p$ ' and  $P(X < 4)$ . (M.U. 2002) [Ans. :  $n = 5$ ,  $p = 0.6$ ,  $2068/3125$ ]

3. Find the Binomial distribution if the mean is 5 and the variance is  $10/3$ . Find  $P(X = 2)$ .

$$(\text{M.U. 2003, 05}) [\text{Ans.} : P(X = x) = {}^{15}C_x \left(\frac{1}{3}\right)^x \left(\frac{2}{3}\right)^{15-x}; 0.06]$$

4. Find the mean, mode and standard deviation of the Binomial distribution whose parameters are  $n = 6$ ,  $p = 1/4$ . (M.U. 1998) [Ans. :  $\bar{X} = 2$ ,  $\sigma = \sqrt{1.5}$ ]

5. In a Binomial distribution consisting of 5 independent trials, probabilities of 1 and 2 successes are 0.4096 and 0.2048 respectively. Find the parameter ' $p$ ' of the distribution. (M.U. 1999)

[Ans. :  $p = 0.2$ ]

6. Find  $P(X \geq 1)$ , where  $X$  is a Binomial variate with mean 4 and variance 3. (M.U. 2004)

[Ans. : 0.09]

7. A Binomial variate  $X$  satisfies the relation  $9P(X = 4) = P(X = 2)$  when  $n = 6$ . Find the value of the parameter  $p$ . [Ans. :  $p = 3/4$ ]

8. Let  $X$  be Binomial distributed with parameter  $n, p$ . For what value of  $p$  variance is maximum, if you assume  $n$  fixed? (M.U. 2003) [Ans. :  $p = 1/2$ ]

- (B) 1. The odds in favour of  $X$ 's winning a game against  $Y$  are 4:3. Find the probability of  $Y$ 's winning 3 games out of 7 played.

$$[\text{Ans.} : {}^7C_3 \left(\frac{3}{7}\right)^3 \left(\frac{4}{7}\right)^4]$$

2. If 10% of bolts produced by a machine are defective. Find the probability that out of 5 bolts selected at random at most one will be defective. [Ans. :  $(1.4)(0.9)^4$ ]

3. On an average 3 out of ten students fail in an examination. What is the probability that out of 10 students that appear for the examination none will fail? [Ans. :  $(0.7)^{10}$ ]

4. If on the average rain falls on 10 days in every thirty, find the probability, (i) that the first three days of a week will be fine and the remaining wet, (ii) that the rain will fall on just three days of a week. (M.U. 1999)

$$[\text{Ans.} : (i) \left(\frac{2}{3}\right)^3 \left(\frac{1}{3}\right)^4, (ii) {}^7C_3 \left(\frac{1}{3}\right)^3 \left(\frac{2}{3}\right)^4]$$

5. 12% of the items produced by a machine are defective. What is the probability that out of a random sample of 20 items produced by the machine, 5 are defective? (Simplification is not necessary). [Ans. :  ${}^{20}C_5 (0.12)^5 (0.88)^{15}$ ]

6. If 10% of the rivets produced are defective, what is the chance that a random sample of 5 rivets will contain (i) exactly two defectives, (ii) fewer than two defectives? [Ans. : 0.0729, 0.918]

7. An unbiased die is rolled five times. What is the probability of its showing 5 twice? What is the probability of its showing 5 at least once? [Ans. : 0.13, 0.598]

8. Find the chance of getting exactly 5 heads in 6 throws of an unbiased coin. [Ans. : 3/32]

9. On an average 20% of population in an area suffer from T.B. What is the probability that out of 5 persons chosen at random from this area at least two suffer from T.B.? [Ans. : 821/3125]

10. If  $X$  is the random variable showing the number of boys in a family with 4 children, construct a table showing the probability distribution of  $X$ . [Ans. : 1/16, 4/16, 6/16, 4/16, 1/16]

11. Three balls are drawn from a box containing 4 red and 6 black balls. If  $X$  denotes the total number of red balls drawn construct probability distribution table. [Ans. : 27/125, 54/125, 36/125, 8/125]

12. Two unbiased dice are thrown three times. Find the probability that the sum nine would be obtained (i) once, (ii) twice. (M.U. 1997) [Ans. : (i) 0.26, (ii) 0.03]

13. If  $X$  is the random variable showing the number of boys in a family with 4 children, construct a table showing the probability distribution of  $X$ . [Ans. : 1/16, 4/16, 6/16, 4/16, 1/16]

14. 5 defective bulbs are accidentally mixed up with 20 good ones. It is not possible to just look at a bulb and tell whether or not it is defective. Find the probability distribution of defective bulbs if 4 bulbs are drawn from this lot. (M.U. 2001, 02, 14)

$$\begin{array}{l|ccccccccc}
\text{Ans. : } & X : & 0 & 1 & 2 & 3 & 4 \\
P(X = x) : & & 0.41 & 0.41 & 0.15 & 0.02 & 0.01
\end{array}$$

15. For special security in a certain protected area it was decided to put three lighting bulbs on each pole. If each bulb has probability ' $p$ ' of burning out in the first 100 hours of service, calculate the probability that at least one of them is still good after 100 hours. If  $p = 0.3$  how many bulbs would be needed on each pole to ensure 99% safety that at least one is good after 100 hours? Find also the probability that at least one of the bulbs is still working after 100 hours. (M.U. 2001, 04, 07, 09) [Ans. : (i)  $1 - p^3$ , (ii) 4, (iii) 0.973]

16. If 10% of the rivets produced by a machine are defective, find the probability that out of 5 randomly chosen rivets (i) none will be defective, (ii) at the most two will be defective. (M.U. 1997) [Ans. : (i) 0.59, (ii) 0.99]

- (C) 1. Assuming that half the population is female and assuming that 100 samples each of 10 individuals are taken, how many samples would you expect to have 3 or less females ?  
 (M.U. 1998) [ Ans. : 17 ]
2. Take 100 sets of 10 tosses of an unbiased coin. In how many cases do you expect to get (a) 7 heads and 3 tails, (b) 7 heads at least ?  
 [ Ans. : 12, 17 ]
3. Assuming that half the population is vegetarian so that the chance of an individual being vegetarian is 1/2 and assuming that 100 investigators can take a sample of 10 individuals to see whether they are vegetarians, how many investigators would you expect to report that three people or less were vegetarians ?  
 (M.U. 1998) [ Ans. : 17 ]
4. An irregular six faced die is thrown. The probability that in 10 throws it will give five even numbers is twice as likely that it will give four even numbers. How many times in 10,000 sets of 10 throws, would you expect to give no even number ?  
 (M.U. 2002) [ Ans. :  $p = 5/8; 1$  ]
5. The probability of failure in Physics practical examination is 20%. If 25 batches of 6 students each take the examination, in how many batches 4 or more students would pass ?  
 (M.U. 2001) [ Ans. : 20 ]
6. A lot contains 1% defective items. What should be the number of items in a lot so that the probability of finding at least one defective item in it, is at least 0.95.  
 (M.U. 1999) [ Ans. : 289 ]
7. The probability that a bomb will hit the target is 0.2. Two bombs are required to destroy the target. If six bombs are used, find the probability that the target will be destroyed.  
 (M.U. 1998) [ Ans. : 0.35 ]
8. The probability of a man hitting the target is 1/4. (i) If he fires 7 times what is the probability of his hitting the target at least twice ? (ii) How many times must be fire so that the probability of his hitting the targets at least once is greater than 2/3 ?  
 (M.U. 2004)  
 [ Ans. : (i) 0.555, (ii) 4 ]
9. Out of 1000 families with 4 children each, how many would you expect to have (i) 2 boys and 2 girls, (ii) at least one boy, (iii) no girl, (iv) at most 2 girls.  
 (M.U. 1998)  
 [ Ans. : (i) 375, (ii) 937.5, (iii) 62.5, (iv) 687.5 ]
10. If we take 1280 sets each of 10 tosses of a fair coin, in how many sets should we expect to get 7 heads and 3 tails ?  
 [ Ans. : 150 ]
11. The mean of defective blades supplied in packets of 10 is 1. In how many packets of this make out of 1000 packets would you expect to find at least 4 non-defective blades.  
 [ Ans. : 13 ]
12. In a sampling of a large number of parts produced by a machine the mean number of defectives in a sample of 20 is 2. Out of 1000 such samples how many samples would you expect to contain at least 3 defectives.  
 [ Ans. : 323 ]
13. Out of 800 families with 5 children each how many would you expect to have (i) 3 Boys and 2 Girls, (ii) 5 girls, (iii) 5 Boys ?  
 (M.U. 2006) [ Ans. : (i) 250, (ii) 25, (iii) 25 ]
14. Assuming boys and girls are equally likely find the expected number of 0 boy, 1 boy, 2 boys, ... 5 boys out of 320 families with 5 children each.  
 [ Ans. : 10, 50, 100, 100, 50, 10 ]
15. On an average a student is present on 5 days a week. Find on how many days in a course of 100 days out of 5 students 0, 1, 2, ..., 4, 5 students will be present. [ Ans. : 0, 2, 12, 30, 37, 19 ]
- (D) 1. Let  $X, Y$  be two independent binomial variates with parameters  $(n_1 = 8, p = 0.3)$  and  $(n_2 = 6, p = 0.3)$  respectively. Find  $P(X + Y = 2)$ .  
 [ Ans. : 0.1134 ]

2. Let  $X, Y$  be two independent binomial variates with parameters  $(n_1 = 5, p = 0.4)$  and  $(n_2 = 7, p = 0.4)$ . Find  $P(X + Y \geq 2)$ .  
 [ Ans. : 0.9804 ]
3. Let  $X, Y$  be two independent binomial variates with parameters  $(n_1 = 9, p = 0.2)$  and  $(n_2 = 7, p = 0.2)$  respectively. Find  $P(X + Y \geq 2)$ .  
 [ Ans. : 0.8593 ]
- (E) 1. Five fair coins are tossed 3200 times, find the frequency distribution of number of heads obtained. Also find mean and standard deviation.  
 (M.U. 2003)  
 [ Ans. : 100, 500, 1000, 1000, 500, 100 ; 1600, 28.28 ]
2. Four fair coins are tossed 160 times and the following results were obtained.
- |                |                    |
|----------------|--------------------|
| No. of heads : | 0, 1, 2, 3, 4,     |
| Frequency :    | 17, 52, 54, 31, 6. |
- Fit a Binomial distribution.
- [ Ans. :  $\bar{x} = \frac{\sum f_i x_i}{N} = 1.73, p = \frac{\bar{x}}{n} = \frac{1.73}{4} = 0.43, q = 0, N = 160$
- |                |                      |
|----------------|----------------------|
| No. of heads : | 0, 1, 2, 3, 4,       |
| Frequency :    | 17, 51, 58, 29, 5. ] |
3. Fit a Binomial distribution to the following data,
- |       |                         |
|-------|-------------------------|
| $x$ : | 0, 1, 2, 3, 4, 5, 6.    |
| $f$ : | 5, 18, 26, 12, 7, 6, 4. |
- [ Ans. :  $n = 6, N = 80, \bar{x} = \frac{\sum f_i x_i}{N} = 2.4 \therefore p = \frac{2.4}{6} = 0.4, q = 0.6$  ]
- |       |                            |
|-------|----------------------------|
| $x$ : | 0, 1, 2, 3, 4, 5, 6.       |
| $f$ : | 4, 15, 25, 22, 11, 3, 0. ] |
4. In an experiment with 500 seeds in groups of 5 the following results were obtained,
- |       |                               |
|-------|-------------------------------|
| $x$ : | 0, 1, 2, 3, 4, 5. Total       |
| $f$ : | 10, 70, 150, 160, 80, 30, 500 |
- [ Ans. :  $\bar{x} = \frac{\sum f_i x_i}{N} = 2.64, n = 5, p = \frac{\bar{x}}{n} = 0.528, q = 0.472$
- |       |                             |
|-------|-----------------------------|
| $x$ : | 0, 1, 2, 3, 4, 5.           |
| $f$ : | 12, 65, 147, 164, 92, 20. ] |
5. Five dice are thrown together 96 times. The number of times 4, 5 or 6 was obtained is given below.
- |   |                       |
|---|-----------------------|
| No. of times 4, 5,<br>or 6 was obtained : | 0, 1, 2, 3, 4, 5.     |
| Frequency :                               | 1, 10, 24, 35, 18, 8. |
- Fit a Binomial distribution if (i) dice are unbiased (ii) the nature of the dice is not known.
- [ Ans. : (i)  $p = \frac{3}{6} = \frac{1}{2}, q = \frac{1}{2}, n = 5, N = 96$ .
- |                    |                       |
|--------------------|-----------------------|
| No. of successes : | 0, 1, 2, 3, 4, 5.     |
| Frequencies :      | 3, 15, 30, 30, 15, 3. |

$$(ii) \bar{x} = \frac{\sum f_i x_i}{N} = 2.86, p = \frac{\bar{x}}{n} = \frac{2.86}{5} = 0.572, q = 0.428, n = 5, N = 96.$$

No. of successes :	0,	1,	2,	3,	4,	5,
Frequencies :	1,	9,	25,	33,	22,	6.

6. Eight unbiased coins are tossed 256 times. Number of heads observed in each throws are shown below.

No. of heads	0	1	2	3	4	5	6	7	8	Total
Observed frequency	2,	8,	24,	63,	64,	50,	36,	10,	1,	256

Fit a Binomial distribution and find the mean and the variance of the fitted distribution. (M.U. 1996)

[Ans.: No. of heads : 0, 1, 2, 3, 4, 5, 6, 7, 8.  
Observed frequency : 1, 8, 28, 56, 70, 56, 28, 8, 1.]

$$\text{Mean} = np = 4, \text{S.D.} = \sqrt{npq} = \sqrt{2}.$$

7. A biased coin was tossed 6 times and the experiment was repeated 150 times. The following table gives the frequencies of 0, 1, 2, 3, ..., 6 heads.

X (No. of heads)	0	1	2	3	4	5	6	Total
Frequency	2,	7,	20,	35,	48,	32,	6,	150

Evaluate the mean. Estimate  $p$  stating the assumptions. Fit a Binomial distribution. (M.U. 1997)

[Ans.:  $\bar{x} = 3.6, p = 0.6$

X (No. of heads)	0	1	2	3	4	5	6	Total
Frequency	1,	5,	21,	41,	47,	28,	7,	150

8. Fit a Binomial distribution to the following data and calculate theoretical frequencies.

X	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.
Frequency	: 6, 20, 28, 12, 8, 6, 0, 0, 0, 0, 0.

(M.U. 1998)

[Ans.:  $\bar{x} = 2.175, n = 10, p = 0.2175, q = 0.7825$

X	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.
Frequency	: 7, 19, 24, 18, 9, 3, 0, 0, 0, 0, 0.]

9. Fit a Binomial distribution to the following data.

X	: 0, 1, 2, 3, 4.
Frequency	: 12, 66, 109, 59, 10.

(M.U. 2004)

[Ans.:  $\bar{x} = 1.46, p = 0.49$

X	: 0, 1, 2, 3, 4.
Frequency	: 17, 67, 96, 61, 15.]

### 3. Poisson Distribution

Poisson distribution was discovered by the French Mathematician Poisson in 1837. Poisson distribution is the limiting case of the binomial distribution under the following conditions :

- (i)  $n$ , the number of trials is infinitely large i.e.  $n \rightarrow \infty$ .
- (ii)  $p$ , the probability of success in each trial is constant and infinitely small i.e.  $p \rightarrow 0$ .
- (iii)  $np$ , the average success is finite say  $m$ , i.e.  $np = m$ .

Siméon Denis Poisson (1781 - 1840)



A French mathematician geometer and physicist was born in Pithiviers, Loiret in France. He was a favourite student of Lagrange and was treated like a son by Laplace. Lagrange and Laplace were his doctoral advisors. In 1806 he became full professor at École Polytechnique, in Paris succeeding Fourier. His notable students were Dirichlet and Liouville. As a teacher of mathematics Poisson is said to have been extremely successful. As a scientific worker, his productivity has rarely, if ever, been equalled. Inspite of his many official duties, he published more than three hundred works, several of them extensive treatises and many of them mémoires dealing with the most abstruse branches of pure mathematics, applied mathematics, mathematical physics and rational mechanics. His mémoires on the theory of electricity and magnetism created a new branch of mathematical physics. He made important advances in planetary theory. Poisson is known for Poisson distribution, Poisson process, Poisson equation, Poisson Kernel, Poisson regression, Poisson summation formula, Poisson ratio, Euler-Poisson-Darboux equation, Conway-Maxwell-Poisson distribution.

#### (a) To Derive Poisson Distribution

Consider  $p(x) = {}^n C_x p^x q^{n-x}$

$$= {}^n C_x \left(\frac{p}{q}\right)^x q^n = {}^n C_x \left(\frac{p}{1-p}\right)^x (1-p)^n$$

Putting  $p = \frac{m}{n}$ ,

$$p(x) = \frac{n(n-1)(n-2)\dots(n-x+1)}{x!} \frac{(m/n)^x}{[1-(m/n)]^x} \left[1 - \frac{m}{n}\right]^x$$

$$p(x) = \frac{\left[1 - \frac{1}{n}\right] \left[1 - \frac{2}{n}\right] \dots \left[1 - \frac{x-1}{n}\right]}{x!} m^x \left[1 - \frac{m}{n}\right]^x$$

Since  $\lim_{n \rightarrow \infty} \left[1 - \frac{m}{n}\right]^n = e^{-m}$  and  $\lim_{n \rightarrow \infty} \left[1 - \frac{m}{n}\right]^x = 1$

Taking the limits of both sides as  $n \rightarrow \infty$

$$p(x) = \frac{m^x \cdot e^{-m}}{x!}$$

Thus, the limit of the Binomial random variable is the Poisson random variable.

(b) **Definition**

A random variable  $X$  is said to follow **Poisson distribution** if the probability of  $x$  is given by

$$P(X=x) = \frac{e^{-m} m^x}{x!}, \quad x = 0, 1, 2, \dots$$

and  $m (> 0)$  is called the parameter of the distribution.

**Remarks**

1. The sum of the probabilities is 1.

$$\begin{aligned} \sum_{x=0}^{\infty} P(X=x) &= \sum_{x=0}^{\infty} \frac{e^{-m} m^x}{x!} = e^{-m} \sum_{x=0}^{\infty} \frac{m^x}{x!} \\ &= e^{-m} \left[ 1 + m + \frac{m^2}{2!} + \dots \right] = e^{-m} \cdot e^m = 1. \end{aligned}$$

2. Poisson distribution occurs where the probability of occurrence  $p$  is very small and the number of trials  $n$  is very large and where the probability of occurrence only can be known e.g. the number of accidents, the number of deaths by a disease, the number of printing mistakes on a page etc. In these cases we can only observe the number of successes but the number of failures cannot be observed. We can observe how many accidents occur; we cannot observe how many times accidents do not occur.

(c) **When do we get Poisson distribution ?**

As seen before we get a Poisson distribution if the following conditions are satisfied.

1. The number of trials  $n$  is infinitely large i.e.  $n \rightarrow \infty$ .
2. A trial results in only two ways-success or failure.
3. If  $p$  and  $q$  are probabilities of success and failure, then  $p + q = 1$ .
4. These probabilities are mutually exclusive, exhaustive but not necessarily equally likely. (i.e.,  $p$  is not necessarily equal to  $1/2$ .)
5. The probability  $p$  of success is very small i.e.  $p \rightarrow 0$ .
6.  $n \rightarrow \infty$  and  $p \rightarrow 0$  such that  $np = m (> 0)$  a constant.

(d) **Uses**

Poisson distribution is used in problems involving :

- (i) the number of deaths due to a disease such as heart attack, cancer etc.
- (ii) the number of accidents during a week or a month etc.
- (iii) the number of phone-calls received at a particular telephone exchange during a period of time.
- (iv) the number of cars passing a particular point on a road during a period of time.
- (v) the number of printing mistakes on a page of a book etc.

**Note**

Since the Poisson distribution is the limiting case of Binomial distribution, we can calculate binomial probabilities approximately by using Poisson distribution whenever  $n$  is large and  $p$  is small. (See Ex. 21, page 7-31 and Ex. 22, page 7-32)

(e) **Moments of the Poisson's Distribution**

We obtain below the first two moments about the origin.

$$\mu_1' = E(x) = \sum p_i x_i$$

$$\begin{aligned} &= \sum_{x=0}^{\infty} \frac{e^{-m} m^x}{x!} x = \sum_{x=1}^{\infty} \frac{e^{-m} m^x}{(x-1)!} = m e^{-m} \sum \frac{m^{x-1}}{(x-1)!} \\ &= m e^{-m} \left[ 1 + m + \frac{m^2}{2!} + \frac{m^3}{3!} + \dots \right] \\ &= m e^{-m} \cdot e^m = m \end{aligned}$$

Hence, **mean =  $m$**

$$\mu_2' = E(x^2) = \sum p_i x_i^2 = \sum_{x=0}^{\infty} e^{-m} \cdot \frac{m^x}{x!} \cdot x^2$$

We can write  $x^2 = x + x(x-1)$

$$\mu_2' = \sum_{x=0}^{\infty} e^{-m} \cdot \frac{m^x}{x!} [x + x(x-1)]$$

$$\begin{aligned} &= m e^{-m} \sum_{x=1}^{\infty} \frac{m^{x-1}}{(x-1)!} + m^2 e^{-m} \sum_{x=2}^{\infty} \frac{m^{x-2}}{(x-2)!} \\ &= m e^{-m} \cdot e^m + m^2 e^{-m} \left[ 1 + \frac{m}{1!} + \frac{m^2}{2!} + \dots \right] \\ &= m e^{-m} \cdot e^m + m^2 e^{-m} \cdot e^m = m + m^2 \\ \therefore \mu_2' &= \mu_1'^2 = m + m^2 - m^2 = m \end{aligned}$$

**Variance =  $m$**

Thus, the mean and variance of the Poisson's distribution are both equal to  $m$ .

(f) **Moment Generating Function**

The m.g.f. about the origin is,

$$\begin{aligned} M_0(t) &= E(e^{tx}) = \sum p(x) e^{tx} = \sum \frac{e^{-m} \cdot m^x}{x!} \cdot e^{tx} \\ &= e^{-m} \sum \frac{(m e^t)^x}{x!} = e^{-m} \cdot e^{m e^t} \end{aligned}$$

$$M_0(t) = e^{m(e^t - 1)}$$

(Note that  $\sum \frac{k^x}{x!} = 1 + k + \frac{k^2}{2!} + \frac{k^3}{3!} + \dots = e^k$ .

We shall often meet expressions of this type in the discussion of Poisson's distribution.)

$$\text{Now } \frac{d}{dt} [M_0(t)] = e^{m(e^t-1)} + me^t$$

$$\therefore \left[ \frac{d}{dt} M_0(t) \right]_{t=0} = m \quad \therefore \mu_1' = m$$

$$\frac{d^2}{dt^2} [M_0(t)] = m \left[ e^t \cdot e^{m(e^t-1)} + me^t + e^{m(e^t-1)} \cdot e^t \right]$$

$$\therefore \left[ \frac{d^2}{dt^2} M_0(t) \right]_{t=0} = m(m+1) = m^2 + m \quad \therefore \mu_2' = m^2 + m$$

$$\therefore \mu_2 = \mu_2' - \mu_1^2 = m^2 + m - m^2 \quad \therefore \mu_2 = m$$

We may denote the logarithm of the m.g.f. (A) by  $L(t)$ . Then

$$L(t) = \log M_0(t) = \log [e^{m(e^t-1)}] \quad \therefore L(t) = m(e^t - 1)$$

Differentiating both sides w.r.t.  $t$

$$L'(t) = m e^t \quad \therefore L'(0) = m$$

$$L''(t) = m e^t \quad \therefore L''(0) = m$$

But as proved in (2B) on page 6-44,  $L'(0) = \mu$  and  $L''(0) = \mu_2$ .

Hence, mean  $\mu = L'(0) = m$  and variance  $\mu_2 = L''(0) = m$ .

**Example :** If the moment generating function about the origin of a discrete random variable  $X$  is  $e^{4(e^t-1)}$ , find  $P(X=\mu+\sigma)$  where  $\mu$  and  $\sigma$  are mean and standard deviation of  $X$ .

Sol.: We know that m.g.f. of a Poisson distribution with mean  $m$  is

(M.U. 2007, 09)

$$M_0(t) = e^{m(e^t-1)}$$

Comparing this with the given m.g.f. we see that  $X$  is a Poisson variate with mean  $m=4$  and variance  $\sigma^2 = m=4$ .

Hence, the Poisson distribution is

$$P(X=x) = \frac{e^{-4} \cdot 4^x}{x!}$$

But  $m+\sigma = 4+2=6$ ,

$$\therefore P(X=6) = \frac{e^{-4} \cdot 4^6}{6!} = 0.1.$$

#### (g) Additive property of Independent Poisson distributions

If two independent variates have Poisson distribution with means  $m_1$  and  $m_2$  then their sum also is a Poisson distribution with mean  $m_1 + m_2$ .

**Proof :** Let  $M_1(t)$  and  $M_2(t)$  be the m.g.f.'s of the two Poisson variates  $X_1$  and  $X_2$  and let  $M(t)$  be the m.g.f. of their sum.

Now  $M_1(t) = E(e^{tX_1})$  and  $M_2(t) = E(e^{tX_2})$

$$M_1(t) = e^{m_1(e^t-1)} \quad \text{and} \quad M_2(t) = e^{m_2(e^t-1)}$$

Since,  $X_1$  and  $X_2$  are independent, m.g.f. of  $X_1 + X_2$  is

$$M(t) = E[e^{t(X_1+X_2)}] = E(e^{tX_1}) \cdot E(e^{tX_2}) \\ = e^{m_1(e^t-1)} \cdot e^{m_2(e^t-1)} = e^{(m_1+m_2)(e^t-1)}$$

But this is the m.g.f. of the Poisson distribution with mean  $m_1 + m_2$ . Hence, the result.

Notes ...

- Although the sum of two Poisson variates is a Poisson variate, the difference between two Poisson variates is not a Poisson variate. If  $X, Y$  are two Poisson variates then,

$$M_{(X-Y)}(t) = M_{X+(-Y)}(t) = M_X(t) \cdot M_{-Y}(t) \\ = M_X(t) \cdot M_Y(-t) \quad [\because M_{-Y}(t) = M_Y(ct)] \\ = e^{m_1(e^t-1)} \cdot e^{m_2(e^{-t}-1)} = e^{m_1(e^t-1)+m_2(e^{-t}-1)}$$

But this cannot be put in the form  $e^{m(e^t-1)}$  and hence  $(X-Y)$  is not a Poisson variate.

- If  $X_1, X_2, \dots, X_n$  are  $n$  independent Poisson variates with parameters  $m_1, m_2, \dots, m_n$  then  $Y = X_1 + X_2 + \dots + X_n$  is also a Poisson variate with parameter  $m_1 + m_2 + \dots + m_n$ .
- If  $X_1$  and  $X_2$  are independent Poisson variates with parameter  $m_1, m_2$  then  $Y = a_1 X_1 + a_2 X_2$  is not a Poisson variate.

(You can very easily prove these two results.)

#### (h) Recurrence Relation For Probabilities

We have for Poisson distribution

$$p(x) = \frac{e^{-m} \cdot m^x}{x!} \quad \therefore p(x+1) = \frac{e^{-m} \cdot m^{x+1}}{(x+1)!} \\ \therefore \frac{p(x+1)}{p(x)} = \frac{m^{x+1}}{(x+1)!} \cdot \frac{x!}{m^x} = \frac{m}{x+1} \quad \therefore p(x+1) = \frac{m}{x+1} \cdot p(x)$$

If we know  $p(0) = e^{-m}$ , we can find the probabilities of  $x = 1, 2, 3, \dots$

Thus,  $p(1) = m \cdot p(0)$ ,  $p(2) = \frac{m}{2} p(1)$ ,  $p(3) = \frac{m}{3} p(2)$  and so on.

Since, expected frequency of  $x$  i.e.  $f(x)$  is  $Np(x)$ , we have from the above relation,

$$Np(x+1) = \frac{m}{x+1} \cdot Np(x) \quad \therefore f(x+1) = \frac{m}{x+1} f(x)$$

This relation can be used to find expected frequencies. This is called fitting a Poisson distribution.

**Example 1 :** Find out the fallacy if any in the following statement "The mean of a Poisson distribution is 2 and the variance is 3".

Sol.: In a Poisson distribution the mean and variance are same. Hence, the above statement is false.

Applied Mathematics - IV

(7-25)

Some Standard Distributions

**Example 2 :** If the mean of the Poisson distribution is 4, find  $P(m - 2\sigma < X < m + 2\sigma)$ .  
(M.U. 2009)

Sol. : For Poisson distribution mean = variance =  $m$ .

Hence,  $m = 4$  and  $\sigma = 2$

$$\therefore P(m - 2\sigma < X < m + 2\sigma) = P(0 < X < 8) \\ = P(X = 1, 2, 3, \dots, 7)$$

$$\text{But } P(X) = e^{-m} \frac{m^x}{x!} = e^{-4} \frac{4^x}{x!}$$

$$\therefore \text{Required probability} = e^{-4} \left[ \frac{4}{1!} + \frac{4^2}{2!} + \frac{4^3}{3!} + \frac{4^4}{4!} + \frac{4^5}{5!} + \frac{4^6}{6!} + \frac{4^7}{7!} \right] = 0.93$$

**Example 3 :** If the variance of a Poisson distribution is 2, find the probabilities of  $r = 1, 2, 3, 4$  from the recurrence relation of Poisson distribution.  
(M.U. 2002)

$$\text{Sol. : We have } P(x) = e^{-m} \frac{m^x}{x!}$$

Since variance =  $m = 2$  by data.

$$P(x) = e^{-2} \frac{2^x}{x!} \text{ when } x = 0, P(0) = e^{-2}$$

$$\text{Now, the recurrence relation is } P(x+1) = \frac{m}{x+1} P(x)$$

$$\text{Putting } x = 0, P(1) = \frac{2}{1} P(0) = 2e^{-2}$$

$$\text{Putting } x = 1, P(2) = \frac{2}{2} P(1) = \frac{2}{2} \cdot 2e^{-2} = e^{-2}$$

$$\text{Putting } x = 2, P(3) = \frac{2}{3} P(2) = \frac{2}{3} \cdot \frac{2}{2} P(1) = \frac{2}{3} e^{-2}$$

$$\text{Putting } x = 3, P(4) = \frac{2}{4} P(3) = \frac{1}{3} e^{-2}$$

**Example 4 :** Find out the fallacy if any in the following statement.

"If  $X$  is a Poisson variate such that  $P(X=2) = 9P(X=4) + 90P(X=6)$  then mean of  $X = 1$ ".  
(M.U. 1997)

Sol. : Let  $m$  be the mean of  $X$ .  $\therefore P(X=x) = e^{-m} \frac{m^x}{x!}$

$$\text{By data, } e^{-m} \frac{m^2}{2!} = 9 \cdot e^{-m} \frac{m^4}{4!} + 90 \cdot e^{-m} \frac{m^6}{6!}$$

$$\therefore \frac{1}{2} = \frac{3m^2}{8} + \frac{m^4}{8} \quad \therefore m^4 + 3m^2 - 4 = 0$$

$$\therefore (m^2 + 4)(m^2 - 1) = 0 \quad \therefore m^2 = -4 \text{ or } m^2 = 1$$

$\therefore$  The mean is 1 since  $m > 0$ .

$\therefore$  The statement is correct.

Applied Mathematics - IV

(7-26)

Some Standard Distributions

**Example 5 :** A car hire firm has two cars which it hires out day by day. The number of demands for a car on each day is distributed as Poisson variate with mean 1.5. Calculate the proportion of days on which (i) neither car is used, (ii) some demand is refused.  
(M.U. 1996, 98)

Sol. : We have  $P(x) = e^{-m} \frac{m^x}{x!} = \frac{e^{-1.5} \cdot (1.5)^x}{x!}, x = 0, 1, 2, \dots$

(i) Probability that there is no demand is

$$P(X=0) = e^{-1.5} \frac{(1.5)^0}{0!} = 0.2231$$

(ii) Probability that some demand is refused means there was demand for more than two cars.

$$\therefore P(X > 2) = P(X=3) + P(X=4) + \dots$$

$$= 1 - [P(X=0) + P(X=1) + P(X=2)]$$

$$= 1 - \left[ e^{-1.5} \frac{(1.5)^0}{0!} + e^{-1.5} \frac{(1.5)^1}{1!} + e^{-1.5} \frac{(1.5)^2}{2!} \right]$$

$$= 1 - [0.2231 + 0.3347 + 0.2510] = 0.1912.$$

$\therefore$  Proportion of days on which (i) neither car is used is 0.2231.

(ii) some demand is refused is 0.1912.

**Example 6 :** If a random variable  $X$  follows Poisson distribution such that  $P(X=1) = 2P(X=2)$ , find the mean and the variance of the distribution. Also find  $P(X=3)$ .  
(M.U. 2002, 05, 16)

Sol. : Let the parameter of the Poisson distribution be  $m$ .

$$\therefore P(X=x) = \frac{e^{-m} \cdot m^x}{x!}$$

We are given that  $P(X=1) = 2P(X=2)$

$$\therefore \frac{e^{-m} \cdot m^1}{1!} = 2 \frac{e^{-m} \cdot m^2}{2!} \quad \therefore m = 1$$

$\therefore$  The mean and the variance = 1.

$$\text{Now, } P(X=3) = \frac{e^{-m} \cdot m^3}{3!} = \frac{e^{-1} \cdot 1^3}{3!} = 0.0613,$$

**Example 7 :** A hospital switch board receives an average of 4 emergency calls in a 10 minutes interval. What is the probability that (i) there are atleast 2 emergency calls, (ii) there are exactly 3 emergency call in an interval of 10 minutes ?

Sol. : We have  $P(x) = \frac{e^{-m} \cdot m^x}{x!}$ . Here,  $m = 4$ .

$$(i) \quad P(X \leq 2) = P(X=0) + P(X=1) + P(X=2)$$

$$= \frac{e^{-4} \cdot 4^0}{0!} + \frac{e^{-4} \cdot 4^1}{1!} + \frac{e^{-4} \cdot 4^2}{2!}$$

$$= e^{-4}(1 + 4 + 8) = 0.238$$

$$(ii) \quad P(X=3) = \frac{e^{-m} \cdot m^x}{x!} = \frac{e^{-4} \cdot 4^3}{3!} = 0.195$$

**Example 8 :** A variable  $X$  follows a Poisson distribution with variance 3. Calculate (i)  $P(X=2)$ , (ii)  $P(X \geq 4)$ .  
(M.U. 1996)

Sol. : We have  $P(X=x) = \frac{e^{-m} \times m^x}{x!}$ ,  $x = 0, 1, 2, \dots$

$$\therefore P(X=2) = \frac{e^{-3} \times 3^2}{2!} = 0.224$$

$$\therefore P(X \geq 4) = 1 - [P(X=0) + P(X=1) + P(X=2) + P(X=3)] \\ = 1 - 0.647 = 0.353.$$

**Example 9 :** If  $X$  and  $Y$  are independent Poisson variates with mean  $m_1$  and  $m_2$ , find the probability that  $X+Y=k$ .

Sol. : Since  $X, Y$  are independent Poisson variates with parameters  $m_1$  and  $m_2$ ,  $Z = X+Y$  is also a Poisson variate with parameter  $m_1+m_2$ .

$$\therefore P(Z=k) = \frac{e^{-(m_1+m_2)}(m_1+m_2)^k}{k!}, k=0, 1, 2, \dots$$

**Example 10 :** If  $X, Y$  are independent Poisson variates with mean 2 and 3, find the variance of  $3X-2Y$ .

Sol. : For Poisson variate mean and variance are equal. Hence,  $\text{Var. } X = 2$  and  $\text{Var. } Y = 3$ .

Since,  $X, Y$  are independent

$$\begin{aligned} \text{Var.}(3X-2Y) &= 9 \text{Var.}(X) + 4 \text{Var.}(Y) \\ &= 9(2) + 4(3) = 30. \end{aligned}$$

**Example 11 :** If  $X, Y$  are independent Poisson variates such that  $P(X=1) = P(X=2)$  and  $P(Y=2) = P(Y=3)$ , find the variance of  $2X-3Y$ .

Sol. : Let the parameter of  $X$  and  $Y$  be  $m_1$  and  $m_2$ .

$$\therefore P(X=1) = P(X=2) \text{ gives } \frac{e^{-m_1} m_1^1}{1!} = \frac{e^{-m_1} m_1^2}{2!}$$

$$\therefore 2e^{-m_1} m_1 - e^{-m_1} m_1^2 = 0 \quad \therefore e^{-m_1} m_1(2-m_1) = 0 \quad \therefore m_1 = 2$$

$$P(Y=2) = P(Y=3) \text{ gives } \frac{e^{-m_2} m_2^2}{2!} = \frac{e^{-m_2} m_2^3}{3!}$$

$$\therefore 3e^{-m_2} m_2^2 - e^{-m_2} m_2^3 = 0 \quad \therefore e^{-m_2} m_2^2(3-m_2) = 0 \quad \therefore m_2 = 3$$

Since,  $X$  and  $Y$  are independent

$$\begin{aligned} V(2X-3Y) &= 4V(X) + 9V(Y) \\ &= 4(2) + 9(3) = 35. \end{aligned}$$

**Example 12 :** If  $X_1, X_2, X_3$  are three independent Poisson variates with parameters  $m_1 = 1, m_2 = 2, m_3 = 3$  respectively, find (i)  $P[(X_1 + X_2 + X_3) \geq 3]$  and (ii)  $P[X_1 = 1 / (X_1 + X_2 + X_3) = 3]$ .  
(M.U. 2005)

Sol. : By additive property of Poisson distribution  $Z = X_1 + X_2 + X_3$  is also a Poisson distribution with parameter  $m = m_1 + m_2 + m_3 = 6$ .

$$\begin{aligned} \therefore P(Z \geq 3) &= 1 - P(Z \leq 2) \\ &= 1 - \sum_{z=0}^2 \frac{e^{-6} 6^z}{z!} = 1 - \left( e^{-6} + 6e^{-6} + \frac{6^2 e^{-6}}{2!} \right) \\ &= 1 - 25e^{-6} = 1 - 25(0.002478) = 0.938 \end{aligned}$$

By definition of conditional probability,

$$P[X_1 = 1 / (X_1 + X_2 + X_3) = 3] = \frac{P(X_1 = 1 \text{ and } X_2 + X_3 = 2)}{P[(X_1 + X_2 + X_3) = 3]}$$

Now,  $X_1$  is a Poisson variate with parameter  $m_1 = 1$ ,  $X_2 + X_3$  is a Poisson variate with parameter  $m_2 + m_3 = 2 + 3 = 5$ ,  $X_1 + X_2 + X_3$  is a Poisson variate with parameter  $m_1 + m_2 + m_3 = 1 + 2 + 3 = 6$ .

$$\therefore P[X_1 = 1 / (X_1 + X_2 + X_3) = 3] = \frac{\left( \frac{e^{-1} \cdot 1}{1} \right) \left( \frac{e^{-5} \cdot 5^2}{2!} \right)}{e^{-6} \cdot \frac{6^3}{3!}} = \frac{25}{72}$$

**Example 13 :** An insurance company found that only 0.01% of the population is involved in a certain type of accident each year. If its 1000 policy holders were randomly selected from the population, what is the probability that no more than two of its clients are involved in such accident next year?  
(M.U. 2002)

Sol. : We have  $p = \frac{0.01}{100} = 0.0001, n = 1000$ .

$$\therefore m = np = 1000 \times 0.0001 = 0.1$$

$$\therefore P(X=x) = \frac{e^{-0.1} (0.1)^x}{x!}$$

$$\therefore P(X \leq 2) = P(X=0) + P(X=1) + P(X=2)$$

$$\therefore P(X \leq 2) = e^{-0.1} \left[ \frac{(0.1)^0}{0!} + \frac{(0.1)^1}{1!} + \frac{(0.1)^2}{2!} \right] = 0.9998$$

**Example 14 :** Find the probability that at most 4 defective bulbs will be found in a box of 200 bulbs if it is known that 2 percent of the bulbs are defective. (Given  $e^{-4} = 0.0183$ ).

Sol. : Since probability of a defective bulb is small we can use Poisson distribution.

We have,  $\therefore m = np = 200 \times 0.02 = 4$

$$\therefore P(X=x) = \frac{e^{-4} \times 4^x}{x!}$$

$$\therefore P(X \leq 4) = p(0) + p(1) + p(2) + p(3) + p(4)$$

$$= \frac{e^{-4} \times 4^0}{0!} + \frac{e^{-4} \times 4^1}{1!} + \frac{e^{-4} \times 4^2}{2!} + \frac{e^{-4} \times 4^3}{3!} + \frac{e^{-4} \times 4^4}{4!}$$

$$= e^{-4} \left[ 1 + \frac{4}{1!} + \frac{16}{2!} + \frac{64}{3!} + \frac{256}{4!} \right]$$

$$= e^{-4} \times \frac{103}{3} = 0.0183 \times \frac{103}{3} = 0.6283.$$

**Example 15 :** Using Poisson distribution find the approximate value of  
 ${}^{300}C_2 (0.02)^2 (0.98)^{298} + {}^{300}C_3 (0.02)^3 (0.98)^{297}$

(M.U. 2004)

**Sol. :** Clearly the above probabilities are the probabilities of Binomial distribution. Comparing them with

$$P(X=x) = {}^nC_x p^x q^{n-x}$$

We see that  $n = 300$ ,  $p = 0.02$ ,  $q = 0.98$ ,  $x = 2$  and  $3$ .

Now, Binomial distribution is related to Poisson distribution where  $m = np$ .

Hence,  $m = 300 \times 0.02 = 6$ .

∴ Corresponding Poisson distribution is given by

$$P(X=x) = \frac{e^{-m} \cdot m^x}{x!} = \frac{e^{-6} \cdot 6^x}{x!}$$

$$\therefore P(X=2) + P(X=3) = \frac{e^{-6} \cdot 6^2}{2!} + \frac{e^{-6} \cdot 6^3}{3!}$$

$$= 0.04462 + 0.08923 = 0.1338$$

**Example 16 :** Find the probability that at most 4 defective bulbs will be found in a box of 200 bulbs if it is known that 2 percent of the bulbs are defective. (Given  $e^{-4} = 0.0183$ ). (M.U. 1997)

**Sol. :** Since probability of a defective bulb is small we can use Poisson distribution.

We have, ∴  $m = np = 200 \times 0.02 = 4$

$$\therefore P(X=x) = \frac{e^{-4} \times 4^x}{x!}$$

$$\therefore P(X \leq 4) = p(0) + p(1) + p(2) + p(3) + p(4)$$

$$= \frac{e^{-4} \times 4^0}{0!} + \frac{e^{-4} \times 4^1}{1!} + \frac{e^{-4} \times 4^2}{2!} + \frac{e^{-4} \times 4^3}{3!} + \frac{e^{-4} \times 4^4}{4!}$$

$$\therefore P(X \leq 4) = e^{-4} \left[ 1 + \frac{4}{1!} + \frac{16}{2!} + \frac{64}{3!} + \frac{256}{4!} \right]$$

$$= e^{-4} \times \frac{103}{3} = 0.0183 \times \frac{103}{3} = 0.6283.$$

**Example 17 :** The number of accidents in a year attributed to taxi drivers in a city follows Poisson distribution with mean 3. Out of 1,000 taxi drivers, find approximately the number of drivers with (i) no accident in a year, (ii) more than 3 accidents in a year. (Given :  $e^{-1} = 0.3679$ ,  $e^{-2} = 0.1353$ ,  $e^{-3} = 0.0498$ )

**Sol. :** For a Poisson variate

$$P(X=x) = \frac{e^{-m} \times m^x}{x!}, \quad x = 0, 1, 2, \dots$$

We are given  $m = 3$

$$\therefore P(X=x) = \frac{e^{-3} \times (3)^x}{x!}, \quad x = 0, 1, 2, \dots$$

$$\therefore P(X=0) = \frac{e^{-3} \times (3)^0}{0!} = e^{-3} = 0.0498$$

$$P(X=1) = \frac{e^{-3} \times (3)^1}{1!} = 0.0498 \times 3 = 0.1494$$

$$P(X=2) = \frac{e^{-3} \times (3)^2}{2!} = 0.0498 \times \frac{9}{2} = 0.2241$$

∴ Expected number of drivers with no accidents

$$= N \times p(0) = 1,000 \times 0.0498 = 49.8 = 50 \text{ nearly.}$$

$$\therefore p(0, 1, 2, 3 \text{ accidents}) = p(0) + p(1) + p(2) + p(3) \\ = 0.0498 + 0.1494 + 0.2241 = 0.4233$$

$$\therefore p(\text{more than 3 accidents}) = 1 - 0.4233 = 0.5767.$$

Expected number of drivers with more than 3 accidents

$$= Np = 1,000 \times 0.5767$$

$$= 576.7 = 577 \text{ nearly.}$$

**Example 18 :** In a certain factory turning out blades, there is a small chance  $1/500$  for any blade to be defective. The blades are supplied in packets of 10. Use the Poisson distribution to calculate the approximate number of packets containing no defective, one defective, two defective blades in a consignment of 10,000 packets. (Given  $e^{-0.02} = 0.9802$ )

**Sol. :** We have,  $n = 10$ ,  $p = \frac{1}{500}$ , ∴  $m = np = 10 \times \frac{1}{500} = 0.02$

$$\therefore P(X=x) = \frac{e^{-0.02} \times (0.02)^x}{x!}$$

$$\therefore P(X=0) = \frac{e^{-0.02} \times (0.02)^0}{0!} = e^{-0.02} = 0.9802$$

$$P(X=1) = \frac{e^{-0.02} \times (0.02)^1}{1!} = e^{-0.02} \times 0.02 = 0.0196$$

$$P(X=2) = \frac{e^{-0.02} \times (0.02)^2}{2!} = e^{-0.02} \times 0.0002 = 0.0002$$

∴ Expected freq. of no defective =  $10000 \times 0.9802 = 9802$

Expected freq. of one defective =  $10000 \times 0.0196 = 196$

Expected freq. of two defective =  $10000 \times 0.0002 = 2$ .

**Example 19 :** Fit a Poisson distribution to the following data

No. of deaths : 0, 1, 2, 3, 4.

Frequencies : 123, 59, 14, 3, 1.

(M.U. 2000, 01, 04)

**Sol. :** Fitting Poisson distribution means finding expected frequencies of  $X = 0, 1, 2, 3, 4$ .

$$\text{Now, mean} = \frac{\sum f_i x_i}{\sum f_i} = m$$

$$\therefore \text{Mean} = 123(0) + 59(1) + 14(2) + 3(3) + 1(4)$$

$$= \frac{100}{200} = 0.5$$

(i) Poisson distribution of  $X$  is

$$P(X=x) = \frac{e^{-m} \cdot m^x}{x!} = \frac{e^{-0.5} \cdot (0.5)^x}{x!}$$

Expected frequency  $= N \times p(x)$

$$= 200 \times \frac{e^{-0.5} \cdot (0.5)^x}{x!}$$

Putting  $x = 0, 1, 2, 3, 4$  we get the expected frequencies as 121, 61, 15, 2, 1.  
Or putting  $x = 0$  in (1).

$$P(X=0) = e^{-0.5} \frac{(0.5)^0}{0!} = 0.6065$$

∴ Expected frequency  $f(0) = Np = 200 \times 0.6065 = 121$ .

$$\text{But } f(x+1) = \frac{m}{x+1} \cdot f(x) = \frac{0.5}{x+1} \cdot f(x)$$

$$\text{Putting } x=0, f(1) = \frac{0.5}{1} \cdot 121 = 61, \quad \text{Putting } x=1, f(2) = \frac{0.5}{2} \cdot 61 = 15.$$

$$\text{Putting } x=2, f(3) = \frac{0.5}{3} \cdot 15 = 3. \quad \text{Putting } x=3, f(4) = \frac{0.5}{4} \cdot 3 = 1.$$

**Example 20 :** Letters were received in an office on each of 100 days. Fit a Poisson distribution and find the expected frequencies for  $x = 0$  and 1. (Given :  $e^{-4} = 0.0183$ ).

Number of letters : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

Frequency : 1, 4, 15, 22, 21, 20, 8, 6, 2, 0, 1.

Sol. :  $\sum f_i = 1 + 4 + 15 + \dots + 1 = 100$

$$m = \frac{\sum f_i x_i}{\sum f_i} = \frac{1 \times 0 + 4 \times 1 + 15 \times 2 + \dots + 1 \times 10}{100} = \frac{400}{100} = 4$$

$$\therefore P(X=x) = \frac{e^{-m} \cdot m^x}{x!} = \frac{e^{-4} \cdot 4^x}{x!} \quad \therefore p(0) = e^{-4} = 0.0183$$

Now, expected frequency  $f(0) = Np = 100 \times 0.0183 = 1.83 = 2$

$$\text{But } f(x+1) = \frac{m}{x+1} \cdot f(x) \quad \therefore f(1) = \frac{4}{1} (1.83) = 7.32 = 7$$

**Example 21 :** A transmission channel has a per-digit error probability  $p = 0.01$ . Calculate the probability of more than 1 error in 10 received digits using (i) Binomial Distribution, (ii) Poisson Distribution.

Also find the m.g.f. in each case.

Sol. : (i) **Binomial Distribution :** We have  $p = 0.01, q = 1 - p = 0.99, n = 10$ .

$$\begin{aligned} P(X=x) &= {}^n C_x p^x q^{n-x} = 10! C_x (0.01)^x (0.99)^{10-x} \\ P(X>1) &= 1 - P(X \leq 1) = 1 - P(X=0) - P(X=1) \\ &\geq 1 - {}^{10} C_0 (0.01)^0 (0.99)^{10} - {}^{10} C_1 (0.01)^1 (0.99)^9 \\ &= 1 - 0.9044 - 0.09135 = 0.00425 \end{aligned}$$

(M.U. 2004)

(ii) **Poisson Distribution :** We have  $m = np = 10(0.01) = 0.1$ ,

$$\therefore P(X=x) = e^{-m} \cdot \frac{m^x}{x!} = e^{-0.1} \frac{(0.1)^x}{x!}$$

$$\begin{aligned} P(X>1) &= 1 - P(X \leq 1) = 1 - P(X=0) - P(X=1) \\ &= 1 - e^{-0.1} \frac{(0.1)^0}{0!} - e^{-0.1} \frac{(0.1)^1}{1!} \\ &= 1 - 0.9048 - 0.0905 = 0.0047 \end{aligned}$$

(iii) M.G.F. of Binomial Distribution is given by

$$M_0(t) = (q + pe^t)$$

[ See (A), page 7-3 ]

Here,  $q = 0.9, p = 0.01, n = 10$

$$\therefore M_0(t) = (0.99 + 0.01 \cdot e^t)^{10}$$

(iv) M.G.F. of Poisson Distribution is given by

$$M_0(t) = e^{m(e^t - 1)}$$

[ See (A), page 7-22 ]

Here,  $m = 0.1, \therefore M_0(t) = e^{0.1(e^t - 1)}$

**Example 22 :** It is known that the probability of an item produced by a certain machine will be defective is 0.05. If the produced items are sent to the market in packets of 20, find the number of packets containing (i) at least, (ii) exactly and (iii) at most 2 defective items in a consignment of 1000 packets using (a) Binomial distribution, (b) Poisson approximation to the Binomial distribution.

(M.U. 2004, 05, 06)

Sol. : We have  $P(\text{defective}) = 0.05, P(\text{non-defective}) = 0.95, n = 20$  and  $N = 1000$ .

(i) **By Binomial Distribution**

$$P(X=x) = {}^{20} C_x (0.05)^x (0.95)^{20-x}$$

$$P(X=0) = {}^{20} C_0 (0.05)^0 (0.95)^{20} = 0.36$$

$$P(X=1) = {}^{20} C_1 (0.05)^1 (0.95)^{19} = 0.38$$

$$P(X=2) = {}^{20} C_2 (0.05)^2 (0.95)^{18} = 0.19$$

No. of packets containing at least 2 defective

$$= N [1 - P(X=0) - P(X=1)]$$

$$= 1000 [1 - 0.36 - 0.38] = 260$$

No. of packets containing exactly 2 defective

$$= N P(X=2) = 1000 \times 0.19 = 190$$

No. of packets containing at most 2 defective

$$= N [P(X=0) + P(X=1) + P(X=2)]$$

$$= 1000 [0.36 + 0.38 + 0.19] = 930$$

(ii) **By Poisson Distribution**

Since,  $m = np = 20 \times 0.05 = 1$

$$P(X=x) = e^{-1} \frac{1^x}{x!}, \quad x = 0, 1, 2, \dots$$

$$\begin{aligned} P(X=0) &= e^{-1} \frac{(1)^0}{0!} = 0.37; & P(X=1) &= e^{-1} \frac{(1)^1}{1!} = 0.37; \\ P(X=2) &= e^{-1} \frac{(1)^2}{2!} = 0.1839 \end{aligned}$$

No. of packets containing at least 2 defective  
 $= N[1 - P(X=0) - P(X=1)]$   
 $= 1000 [1 - 0.37 - 0.37] = 260$

No. of packets containing exactly 2 defective  
 $= N \cdot P(X=2) = 100 \times 0.1839 = 180$

No. of packets containing atmost 2 defective  
 $= N[P(X=0) + P(X=1) + P(X=2)]$   
 $= 1000 [0.37 + 0.37 + 0.1839] = 924.$

**Remark ...**

As seen on page 7-20 when  $n$  is large Binomial Distribution tends to Poisson Distribution. In this example,  $n = 1000$  and both distributions give nearly same frequencies.

**EXERCISE - II**

- (A) 1. Can we have a Poisson distribution with mean 4 and variance 5? Give reasoning for your answer. [Ans.: No]
2. Find the mean and variance of the following distribution
- $$P(X=x) = \frac{e^{-3} \times (3)^x}{x!}, \quad x=0, 1, 2, \dots$$
- [Ans.: Mean = variance = 3]
3. The mean and the variance of a probability distribution is 2. Write down the distribution.
- $$(M.U. 2002, 05) [Ans.: P(X=x) = \frac{e^{-2} \times (2)^x}{x!}, \quad x=0, 1, 2, \dots]$$
4. In a Poisson distribution  $P(X=3)$  is  $2/3$  of  $P(X=4)$ . Find the mean and the standard deviation. [Ans.:  $m = 6, \sqrt{6}$ ]
5. In a Poisson distribution the probability  $p(x)$  for  $x=0$  is 20 percent. Find the mean of the distribution. [Ans.:  $m = 2.9957$ ]
6. If  $X$  is a Poisson variate and  $P(X=0) = 6P(X=3)$ , find  $P(X=2)$ . [Ans.:  $0.1901$ ]
7. If a random variable  $X$  follows Poisson distribution such that  $P(X=2) = 9P(X=4) + 90P(X=6)$ , find the mean and the variance of  $X$ . [Ans.: mean = variance =  $m = 1$ ]
8. If  $X$  is a Poisson variate such that  $P(X=1) = P(X=2)$ , find  $E(X^2)$ . [Ans.:  $6$ ]
9. The probability that a Poisson variable  $X$  takes a positive value is  $1 - e^{-1.5}$ . Find the variance and the probability that  $X$  lies between  $-1.5$  and  $1.5$ .

- (Hint:  $P(X>0) = 1 - P(X=0) = 1 - e^{-1.5}$   
 $\therefore 1 - e^{-m} = 1 - e^{-1.5} \therefore m = 1.5$
- $$P(-1.5 < X < 1.5) = P(X=0) + P(X=1) = 2.5(e^{-1.5})$$
10. If  $X$  is a Poisson variate with mean 4 and  $Y$  is a Poisson variate with mean 5, what is the mean of the variate  $X+Y$ ? [Ans.: 9]
11. If  $X$  and  $Y$  are Poisson variates with mean 2 and 4 respectively, find  $P((X+Y) \geq 4)$ . [Ans.: 0.45]
12. If  $X$  and  $Y$  are Poisson variates with parameters 3 and 4, find the variance of  $4X-3Y$ . [Ans.: 84]
13. If  $X$  and  $Y$  are independent Poisson variates such that  $P(X=1) = P(X=2)$  and  $P(Y=2) = P(Y=3)$ , find the variance of  $3X-4Y$ . [Ans.: 66]
14. If the mean of the Poisson distribution is 2. Find the probabilities of  $x=1, 2, 3, 4$ , from the recurrence relation of probability. (M.U. 2004)
- [Ans.:  $m = 2, p(x+1) = \frac{m}{x+1} p(x)$
- $$P(0) = e^{-2}, p(1) = 2e^{-2}, p(2) = e^{-2}, p(3) = \frac{2}{3}e^{-2}, p(4) = \frac{1}{3}e^{-2}.$$
15. If the variance of the Poisson distribution is 1.2. Find the probabilities for  $r=1, 2, 3, 4$  from the recurrence relation. (M.U. 2004) [Ans.:  $m = 1.2, P(0) = e^{-1.2}$  etc.]
16. In sampling a large number of parts manufactured by a machine, the mean number of defectives in a sample of 20 is 2. Out of 100 such samples, how many would you expect to contain 3 defectives (i) using the Binomial distribution, (ii) Poisson distribution. (M.U. 2004, 15)
- [Ans.: (i)  $p = 0.1, q = 0.9, p(x=3) = {}^{20}C_3 (0.1)^3 (0.9)^{17} = 0.1901$ , No. =  $Np = 190$ .  
(ii)  $m = np = 20 \times \frac{1}{10} = 2, P(X=3) = e^{-2} \times \frac{2^3}{3!} = 0.18$ , No. =  $Np = 180$ ]
17. If  $X_1, X_2, X_3$  are three independent Poisson variates with parameters 1, 2, 3 respectively, find  $P[(X_1 + X_2 + X_3) \leq 3]$  and  $P[X_1 = 1 / (X_1 + X_2 + X_3) = 3]$  [Ans.: (i) 0.15, (ii) 25/72]
18. Using Poisson distribution, find the approximate value of  ${}^{300}C_2 (0.03)^2 (0.97)^{298} + {}^{300}C_3 (0.03)^3 (0.97)^{297}$ . [Ans.: 0.1338]
19. If 2 percent bulbs are known to be defective bulbs, find the probability that in a lot of 300 bulbs there will be 2 or 3 defective bulbs, using (i) Binomial distribution, (ii) Poisson distribution. [Ans.: (i) 0.1319, (ii) 0.1338]
- (B) 1. In a certain manufacturing process 5% of the tools produced turn out to be defective. Find the probability that in a sample of 40 tools at most 2 will be defective. (Given:  $e^{-2} = 0.135$ ) [Ans.:  $m = np = 40 \times \frac{5}{100} = 2$ , prob. = 0.675]
2. It is 1 in 1000 that an article is defective. There are in a box 100 articles of this type. Assuming Poisson distribution, find the probability that the box contains one or more defective articles. (Given:  $e^{-0.1} = 0.9048$ ). [Ans.: 0.0952]

3. If the probability that an individual suffers a bad reaction from a particular injection is 0.01, determine the probability that out of 2,000 individuals (i) exactly three, (ii) more than two individuals will suffer a bad reaction.  
 (Given :  $e^{-2} = 0.1353$ ). (M.U. 2001) [Ans. : (i) 0.1804, (ii) 0.3233]

4. In a city there are a large number of street-lamps of which on an average 3 are non-working. Find the probability that on a particular night exactly two lamps are not working.  
 (Given :  $e^{-3} = 0.0498$ ). [Ans. : 0.2240]

5. The number of accidents on a particular highway in a month is a Poisson variable with parameter 5. Find the probability that more than 2 accidents have occurred on the road in a given month. [Ans. : 0.7554]

6. It is known from the past experience that in a certain plant there are on the average 4 industrial accidents per year. Find the probability that in a given year there will be less than 4 accidents. Assume Poisson distribution. (M.U. 1998) [Ans. : 0.43]

7. Find the probability that at most 5 defective fuses will be found in a box of 200 fuses, if experience shows that 2% of such fuses are defective. (M.U. 2002) [Ans. :  $m = np = 200 \times 0.02 = 4; 0.7851$ ]

8. Assume that the probability of an individual coal miner being killed in a mine accident during a year is  $1/2400$ . Use appropriate statistical distribution to calculate the probability that in a mine employing 200 miners there will be at least one fatal accident every year. (M.U. 2001) [Ans. : 0.200 / 2400 : 0.08]

9. If the variance of a Poisson distribution is 1.2, find the probabilities of  $X = 1, 2, 3, 4$  from recurrence relation. (M.U. 2004) [Ans. : 0.3614, 0.2169, 0.0867, 0.026]

10. The probability that a man aged 40 years will die within next year is 0.001. What is the probability that out of 100 such persons at least 99 will survive till next year?  
 (Given :  $e^{-0.1} = 0.9048$ ). [Ans. : 0.9996]

11. Between the hours of 2 and 4 p.m. the average number of phone calls per minute coming into the switch board of a company is 2.5. Find the probability that during a particular minute there will be (i) no phone call at all, (ii) 4 or less calls. (M.U. 2003) [Ans. : (i) 0.0821, (ii) 0.8909]

12. Which probability distribution is appropriate to describe the situation where 100 misprints are randomly distributed over 100 pages of a book. For this distribution find the probability that a page selected at random will contain atleast 3 misprints ?  
 (Given :  $e^{-1} = 0.3679$ ). [Ans. : Poisson  $m = 1, 0.0803$ ]

13. A manufacturer of pins knows that on an average 5% of his product is defective. He sells pins in boxes of 100 and guarantees that no more than 4 pins will be defective. What is the probability that a box will meet the guaranteed quality ? [Ans. : 0.44]

14. Suppose that a local appliances shop has found from experience that the demand for tube lights is roughly distributed as Poisson with a mean of 4 tube lights per week. If the shop keeps 6 during that week what is the probability that the demand will exceed the supply  
 (Given :  $e^{-4} = 0.0183$ ). (M.U. 1998) [Ans. : 0.3066]

15. It is known that in a certain plant, there are on an average 4 industrial accidents per month. Find the probability that in a given month there will be less than 4 accidents.  
 (Given :  $e^{-4} = 0.0183$ ). [Ans. : 0.4335]

16. Accidents occur on a particular stretch of highway at an average rate 3 per week. What is the probability that there will be exactly two accidents in a given week ?  
 (Given :  $e^{-3} = 0.0498$ ). [Ans. : 0.224]

17. 1% articles produced by a machine are defective. What is the probability that (i) none, (ii) two or more articles are defective in a sample of 100 ? [Ans. : (i) 0.3679, (ii) 0.2842]

18. If 3% bulbs manufactured by a company are defective, assuming Poisson distribution find the probability that in a pack of 100 bulbs (i) none, (ii) two bulbs are defective. [Ans. : (i) 0.0498, (ii) 0.2240]

19. In a town 10 accidents occur in a period of 50 days. Assuming Poisson distribution find the probability that there will be three or more accidents per day. [Ans. : 0.0012]

20. The average number of customers who appear at a counter of a certain bank per minute is two. Find the probability that during a given minute (i) no customer appears, (ii) three or more customers appear. [Ans. : (i) 0.1353, (ii) 0.3233]

- (C) 1. A manufacturer of electric bulbs sends out 500 lots each consisting of 100 bulbs. If 5% bulbs are defective in how many lots can we expect (i) 97 or more good bulbs, (ii) less than 97 good bulbs ? (M.U. 1997) [Ans. : (i) 62, (ii) 368]

2. In sampling a large number of parts manufactured by a machine, the number of defectives in a sample of 40 is 2. Out of 1000 such samples, how many would be expected to contain 3 defective parts, by using (i) Binomial distribution, (ii) Poisson distribution ? (M.U. 2003)

$$[Ans. : (i) 1000 \cdot {}^{20}C_3 (0.1)^3 (0.9)^{17} = 190, (ii) 1000 \cdot e^{-2} \frac{(2)^3}{3!} = 180]$$

3. A firm produces articles, 0.1 percent of which are defective. It packs them in cases containing 500 articles. If a wholesaler purchases 100 such cases, how many cases can be expected (i) to be free from defective, (ii) to have one defective ? (M.U. 1999, 2001) [Ans. : (i) 61, (ii) 30]

4. A manufacturer finds that the average demand per day for the mechanic to repair his new production is 1.5. Over a period of one year the demand per day is distributed as Poisson distribution. He employs two mechanics. On how many days in one year (a) both mechanics would be free, (b) some demand is refused ? (Given :  $e^{-1.5} = 0.2231$ ). [Ans. : (a) 81.4, (b) 69.6]

5. In a certain factory producing certain articles the probability that an article is defective is 1 / 500. The articles are supplied in packets of 20. Find approximately the number of packets containing no defective, one defective, two defectives in a consignment of 20,000 packets. (M.U. 1999) [Ans. : 19200, 768, 15]

6. A manufacturer of certain articles knows that on an average 5% of the articles are defective. He sells them in boxes of 100 and guarantees that no more than 4 articles will be defective. In how many boxes out of 1000 he will meet the guaranteed quality ? [Ans. : 440]

7. In a certain factory turning out blades there is a small chance 1 / 250 for a blade to be defective. The blades are supplied in packets of 10. Calculate the approximate number of packets containing (i) no defective, (ii) one defective, (iii) two defective blades in a consignment of 10,000 packets using (a) Binomial Distribution, (b) Poisson approximation to Binomial distribution. [Ans. : (a) (i) 9607, (ii) 386, (iii) 7; (b) (i) 9608, (ii) 384, (iii) 8]

8. In a certain factory producing certain articles the probability that an article is defective is 1 / 400. The articles are supplied in packets of 10. Find approximately the number of packets in a

consignment of 20,000 packets containing (i) no defective, (ii) one defective and (iii) two defective blades using (a) Binomial Distribution, (b) Poisson approximation to Binomial distribution.

[Ans. : (a) (i) 19506, (ii) 489, (iii) 6; (b) (i) 19506, (ii) 488, (iii) 6]

(D) 1. Fit a Poisson distribution to the following data

$X$	0	1	2	3	4	Total
$f$	192	100	24	3	1	320

[Ans. :  $m = 0.5$ , Frequencies : 194, 97, 24, 4, 1]

2. Fit a Poisson distribution to the following data.

$X$	0	1	2	3	4	Total
$f$	122	60	15	2	1	200

[Ans. :  $m = 0.595$ , Frequencies : 121, 61, 15, 3, 0]

3. The following mistakes per page were observed in a book.

No. of mistakes	0	1	2	3	4	Total
No. of pages	211	90	19	5	0	325

Fit a Poisson distribution.

[Ans. :  $m = 0.44$ , Frequencies : 209, 92, 20, 3, 1]

4. Fit a Poisson distribution to the following data.

No. of defects per piece	0	1	2	3	4	Total
No. of pieces	43	40	25	10	2	120

[Ans. : No. of defects per piece : 0, 1, 2, 3, 4, Total (M.U. 1997)]

No. of pieces	42	44	24	8	2	120
---------------	----	----	----	---	---	-----

5. Fit a Poisson distribution to the following data.

$X$	0	1	2	3	4	5	6	7
$f$	314	335	204	86	29	9	3	0

[Ans. :  $X$  : 0, 1, 2, 3, 4, 5, 6, 7 (M.U. 2004)]

$f$	295	354	212	85	26	6	1	11
-----	-----	-----	-----	----	----	---	---	----

6. Fit a Poisson distribution to the following data.

$X$	0	1	2	3	4	5	6	7	8
$f$	56	156	132	92	37	22	4	0	1

[Ans. :  $X$  : 0, 1, 2, 3, 4, 5, 6, 7, 8 (M.U. 2004, 07, 09, 15)]

$f$	70	137	135	89	44	17	6	2	0
-----	----	-----	-----	----	----	----	---	---	---

7. Fit a Poisson distribution to the following data.

$X$	0	1	2	3	4	5	Total
$f$	142	156	69	27	5	1	400

[Ans. :  $X$  : 0, 1, 2, 3, 4, 5 Total (M.U. 2002, 03, 04, 11)]

$f$	147	147	74	24	6	2	400
-----	-----	-----	----	----	---	---	-----

#### 4. Normal Distribution

Normal distribution is one of the most important and commonly used continuous distribution. It was first developed by DeMoivre but it is credited to Gauss who referred to it first in 1809. A large number of continuous variates follow this distribution, hence, the name 'normal'.

Abraham De Moivre (1667 - 1754)

A French mathematician who made important contributions to statistics, theory of probability and trigonometry. The concept of statistically independent events was first developed by De Moivre. Through the use of complex number he transformed trigonometry from a branch of geometry to a branch of analysis. His treatise on probability has influenced the development of probability theory.

Karl Friedrich Gauss (1777 - 1855)

Biography about Karl Friedrich Gauss is given in Chapter 4 on page 4-1.



A renowned mathematician Poincaré has remarked that "there must be something mysterious about the normal distribution because mathematicians think it is a law of nature whereas physicists are convinced that it is a mathematical theorem."

1. Definition : A continuous random variable  $X$  is said to follow **normal distribution** with parameter  $m$  (called mean) and  $\sigma^2$  (called variance), if its probability density function is given by

$$f(x) = \frac{1}{\sqrt{2\pi} \cdot \sigma} e^{-\frac{1}{2} \left( \frac{x-m}{\sigma} \right)^2} \quad -\infty < x < \infty$$

$$-\infty < m < \infty, \sigma^2 > 0$$

Remarks ....

(i) A continuous random variate  $X$  following normal distribution with mean  $m$  and standard deviation  $\sigma$  is referred to as  $X \sim N(m, \sigma)$ .

(ii) If  $X$  is a normal variate with parameter  $m, \sigma$ , then  $Z = \frac{X-m}{\sigma}$  is also a normal variate with mean = 0 and standard deviation = 1.

It is called **Standard Normal Variate**.

#### 2. Importance of Normal Distribution

- (i) The variables such as height, weight, intelligence etc. follow normal distribution.
- (ii) Many other distributions occurring in practice such as Binomial, Poisson etc. can be approximated by normal distribution.
- (iii) Many of the distributions of sample statistic e.g. Sample Mean, Sample Variance tend to normal distribution for large samples.
- (iv) Normal distribution has wide applications in Statistical Quality Control.
- (v) Errors in measurements of physical quantities follow normal distribution.
- (vi) It is also useful in psychological and educational research.

## (a) Mean and Variance of the Normal Distribution

(i) By definition mean is given by

$$\begin{aligned} \text{Mean} &= E(X) = \int_{-\infty}^{\infty} x f(x) dx \\ &= \int_{-\infty}^{\infty} [(x-m) + m] f(x) dx \\ &= \int_{-\infty}^{\infty} (x-m) f(x) dx + m \int_{-\infty}^{\infty} f(x) dx \end{aligned}$$

But the first integral is zero, because the first moment about the mean is zero [ See (2), § 12, page 6-22 ] and the second integral is unity.

∴ Mean =  $m$ 

$$\begin{aligned} \text{(ii) Now, } \text{Var}(X) &= E(X-m)^2 = \int_{-\infty}^{\infty} (x-m)^2 f(x) dx \\ &= \int_{-\infty}^{\infty} (x-m)^2 \cdot \frac{1}{\sqrt{2\pi} \cdot \sigma} e^{-\frac{1}{2} \left(\frac{x-m}{\sigma}\right)^2} dx \end{aligned}$$

Now, put  $\frac{x-m}{\sigma} = t \quad \therefore dx = \sigma dt$ .

$$\begin{aligned} \therefore \text{Var}(X) &= \int_{-\infty}^{\infty} \sigma^2 \cdot t^2 \cdot \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{1}{2} t^2} dt \\ &= \frac{\sigma^2}{\sqrt{2\pi}} \int_{-\infty}^{\infty} t^2 \left( -e^{-\frac{1}{2} t^2} \right) dt \end{aligned}$$

Now, integrating by parts

$$\text{Var}(X) = \frac{\sigma^2}{\sqrt{2\pi}} \left[ t \left( -e^{-\frac{1}{2} t^2} \right) \right]_{-\infty}^{\infty} + \int_{-\infty}^{\infty} e^{-\frac{1}{2} t^2} dt$$

[ By Gamma Functions,  $\int_{-\infty}^{\infty} e^{-\alpha x^2} dx = \sqrt{\frac{\pi}{\alpha}}$ . Refer to Applied Mathematics - II ]

$$= \frac{\sigma^2}{\sqrt{2\pi}} [0 + \sqrt{2\pi}] = \sigma^2$$

∴ Var.(X) =  $\sigma^2$ 

Note ...

A normal variate with mean  $m$  and standard deviation  $\sigma$  is shortly denoted as  $N(m, \sigma)$ .

Remark ...

Here we simply note that mean, median and mode of the normal distribution are equal to  $m$ .

$$\text{Mean} = \text{Median} = \text{Mode} = m$$

(M.U. 2009)

## (b) Moment Generating Function of Normal Distribution

By definition,

$$\begin{aligned} M_0(t) &= E(e^{tX}) = \int_{-\infty}^{\infty} e^{tx} f(x) dx \\ &= \int_{-\infty}^{\infty} e^{tx} \frac{1}{\sqrt{2\pi} \cdot \sigma} e^{-\frac{1}{2} \left(\frac{x-m}{\sigma}\right)^2} dx \end{aligned}$$

Putting  $\frac{x-m}{\sigma} = z, \frac{dx}{\sigma} = dz$ 

$$\begin{aligned} M_0(t) &= \int_{-\infty}^{\infty} e^{t(m+\sigma z)} \cdot \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{1}{2} z^2} dz \\ &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} \cdot e^{mt} \cdot e^{-\frac{1}{2} (z^2 - 2t\sigma z)} dz \end{aligned}$$

Now  $z^2 - 2t\sigma z = (z-t\sigma)^2 - t^2\sigma^2$ 

$$\therefore M_0(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{mt} \cdot e^{-\frac{1}{2} (z-t\sigma)^2} \cdot e^{\frac{1}{2} t^2 \sigma^2} dz$$

Putting  $u = z - t\sigma$ 

$$\begin{aligned} M_0(t) &= \frac{1}{\sqrt{2\pi}} \cdot e^{mt + \frac{t^2 \sigma^2}{2}} \int_{-\infty}^{\infty} e^{-\frac{1}{2} u^2} du \\ &= \frac{1}{\sqrt{2\pi}} \cdot e^{mt + \frac{t^2 \sigma^2}{2}} \cdot 2 \int_0^{\infty} e^{-\frac{1}{2} u^2} du \\ &= e^{mt + \frac{t^2 \sigma^2}{2}} \cdot \frac{1}{\sqrt{2\pi}} \cdot \sqrt{2\pi} \quad \left[ \because \int_0^{\infty} e^{-ax^2} dx = \frac{1}{2} \sqrt{\frac{\pi}{a}} \right] \end{aligned}$$

$$M_0(t) = e^{mt + \frac{t^2 \sigma^2}{2}}$$

$$\text{Now, } M_0(t) = e^{mt} \cdot e^{t^2 \sigma^2 / 2} = \left[ 1 + mt + \frac{m^2 t^2}{2!} + \dots \right] \left[ 1 + \frac{t^2 \sigma^2}{2!} + \frac{t^4 \sigma^4}{4!} + \dots \right]$$

∴  $\mu_1' = \text{Coefficient of } t = m$ ,

$$\mu_2' = \text{Coefficient of } \frac{t^2}{2!} = m^2 + \sigma^2$$

∴ Mean =  $\mu_1' = m$ 

$$\text{Variance} = \mu_2' - \mu_1'^2 = m^2 + \sigma^2 - m^2 = \sigma^2$$

**Corollary :** Since mean of the standard normal variate is zero and the standard deviation is unity, putting  $m = 0$  and  $\sigma = 1$  in the above m.g.f., we get the moment generating function of the standard normal variate as

$$M_0(t) = e^{t^2/2}$$

**Moments of Normal Distribution :** The m.g.f. about mean is given by

$$\begin{aligned} M_2(t) &= E[e^{t(x-m)}] = E(e^{tx} \cdot e^{-tm}) \\ &= e^{-tm} E(e^{tx}) = e^{-tm} M_0(t) \\ &= e^{-tm} + e^{tm} + t^2 \sigma^2 / 2 = e^{tm} e^{t^2 \sigma^2 / 2} \\ &= 1 + (t^2 \sigma^2 / 2) + \frac{(t^2 \sigma^2 / 2)^2}{2!} + \frac{(t^2 \sigma^2 / 2)^3}{3!} + \dots \end{aligned}$$

Now,  $\mu_r$  = coefficient of  $\frac{t^r}{r!}$ .

Since, no odd power of  $t$  appears in the above expansion, moments of odd powers about mean of a normal distribution are zero.

$$\therefore \mu_{2n+1} = 0, \quad n = 0, 1, 2, \dots \quad (1)$$

Moments of even power

$$\begin{aligned} \mu_{2n} &= \text{coefficient of } \frac{t^{2n}}{(2n)!} = \frac{(\sigma^2/2)^n}{n!} \cdot (2n)! \\ &= \frac{\sigma^{2n}}{2^n n!} [2n(2n-1)(2n-2)\dots 4 \cdot 3 \cdot 2 \cdot 1] \\ &= \frac{\sigma^{2n}}{2^n n!} [2 \cdot n(2n-1) \cdot 2(n-1)(2n-3)\dots 4 \cdot 3 \cdot 2 \cdot 1] \\ &= \frac{\sigma^{2n}}{2^n n!} 2^n n!(2n-1)(2n-3)\dots 5 \cdot 3 \cdot 1 \\ \mu_{2n} &= 1 \cdot 3 \cdot 5 \dots (2n-1) \cdot \sigma^{2n} \quad (2) \end{aligned}$$

(c) **Moment Generating Function of Standard Normal Variate**

(M.U. 2006)

We shall here find the moment generating function of Standard Normal Variate and from the m.g.f., we shall obtain the mean and variance of S.N.V.  $Z = \frac{X-m}{\sigma}$ .

$$\text{Let } f(x) = \frac{1}{\sqrt{2\pi} \cdot \sigma} e^{-\frac{1}{2} \left( \frac{x-m}{\sigma} \right)^2}, \quad -\infty < x < \infty, \quad -\infty < m < \infty, \quad \sigma^2 > 0$$

Now putting,  $\frac{x-m}{\sigma} = z$ ,  $dx = \sigma dz$ , we get  $f(z) = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2} z^2}$ .

$$\begin{aligned} \therefore M_0(t) &= E(e^{tz}) = \int_{-\infty}^{\infty} e^{tz} f(z) dz = \int_{-\infty}^{\infty} e^{tz} \cdot \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2} z^2} dz \\ &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{\frac{1}{2}(t^2 - 2tz)} dz. \end{aligned}$$

$$\text{Now, } z^2 - 2tz = (z-t)^2 - t^2$$

$$\therefore M_0(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{1}{2}(z-t)^2} \cdot e^{t^2/2} dz$$

Now, put  $z-t=u$ ,  $dz=du$

$$\begin{aligned} M_0(t) &= \frac{e^{t^2/2}}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{1}{2}u^2} \cdot du = \frac{e^{t^2/2}}{\sqrt{2\pi}} \int_0^{\infty} 2 \cdot e^{-u^2/2} \cdot du \\ &= \frac{e^{t^2/2}}{\sqrt{2\pi}} \cdot 2 \cdot \sqrt{\frac{\pi}{2}} = e^{t^2/2} = 1 + \frac{t^2}{2} + \frac{(t^2/2)^2}{2!} + \dots \end{aligned}$$

$\therefore$  Mean = coefficient of  $t = 0$ . Variance = coefficient of  $\frac{t^2}{2!} = 1$ .

$\therefore$  Mean and standard deviation of Standard Normal Variate are zero and one respectively.

**After:** We shall obtain mean and variance of Standard Normal Variate from the definitions.

$$(i) \text{ Mean } \bar{Z} = E(Z) = \int_{-\infty}^{\infty} z \cdot e^{-z^2/2} dz$$

But the function on the r.h.s. is an odd function, hence, the definite integral is zero.

$\therefore$  Mean = 0.

$$(ii) \mu_2' = E(Z^2) = \int_{-\infty}^{\infty} z^2 \cdot e^{-z^2/2} dz$$

Since the function on the r.h.s. is an even function,

$$\mu_2' = \frac{2}{\sqrt{2\pi}} \int_0^{\infty} z^2 \cdot e^{-z^2/2} dz$$

$$\text{Now, put } \frac{z^2}{2} = t \quad \therefore z = \sqrt{2t} \quad \therefore dz = \frac{\sqrt{2}}{2\sqrt{t}} dt$$

$$\therefore \mu_2' = \frac{2}{\sqrt{2\pi}} \int_0^{\infty} 2t \cdot e^{-\frac{t}{2}} \cdot \frac{\sqrt{2}}{2\sqrt{t}} dt = \frac{2}{\sqrt{\pi}} \int_0^{\infty} e^{-t/2} t^{1/2} dt = \frac{2}{\sqrt{\pi}} \int_0^{\infty} \frac{1}{2} t^{1/2} dt$$

$$= \frac{2}{\sqrt{\pi}} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{2}{\sqrt{\pi}} \cdot \frac{1}{2} \cdot \frac{1}{2} \sqrt{\pi} = 1$$

$\therefore$  Variance =  $\mu_2' - \mu_1'^2 = 1 - 0 = 1$ .

(d) **Linear Combination (Additive Property)**

**Theorem :** Let  $X_i, i = 1, 2, 3, \dots, n$  be  $n$  independent normal variates with mean  $m_i$  and variance  $\sigma_i^2$ . Let their linear combination be denoted by  $Y$  i.e.

$$Y = a_1 X_1 + a_2 X_2 + \dots + a_n X_n$$

Then  $Y$  is also a normal variate with mean  $m$  and variance  $\sigma^2$  where

$$m = a_1 m_1 + a_2 m_2 + \dots + a_n m_n \quad \text{and} \quad \sigma^2 = a_1 \sigma_1^2 + a_2 \sigma_2^2 + \dots + a_n \sigma_n^2.$$

**Proof :** We know that m.g.f. of a normal variate with mean  $m$  and variance  $\sigma^2$  is given by

$$M_0(t) = e^{mt + t^2 \sigma^2 / 2}$$

Further  $M_Y(t) = M_{a_1 X_1 + a_2 X_2 + \dots + a_n X_n}$   
 $= M_{a_1 X_1}(t) \cdot M_{a_2 X_2}(t) \cdots M_{a_n X_n}(t)$   
(since  $X_1, X_2, \dots, X_n$  are independent variates.)

$$\begin{aligned} &= M_{X_1}(a_1 t) \cdot M_{X_2}(a_2 t) \cdots M_{X_n}(a_n t) \quad [\because M_{cX}(t) = M_X(ct)] \\ &= e^{a_1 m_1 t + a_1^2 \sigma_1^2 t^2/2} \cdot e^{a_2 m_2 t + a_2^2 \sigma_2^2 t^2/2} \cdots \\ &= e^{(a_1 m_1 + a_2 m_2 + \dots) t + (a_1^2 \sigma_1^2 + a_2^2 \sigma_2^2 + \dots) t^2/2} \end{aligned}$$

But from its form this is m.g.f. of a normal variate whose mean is  $(a_1 m_1 + a_2 m_2 + \dots)$  and whose variance is  $(a_1^2 \sigma_1^2 + a_2^2 \sigma_2^2 + \dots)$ .

**Remarks ...**

- This property is known as additive property of normal distribution.
- If  $a_3 = a_4 = \dots = a_n = 0$  then  $Y = a_1 X_1 + a_2 X_2$  is a normal variate with mean  $a_1 m_1 + a_2 m_2$  and variance  $a_1^2 \sigma_1^2 + a_2^2 \sigma_2^2$ .
- If  $a_1 = a_2 = 1, a_3 = a_4 = \dots = a_n = 0$ , then  $Y = X_1 + X_2$  is a normal variate with mean  $m_1 + m_2$  and variance  $\sigma_1^2 + \sigma_2^2$ .
- If  $a_1 = 1, a_2 = -1, a_3 = a_4 = \dots = a_n = 0$  then  $Y = X_1 - X_2$  is also a normal variate with mean  $m_1 - m_2$  and variance  $\sigma_1^2 + \sigma_2^2$ .
- Comparing Normal Distribution with Poisson Distribution we find that sum of two Normal or Poisson Variates is a Normal or Poisson variate. But although difference of two normal variates is a normal variate, the difference of two Poisson variates is not a Poisson variate.
- If  $X_i ; i = 1, 2, 3, \dots, n$  are  $n$  independent, identical normal variates all with the same mean  $m$  and same standard deviation  $\sigma$  and if we put  $a_1 = a_2 = a_3 = \dots = a_n = 1/n$  then  $Y = X_1 + X_2 + \dots + X_n$  is a normal variate with mean

$$m = \frac{m + m + \dots + m}{n} = m$$

$$\text{and } \sigma^2 = \frac{1}{n^2} \sigma^2 + \frac{1}{n^2} \sigma^2 + \dots + \frac{1}{n^2} \sigma^2 = \frac{n \sigma^2}{n^2} = \frac{\sigma^2}{n}$$

In other words,  $Y$  is a normal variate with mean  $m$  and standard deviation  $\sigma/\sqrt{n}$ .

**(e) Area Property**

\* If  $X$  is a normal variate with mean  $m$  and variance  $\sigma^2$  and  $Z$  is standard normal variate (with mean zero and variance one) then the area under the normal curve of  $X$  between  $X = m$  and  $X = x_1$  is equal to the area under the S.N. Curve of  $Z$  between  $Z = 0$  to  $Z = z_1$  (say, corresponding to  $x_1$ ).

**Proof :** Consider a normal variate  $X$  with mean  $m$  and variance  $\sigma^2$ .

$$\text{Then } P(m \leq X \leq x_1) = \frac{1}{\sqrt{2\pi} \cdot \sigma} \int_m^{x_1} e^{-\frac{1}{2} \left(\frac{X-m}{\sigma}\right)^2} dx$$

$$\text{Now, put } \frac{X-m}{\sigma} = Z$$

When  $X = m, Z = 0$ ; when  $X = x_1, Z = \frac{x_1 - m}{\sigma} = z_1$  say

$$\therefore P(m \leq X \leq x_1) = P(0 \leq Z \leq z_1) = \frac{1}{\sqrt{2\pi}} \int_0^{z_1} e^{-\frac{1}{2} z^2} dz$$

Thus, the area under the normal curve from  $m$  to  $x_1$  is equal to the area under the standard normal curve from  $0$  to  $z_1$ .

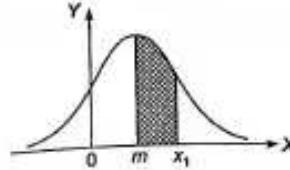


Fig. 7.1

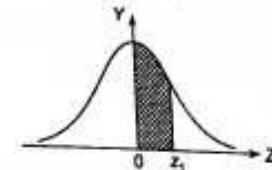


Fig. 7.2

The integral  $\frac{1}{\sqrt{2\pi}} \int_0^{z_1} e^{-\frac{1}{2} z^2} dz$  is denoted by  $\int_0^{z_1} \phi(z) dz$  and is known as normal probability integral. The areas under standard normal curve from  $z = 0$  to various values of  $z_1$  have been calculated and are given in the table at the end of the book.

**Reverse Problem :** In some problems we know that  $X$  is a normal variate with mean  $m$  and standard deviation  $\sigma$ . We are required to find the value of  $X = x_1$  corresponding to a given probability. Suppose, we want to find of  $X = x_1$  such that  $P(X > x_1) = \alpha$ . In this case also we consider

$$\text{S.N.V. } Z = \frac{X - m}{\sigma}$$

We now consult the area table and find the value of  $Z = z_1$  for which area to the right is  $\alpha$  i.e. area between  $z = 0$  to  $Z = z_1$  is  $(0.5 - \alpha)$ . From this value of  $z_1$  we get  $X$  using

$$z_1 = \frac{x_1 - m}{\sigma}$$

$$\text{i.e. } x_1 = m + z_1 \sigma.$$

**Remarks ...**

- Since standard normal curve is symmetrical about the y-axis it is enough to find the areas to the right. The areas to the left of y-axis at equal distances will be equal.
- The total area under the curve is unity. Hence, because of symmetry the area under S.N.V. to the right of the y-axis is 0.5.
- To find the probability that  $X$  will lie between  $x_1$  and  $x_2$  ( $x_1 < x_2$ ), we find the corresponding values of S.N.V.  $Z$  (from  $Z = \frac{X - m}{\sigma}$ ) say  $z_1$  and  $z_2$  and find the area from  $z_1$  to  $z_2$  and S.N. Curve. The required probability is this area.

$$P(x_1 \leq X \leq x_2) = P(z_1 \leq Z \leq z_2)$$

= area between  $Z = z_1$  and  $Z = z_2$  under the S.N. curve.

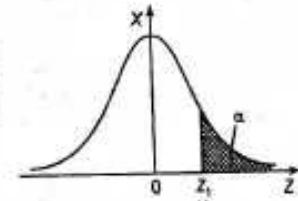


Fig. 7.3

(i) The Quartile Deviation of a Normal Distribution is  $(2/3)$  S.D.

Let  $X$  be a normal variate with mean  $m$  and variance  $\sigma^2$ . Consider the standard normal variate

$$Z = \frac{X - m}{\sigma}$$

When  $X = m$ ,  $Z = 0$  and when  $X = Q_3$  the third quartile let  $Z = \frac{Q_3 - m}{\sigma} = z_1$ .

We know that for Normal variate mean = median = mode =  $m$ , i.e. the mean  $m$  divides the area into two equal parts. Hence, the area from  $Q_1$  to  $m$  is 0.25. For S.N.V. area from 0 to  $z_1$  is 0.25. For area 0.25 we find from the table that,

$$z_1 = 0.6745 = \frac{2}{3}$$

$\therefore Q_3 = m + \sigma z_1 = m + \frac{2}{3} \sigma$ , Similarly,  $Q_1 = m - \sigma z_1 = m - \frac{2}{3} \sigma$ .

$$\text{Quartile Deviation} = \frac{Q_3 - Q_1}{2} = \frac{2}{3} \sigma$$

#### (g) Properties of the Normal Distribution

We summaries below important properties of normal distribution which we have proved above. They are given in terms of the properties of the normal curve.

(i) The normal curve is bell-shaped and symmetrical about the maximum ordinate at  $x = m$ , the mean. In other words, the curve is divided into two equal parts by this ordinate. The curve on one side of this ordinate is the mirror image of the curve on the other side.

(ii) The curve has maximum height at  $x = m$ . Hence the mode of the distribution is also  $m$ . The ordinate  $x = m$  divides the area under the curve into two equal parts. Hence the median of the distribution is also  $m$ . Thus, for the normal distribution,

$$\text{mean} = \text{median} = \text{mode} = m$$

(iii) The height of the curve goes on decreasing on either side of the ordinate at  $x = m$  but never becomes zero. In other words, the curve never intersects the  $x$ -axis at any finite point. The  $x$ -axis touches it at infinity.

(iv) Since the curve is symmetrical about mean, the first quartile  $Q_1$  and the third quartile  $Q_3$  are at the same distance on the two sides of the mean. The distance of any quartile from the mean is 0.6745  $\sigma$  units. Hence,

$$Q_1 = m - 0.6745 \sigma \quad \text{or} \quad Q_1 = m - \frac{2}{3} \sigma \quad \text{and}$$

$$Q_3 = m + 0.6745 \sigma \quad \text{or} \quad Q_3 = m + \frac{2}{3} \sigma$$

Hence, middle 50% items lie between  $m - \frac{2}{3} \sigma$  and  $m + \frac{2}{3} \sigma$ . Further, the quartile deviation of a normal distribution is given by

$$\text{Q.D.} = \frac{Q_3 - Q_1}{2} = \frac{\left(m + \frac{2}{3} \sigma\right) - \left(m - \frac{2}{3} \sigma\right)}{2} = \frac{2}{3} \sigma$$

$$\therefore \text{Q.D.} = \frac{2}{3} \sigma$$

(v) The mean of the distribution is  $m$  and the standard deviation is  $\sigma$ .

(vi) The mean deviation is given by

$$\text{M.D.} = \frac{4}{5} \sigma$$

$$(\text{vii}) \text{ Now, } \frac{\text{Q.D.}}{\text{M.D.}} = \frac{(2/3)\sigma}{(4/5)\sigma} = \frac{2}{3} \times \frac{5}{4} = \frac{10}{12}$$

$$\text{Also, } \text{M.D.} = \frac{4}{5} \sigma \quad \therefore \frac{\text{M.D.}}{\sigma} = \frac{4}{5} = \frac{12}{15}$$

$$\therefore \text{Q.D. : M.D. : S.D.} = 10 : 12 : 15$$

(viii) Odd central moments are zero i.e.

$$\mu_{2r+1} = 0 \quad \text{for } (r = 0, 1, 2, \dots)$$

$$\text{and} \quad \mu_{2r} = 1 + 3 + 5 + \dots + (2r-1) \sigma^{2r} (r = 0, 1, 2, \dots)$$

$$\text{i.e.,} \quad \mu_2 = \sigma^2, \quad \mu_4 = 3\sigma^4, \quad \mu_6 = 15\sigma^6$$

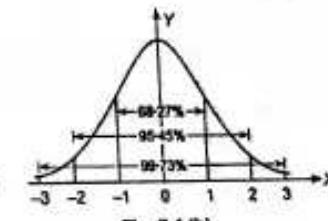
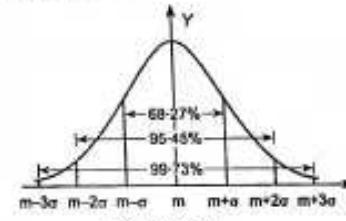
(ix) The area under the normal curve is distributed as follows,

(a) The area between  $x = m - \sigma$  and  $x = m + \sigma$  is 68.27 %.

(b) The area between  $x = m - 2\sigma$  and  $x = m + 2\sigma$  is 95.45 %.

(c) The area between  $x = m - 3\sigma$  and  $x = m + 3\sigma$  is 99.73 %.

These areas under the normal curve and standard normal curve are shown below.



#### (h) Normal Approximation To The Binomial Distribution

It can be proved, although we do not, that if  $X$  is a Binomial variate with parameter  $n$  and  $p$  (i.e. mean =  $np$  and S.D. =  $\sqrt{npq}$  where  $q = 1 - p$ ) then

$$Z = \frac{X - np}{\sqrt{npq}}$$

is a Standard Normal Variate if  $n \rightarrow \infty$  (i.e.  $n$  is large) and neither  $p$  nor  $q$  is small.

**Remark ...**

1. Normal distribution can be used in place of Binomial distribution when  $np$  and  $nq$  are both greater than 15.

2. Normal distribution can also be obtained from Poisson distribution when the parameter  $n \rightarrow \infty$ .

**Type I**

**Example 1 :** For a normal distribution the mean is 60 and the standard deviation is 15. Find (i)  $Q_1$  and  $Q_3$ , (ii) mean deviation (Also the interquartile range).

Sol. : (i) For a normal distribution

$$Q_1 = m - \frac{2}{3}\sigma = 60 - \frac{2}{3} \times 15 = 40$$

$$\text{Again } Q_3 = m + \frac{2}{3}\sigma = 60 + \frac{2}{3} \times 15 = 60$$

(ii) The mean deviation of the normal distribution is,

$$M.D. = \frac{4}{5}\sigma = \frac{4}{5} \times 15 = 12$$

$$\therefore \text{Interquartile range} = Q_3 - Q_1 = 60 - 40 = 20.$$

**Example 2 :** The first and the third quartiles of a normal distribution are 36 and 44. Find mean, standard deviation and the mean deviation.

Sol. : We have  $Q_1 = m - \frac{2}{3}\sigma$  and  $Q_3 = m + \frac{2}{3}\sigma$

$$\therefore 36 = m - \frac{2}{3}\sigma \quad \text{and} \quad 44 = m + \frac{2}{3}\sigma$$

$$\text{Adding } 80 = 2m \quad \therefore m = 40$$

$$\text{Then, } 36 = 40 - \frac{2}{3}\sigma \quad \therefore \frac{2}{3}\sigma = 4 \quad \therefore \sigma = 6$$

$$\text{And mean deviation} = \frac{4}{5}\sigma = \frac{4}{5} \times 6 = \frac{24}{5}$$

**Example 3 :** Find the probability that a random variable having the standard normal distribution will take on a value between 0.87 and 1.28.

Sol. :  $P(0.87 < Z < 1.28)$

= area between  $Z = 0.87$  and  $Z = 1.28$ .

= (area from  $Z = 0$  to  $Z = 1.28$ )

- (area from  $Z = 0$  to  $Z = 0.87$ )

= 0.3997 - 0.3078 = 0.0919.

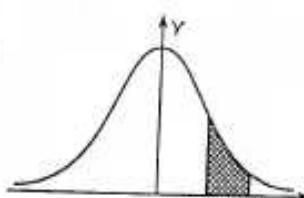


Fig. 7.5

**Example 4 :** Find the probability that a random variable having standard normal distribution will take a value between (i) 0.87 and 1.28, (ii) -0.34 and 0.62.

Sol. : (i) As in the above example.

(ii) Area from  $Z = -0.34$  to 0 is the same as  $Z = 0$  to  $Z = 0.34$  and is 0.1331.

Area from  $Z = 0$  to  $Z = 0.62$  is 0.2324.

Required area is the sum of the two

$$\therefore P(-0.34 < Z < 0.62) = 0.1331 + 0.2324$$

$$= 0.3655.$$

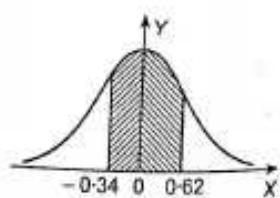


Fig. 7.6

**Example 5 :** For a normal variate with mean 2.5 and standard deviation 3.5, find the probability that (i)  $2 \leq X \leq 4.5$ , (ii)  $-1.5 \leq X \leq 5.5$ .

Sol. : We have S.N.V.  $Z = \frac{X - m}{\sigma} = \frac{X - 2.5}{3.5}$

$$(i) \text{ When } X = 2, \quad Z = \frac{2 - 2.5}{3.5} = -0.14$$

$$\text{When } X = 4.5, \quad Z = \frac{4.5 - 2.5}{3.5} = 0.57$$

$$P(2 \leq X \leq 4.5) = P(-0.14 \leq Z \leq 0.57)$$

= Area between ( $Z = -0.14$  and  $Z = 0.57$ )

+ Area between ( $Z = 0$  and  $Z = 0.57$ )

$$= 0.0557 + 0.2157 = 0.2714.$$

$$(ii) \text{ When } X = -1.5, \quad Z = \frac{-1.5 - 2.5}{3.5} = -1.14$$

$$\text{When } X = 5.5, \quad Z = \frac{5.5 - 2.5}{3.5} = 0.8$$

$$P(-1.5 \leq X \leq 5.5) = P(-1.14 \leq Z \leq 0.8)$$

= Area between ( $Z = -1.14$  and  $Z = 0.8$ )

+ Area between ( $Z = 0$  and  $Z = 0.8$ )

$$= 0.3729 + 0.2881 = 0.6610.$$

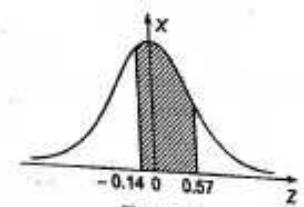


Fig. 7.7 (a)

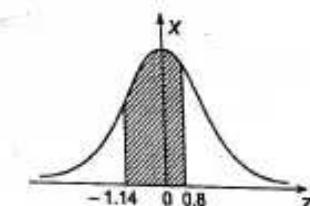


Fig. 7.7 (b)

**Example 6 :** If  $Z$  is a standard normal variate, find  $c$  such that

$$(i) P(-c < Z < c) = 0.95, \quad (ii) P(|Z| > c) = 0.01.$$

If  $X$  is a normal variate with mean 120 and standard deviation 10, find  $c$  such that

$$(i) P(X > c) = 0.02, \quad (ii) P(X < c) = 0.05.$$

Sol. : Consulting the table of S.N.V. we have to find the entry 0.475 and the corresponding value of  $Z$ . We find from the table that corresponding to the entry 0.4750,  $Z = 1.96$ .

Again consulting the table of S.N.V. we find the entry 0.495. Corresponding to the entry 0.495,  $Z = 2.58$ .  $\therefore c = 2.58$ .

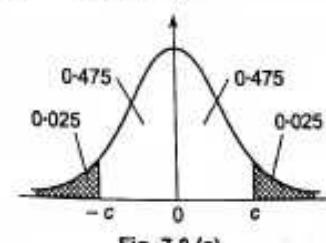


Fig. 7.8 (a)

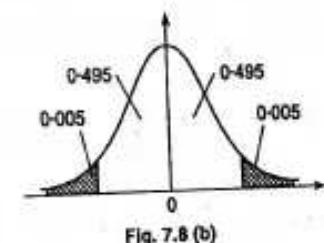


Fig. 7.8 (b)

If  $Z$  is a S.N.V. then  $Z = \frac{X - m}{\sigma} \therefore Z = \frac{X - 120}{10}$

$$\therefore P(X > c) = P(Z > c) = 0.02.$$

Corresponding to entry  $0.5 - 0.02 = 0.48$ ,  $Z = 2.05$ .

$$\therefore 2.05 = \frac{X - 120}{10} \quad \therefore X = 120 + 2.05 \times 10 = 140.5.$$

Again  $P(X < c) = P(Z < c) = 0.05$ .

Corresponding to entry  $0.5 - 0.05 = 0.45$ ,  $Z = 1.64$ .

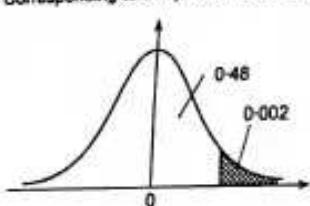


Fig. 7.8 (c)

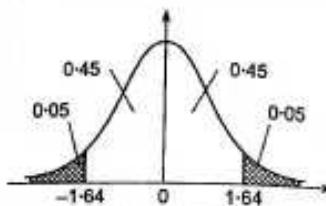


Fig. 7.8 (d)

$\therefore$  Since  $Z$  is less than  $c$ ,  $c$  must be negative  $\therefore c = -1.64$ .

$$\therefore -1.64 = \frac{X - 120}{10} \quad \therefore X = 120 - 10 \times 1.64 = 103.6$$

**Example 7:** If  $X$  is a normal variate with mean 10 and standard deviation 4, find

$$(i) P(|X - 14| < 1), (ii) P(5 \leq X \leq 18), (iii) P(X \leq 12). \quad (\text{M.U. 2002, 09, 16, 17})$$

**Sol.:** We have  $Z = \frac{X - m}{\sigma} = \frac{X - 10}{4}$

$$(i) \text{ When } X = 14, Z = \frac{14 - 10}{4} = 1$$

$$\therefore P(|X - 14| \leq 1) = P(|Z| \leq 1) = \text{area between } (Z = -1 \text{ and } Z = 1) \\ = 2(\text{area between } Z = 0 \text{ and } Z = 1) \\ = 2(0.3413) = 0.6826$$

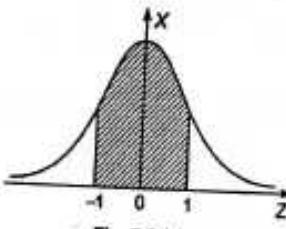


Fig. 7.9 (a)

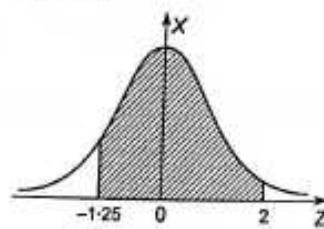


Fig. 7.9 (b)

$$(ii) \text{ When } X = 5, Z = \frac{5 - 10}{4} = -1.25,$$

$$\text{When } X = 18, Z = \frac{18 - 10}{4} = 2$$

$$P(5 \leq X \leq 18) = P(-1.25 \leq Z \leq 2)$$

= area between  $Z = -1.25$  and  $Z = 2$

= (area between  $Z = 0$  and  $Z = 1.25$ ) + (area between  $Z = 0$  and  $Z = 2$ )

$$= 0.3944 + 0.4772 = 0.8716$$

$$(iii) \text{ When } Z = 12, Z = \frac{12 - 10}{4} = 0.5$$

$$\therefore P(X \leq 12) = P(Z \leq 0.5) = \text{area upto } Z = 0 \leq 0.5$$

= (area from  $-\infty$  to  $Z = 0$ ) + (area from  $Z = 0$  to  $Z = 0.5$ )

$$= 0.5 + 0.1915 = 0.6915.$$

#### Type II

**Example 1:** In a factory turning out blades in mass production, it was found that in a packet of 100 blades on an average 16 blades are defective. Find the standard deviation of the defective blades. Can the distribution of defective blades be approximated to a normal distribution? If so write its equation. (M.U. 1999)

**Sol.:** The distribution of defective blades is a Binomial distribution,

$$\text{We have } n = 100, p = \frac{16}{100} = 0.16$$

$$\therefore \text{Mean } \bar{X} = np = 100 \times 0.16 = 16$$

$$\therefore q = 1 - p = 0.84 \quad \therefore nq = 100 \times 0.84 = 84.$$

Since both  $np$  and  $nq$  are greater than 15 as stated in the Remark 1 (page 7-46), the Binomial distribution can be approximated to Normal distribution.

$$\text{Now, as seen above, } \bar{X} = 16 \text{ and } \sigma = \sqrt{npq} = \sqrt{100 \times 0.16 \times 0.84} = 3.67.$$

$\therefore$  The equation of the normal distribution is

$$y = \frac{1}{\sqrt{2\pi} \cdot \sigma} e^{-\frac{1}{2} \left( \frac{x-m}{\sigma} \right)^2} = \frac{1}{\sqrt{2\pi} \cdot (3.67)} e^{-\frac{1}{2} \left( \frac{x-16}{3.67} \right)^2}.$$

**Example 2:** The marks obtained by students in a college are normally distributed with mean 65 and variance 25. If 3 students are selected at random from this college what is the probability that at least one of them would have scored more than 75 marks? (M.U. 2005)

$$\text{Sol. : We have S.N.V. } Z = \frac{X - m}{\sigma} = \frac{X - 65}{5}. \quad \text{When } X = 75, Z = \frac{75 - 65}{5} = 2$$

$$\therefore P(X > 75) = P(Z > 2) = 0.5 - (\text{area from } z = 0 \text{ to } z = 2) \\ = 0.5 - 0.4772 = 0.0228$$

This is the probability that a student chosen at random has scored more than 75 marks.

$$\therefore P(\text{a student has not scored more than 75}) = 1 - 0.0228 = 0.9772$$

$$P(\text{all three students have not scored more than 75 marks}) = 0.9772 \times 0.9772 \times 0.9772 \\ = 0.93$$

$$\therefore P(\text{at least one of 3 has scored more than 75 marks}) = 1 - 0.93 = 0.07.$$

**Example 3 :** For a normal variate  $X$  with mean 25 and standard deviation 10, find the area between (i)  $X = 25, X = 35$ , (ii)  $X = 15, X = 35$  and also the area such that, (iii)  $X \geq 15$ , (iv)  $X \geq 35$ .

$$\text{Sol. : S.N.V. } Z = \frac{X - m}{\sigma} = \frac{X - 25}{10}$$

(i) When  $X = 25, Z = 0$ , and when  $X = 35, Z = 1$ .

$$\therefore \text{Area (between } X = 25 \text{ and } X = 35) = \text{area (between } Z = 0 \text{ and } Z = 1) \\ = 0.3413.$$

(ii) When  $X = 15, Z = -1$  and when  $X = 35, Z = 1$ .

$$\therefore \text{Area between } (X = 15 \text{ and } X = 35) = \text{area between } (Z = -1 \text{ and } Z = 1) \\ = 2(\text{area between } Z = 0 \text{ and } Z = 1) \\ = 2(0.3413) = 0.6826.$$

(iii) When  $X \geq 15, Z \geq -1$

$$\therefore \text{Area to the right of } (X = 15) \\ = \text{area to the right of } (Z = -1) \\ = (\text{area between } Z = -1 \text{ and } Z = 0) + (\text{area to the right of } Z = 0) \\ = 0.3413 + 0.5 = 0.8413.$$

(iv) When  $X \geq 35, z \geq 1$ .

$$\therefore \text{Area to the right of } (X = 35) \\ = \text{area to the right of } (Z = 1) \\ = (\text{area to the right of } Z = 0) - (\text{area between } Z = 0 \text{ and } Z = 1) \\ = 0.5 - 0.3413 = 0.1587.$$

**Example 4 :** A normal population has mean 0.1 and standard deviation 2.1. Find the probability that the value of the mean of the sample of size 900 drawn from this population will be negative.

(M.U. 2004)

**Sol. :** The mean  $\bar{X}$  of the sample is a S.N.V. We have  $Z = \frac{\bar{X} - \mu}{\sigma/\sqrt{n}}$ .

$$\because \mu = 0.1, \sigma = 2.1, n = 900 \quad \therefore Z < -\frac{0.1}{2.1/\sqrt{900}} = -1.43$$

$$\therefore P(Z < -1.43) = P(Z > 1.43) = 0.5 - (\text{area from } Z = 0 \text{ to } Z = 1.43) \\ = 0.5 - 0.4236 = 0.0764.$$

**Example 5 :** A manufacturer knows from his experience that the resistance of resistors he produces is normal with  $\mu = 100$  ohms and standard deviation  $\sigma = 2$  ohms. What percentage of resistors will have resistance between 98 ohms and 102 ohms?

(M.U. 1996, 10)

**Sol. :** We have S.N.V.  $Z = \frac{X - m}{\sigma} = \frac{X - 100}{2}$

$$\text{When } X = 98, Z = \frac{98 - 100}{2} = -1, \quad \text{When } X = 102, Z = \frac{102 - 100}{2} = 1.$$

$$\therefore P(98 \leq X \leq 102) = P(-1 \leq Z \leq 1) \\ = \text{Area between } (Z = -1 \text{ and } Z = 1)$$

$$\therefore P(98 \leq X \leq 102) = \text{Area from } (Z = -1 \text{ to } Z = 0) + \text{Area from } (Z = 0 \text{ to } Z = 1) \\ = 2 \times \text{Area from } (Z = 0 \text{ to } Z = 1) \\ = 2 \times 0.3413 = 0.6826.$$

$\therefore$  % of resistors having resistance between 98 and 102 = 68.26 %.

### Type III

**Example 1 :** Monthly salary  $X$  in a big organisation is normally distributed with mean ₹ 3000 and standard deviation of ₹ 250. What should be the minimum salary of a worker in this organisation, so that the probability that he belongs to top 5% workers?

(M.U. 2017)

$$\text{Sol. : We have } Z = \frac{X - m}{\sigma} = \frac{X - 3000}{250}.$$

We want to find  $Z_1$  such that

$$P(Z > Z_1) = \frac{5}{100} = 0.05$$

Since  $0.5 - 0.05 = 0.45$ , and corresponding to 0.45 the entry in the area table is 1.64.  $\therefore Z_1 = 1.64$ .

$$\therefore 1.64 = \frac{X - 3000}{250}$$

$$\therefore X = 3000 + 250 \times 1.64 = ₹ 3410.$$

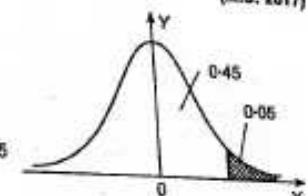


Fig. 7.10 (a)

**Example 2 :** The diameters of can tops produced by a machine are normally distributed with standard deviation of 0.05 cms. At what mean diameter the machine be set so that not more than 5% of the can tops produced by the machine have diameters exceeding 3 cms.?

**Sol. :** Let  $X$  denote the diameter of the can tops.  $X$  is normally distributed with mean  $\mu$  (unknown) and standard deviation  $\sigma = 0.05$ . We are given that

$$P(Z > Z_1) = 0.05$$

Now,  $0.5 - 0.05 = 0.45$  and corresponding to 0.45 the entry in the area table is 1.64.

$$\therefore Z_1 = 1.64$$

$$\therefore Z = \frac{X - m}{\sigma} \text{ gives } 1.64 = \frac{3 - m}{0.05}$$

$$\therefore m = 3 - 1.64 \times 0.05 = 2.984$$

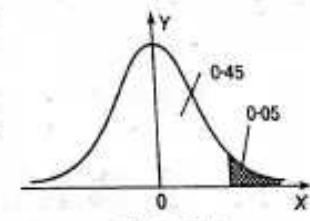


Fig. 7.10 (b)

**Example 3 :** If  $X$  is a normal variate with mean 25 and standard deviation 5, find the value (i) of  $X = x_1$ , such that  $P(X \geq x_1) = 0.32$ , (ii) of  $X = x_2$ , such that  $P(X \leq x_2) = 0.73$ , (iii) of  $X = x_3$  such that  $P(X \leq x_3) = 0.24$ .

**Sol. :** (i) Since 0.32 is less than 0.5. We have to find  $Z = z_1$  corresponding to area = 0.5 - 0.32 = 0.18.

Now, from the table we find that corresponding to  $Z = 0.47$  the area under S.N.V. is 0.18.

$$\therefore Z = \frac{X - m}{\sigma} \text{ gives } 0.47 = \frac{X - 25}{5}$$

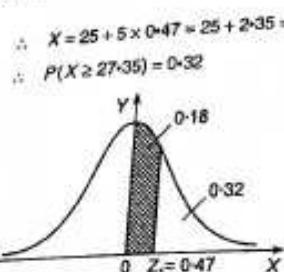


Fig. 7.11 (a)

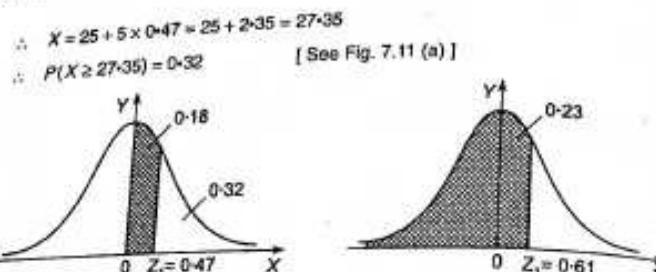


Fig. 7.11 (b)

- (ii) Since 0.73 is greater than 0.5, we have to find  $Z = z_1$  corresponding to area  $0.73 - 0.5 = 0.23$ . Now, from the table we find that corresponding to  $Z = 0.61$  the area under S.N.V. is 0.23.

$$\therefore Z = \frac{X - m}{\sigma} \text{ gives } 0.61 = \frac{X - 25}{5}$$

$$\therefore X = 25 + 5 \times 0.61 = 28.05$$

$$\therefore P(X \leq 28.05) = 0.73 \quad [\text{See Fig. 7.11 (b)}]$$

- (iii) Since 0.24 is less than 0.5, we have to find  $Z = z_1$  corresponding to area  $0.5 - 0.24 = 0.26$ .

Now, from the table, we find that corresponding to  $Z = 0.71$ , the area under the S.N.V. is 0.26.

Since, we want  $X$  less than the desired value, we must take  $Z_1$  on the left hand area i.e.  $Z_1 = -0.71$ .

$$\therefore Z = \frac{X - m}{\sigma} \text{ gives } -0.71 = \frac{X - 25}{5}$$

$$\therefore X = 25 - 5 \times 0.71 = 25 - 3.55 = 21.45$$

$$\therefore P(X \leq 21.45) = 0.24. \quad [\text{See Fig. 7.11 (c)}]$$

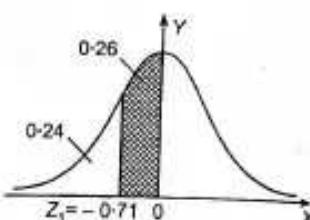


Fig. 7.11 (c)

**Example 4 :** The marks obtained by 1000 students in an examination are found to be normally distributed with mean 70 and standard deviation 5. Estimate the number of students whose marks will be (i) between 60 and 75, (ii) more than 75.

(M.U. 2003, 16)

$$\text{Sol. : We have S.N.V. } Z = \frac{X - m}{\sigma} = \frac{X - 70}{5}$$

$$(i) \text{ When } X = 60, Z = \frac{60 - 70}{5} = -2;$$

$$\text{When } X = 75, Z = \frac{75 - 70}{5} = 1.$$

$$P(60 \leq X \leq 75) = P(-2 < Z < 1)$$

= Area between ( $Z = -2$  and  $Z = 1$ )

= Area from ( $Z = 0$  to  $Z = 2$ ) + area from ( $Z = 0$  to  $Z = 1$ )

$$= 0.4772 + 0.3413 = 0.8185$$

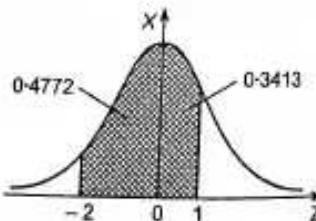


Fig. 7.12

(i) Number of students getting marks between 60 and 75  
=  $Np = 1000 \times 0.8185 = 818$

$$(ii) P(X \geq 75) = P(Z \geq 1)$$

Area to the right of  $Z = 1$   
=  $0.5 - (\text{area between } Z = 0 \text{ and } Z = 1)$   
=  $0.5 - 0.3413 = 0.1587$

Number of students getting more than 75 marks  
=  $Np = 1000 \times 0.1587 = 159$

**Example 5 :** In an intelligence test administered to 1000 students, the average was 42 and standard deviation was 24. Find the number of students (i) exceeding the score 50 and (ii) between 30 and 54.

$$\text{Sol. : We have S.N.V. } Z = \frac{X - m}{\sigma}$$

By data,  $m = 42$  and  $\sigma = 24$ .

$$\therefore Z = \frac{X - 42}{24}$$

$$(i) \text{ When } X = 50, Z = \frac{50 - 42}{24} = \frac{8}{24} = 0.33$$

$$P(Z \geq 50) = \text{area to the right of } 0.33  
= 0.5 - (\text{area between } Z = 0 \text{ and } Z = 0.33)  
= 0.5 - 0.1293 = 0.3707$$

(ii) When  $X = 30$  and  $X = 54$ , we get

$$Z = \frac{30 - 42}{24} = -0.5 \quad \text{and} \quad Z = \frac{54 - 42}{24} = 0.5$$

$$P(30 \leq Z \leq 54) = \text{area between } Z = -0.5 \text{ to } Z = 0.5  
= 2(\text{area between } Z = 0 \text{ and } Z = 0.5)  
= 2(0.1915) = 0.3830$$

Number of students getting more than 50 marks

$$= Np = 1000 \times 0.3707 = 371$$

Number of students getting marks between 30 and 54

$$= Np = 1000 \times 0.3830 = 383$$

**Type IV**

**Example 1 :** If  $X_1$  and  $X_2$  are two independent random variates with means 30 and 25 and variances 16 and 12 and if  $Y = 3X_1 - 2X_2$ , find  $P(60 \leq Y \leq 80)$ .

(M.U. 2005)

**Sol. :** Since  $X_1, X_2$  are independent normal variates with means 30 and 25 and variances 16 and 12,  $Y = 3X_1 - 2X_2$  is also a normal variate with mean

$$m = a_1 \bar{X}_1 + a_2 \bar{X}_2 = 3(30) + (-2)(25) = 90 - 50 = 40.$$

and variance  $\sigma^2 = a_1^2 \sigma_1^2 + a_2^2 \sigma_2^2 = 9(16) + 4(12) = 192$ .

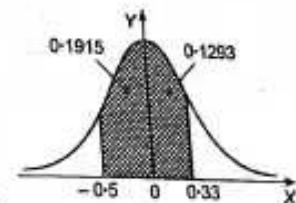


Fig. 7.13

$$\text{S.N.V. } Z = \frac{Y - m}{\sigma} = \frac{Y - 40}{\sqrt{192}}$$

$$\text{When } Y = 60, \quad Z = \frac{20}{\sqrt{192}} = 1.44$$

$$\text{When } Y = 80, \quad Z = \frac{40}{\sqrt{192}} = 2.89$$

$$\begin{aligned} \therefore P(60 \leq Y \leq 80) &= P(1.44 \leq Z \leq 2.89) \\ &= \text{area between } Z = 1.44 \text{ and } Z = 2.89 \\ &= (\text{area from } Z = 0 \text{ to } Z = 2.89) - (\text{area from } Z = 0 \text{ to } Z = 1.44) \\ &= 0.4981 - 0.4251 = 0.0730. \end{aligned}$$

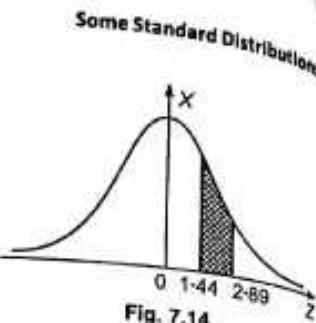


Fig. 7.14

**Example 2 :** Two independent random variates  $X$  and  $Y$  are distributed normally with mean pair of values of  $X$  and  $Y$  will differ by 1.7 or more.

**Sol. :** If  $U = X - Y$  then by the additive property of normal variates,  $U$  is a normal variate with mean  $= 52 - 50 = 2$  and standard deviation  $\sqrt{9 + 4} = \sqrt{13}$  i.e.  $N(2, \sqrt{13})$ . [ See (4), page 7-43 ]

$$\therefore Z = \frac{U - m}{\sigma} = \frac{U - 2}{\sqrt{13}} \text{ is a S.N.V.}$$

Now,  $P(X \text{ and } Y \text{ will differ by 1.7 or more})$

$$\begin{aligned} &= P(|X - Y| \geq 1.7) \\ &= P(|U| \geq 1.7) = 1 - P(|U| \leq 1.7) \\ &= 1 - P(-1.7 \leq U \leq 1.7) \end{aligned}$$

$$\text{Now, when } U = -1.7, \quad Z = \frac{-1.7 - 2}{\sqrt{13}} = -1.03$$

$$\text{and when } U = 1.7, \quad Z = \frac{1.7 - 2}{\sqrt{13}} = 0.08$$

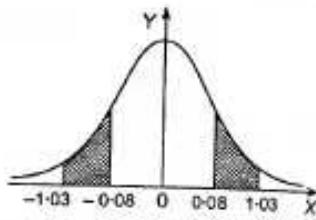


Fig. 7.15

$$\begin{aligned} \therefore P(X \text{ and } Y \text{ will differ by 1.7 or more}) &= 1 - P(-1.03 \leq Z \leq 0.08) \\ &= 1 - (\text{area from } Z = 0.08 \text{ to } Z = 1.03) \\ &= 1 - [(\text{area from } Z = 0 \text{ to } Z = 1.03) - (\text{area from } Z = 0 \text{ to } Z = 0.08)] \\ &= 1 - (0.3485 - 0.0319) = 1 - 0.3766 \\ &= 0.6234 \end{aligned}$$

**Example 3 :** If  $X$  and  $Y$  are two independent random variates  $N(3, 4)$  and  $N(8, 5)$ , find the probability that a point  $(X, Y)$  will lie between the lines  $5X + 3Y = 8$  and  $5X + 3Y = 15$ .

**Sol. :** Since  $X$  is  $N(3, 4)$  and  $Y$  is  $N(8, 5)$  by additive property of normal distribution  $U = 5X + 3Y$  follows a normal distribution with mean

$$m = 5 \times 3 + 3 \times 8 = 39 \quad \text{and} \quad \sigma = \sqrt{25 \times 16 + 9 \times 25} = 25.$$

$$P(\text{the point } (X, Y) \text{ lies between the lines } 5X + 3Y = 8 \text{ and } 5X + 3Y = 15) = P(8 \leq U \leq 15)$$

$$\text{Now, } Z = \frac{U - 39}{25} \text{ is a S.N.V.}$$

$$\text{When } U = 8, \quad Z = \frac{8 - 39}{25} = -1.24$$

$$\text{and when } U = 15, \quad Z = \frac{15 - 39}{25} = -0.96$$

$\therefore P(\text{the point lies between the two lines})$

$$= \text{area between } Z = -0.96 \text{ and } Z = -1.24$$

$$= \text{area between } Z = 0.96 \text{ and } Z = 1.24$$

$$= (\text{area from } z = 0 \text{ to } z = 1.24) - (\text{area from } z = 0 \text{ to } z = 0.96)$$

$$= 0.3925 - 0.3315$$

$$= 0.061$$

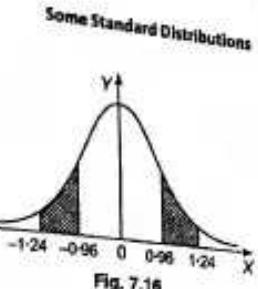


Fig. 7.16

**Example 4 :** If  $X$  and  $Y$  are two independent normal random variates such that their means are 8, 12 and standard deviations are 2 and  $4\sqrt{3}$  respectively, find the value  $\alpha$  such that  $P(2X - Y \leq 2\alpha) = P((X + 2Y) \geq 3\alpha)$ .

**Sol. :** By additive property of normal distribution  $U = 2X - Y$  is a normal variate with mean,  $m = 2 \times 8 - 1 \times 12 = 4$

and standard deviation,  $\sigma = \sqrt{2^2 \times 2^2 + 1^2 \times (4\sqrt{3})^2} = \sqrt{16 + 48} = 8$

$\therefore U$  is a S.N.V. with mean 4 and S.D. = 8.

$V = X + 2Y$  is a normal variate with mean  $m = 1 \times 8 + 2 \times 12 = 32$  and standard deviation

$$\sigma = \sqrt{1^2 \times 2^2 + 2^2 \times (4\sqrt{3})^2} = \sqrt{4 + 192} = 14$$

$\therefore V$  is a S.N.V. with mean 32 and S.D. = 14.

Now,  $P(2X - Y \leq 2\alpha) = P((X + 2Y) \geq 3\alpha)$

$$\therefore P(U \leq 2\alpha) = P(V \geq 3\alpha)$$

$$\therefore P\left(\frac{U - 4}{8} \leq \frac{2\alpha - 4}{8}\right) = P\left(\frac{V - 32}{14} \geq \frac{3\alpha - 32}{14}\right)$$

This means if  $Z$  is a S.N.V.

$$P\left(Z \leq \frac{2\alpha - 4}{8}\right) = P\left(Z \geq \frac{3\alpha - 32}{14}\right)$$

By symmetry of normal distribution if  $P(Z \geq z_1) = \alpha$  then  $P(Z \leq -z_1) = \alpha$ .

$$\therefore P\left(Z \leq \frac{2\alpha - 4}{8}\right) = P\left(Z \leq -\left(\frac{3\alpha - 32}{14}\right)\right)$$

$$\therefore \frac{2\alpha - 4}{8} = -\frac{(3\alpha - 32)}{14}$$

$$\therefore \frac{\alpha - 2}{4} = -\frac{3\alpha - 32}{14}$$

$$\therefore 14\alpha - 28 = -12\alpha + 128$$

$$\therefore 26\alpha = 156$$

$$\therefore \alpha = 6.$$

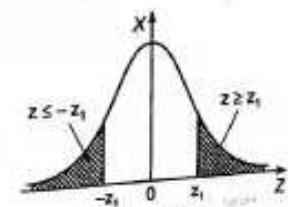


Fig. 7.17

**Example 5 :** In an examination marks obtained by students in Mathematics, Physics and Chemistry are normally distributed with means 51, 53 and 46 with standard deviation 15, 12, 16 respectively. Find the probability of securing total marks (i) 180 or above, (ii) 80 or below.

(M.U. 2005, 10)

Sol. : Let  $X_1, X_2, X_3$  denote the marks obtained in the three subjects. Then  $X_1, X_2, X_3$  are normal variates with mean 51, 53, 46 and variance  $15^2, 12^2, 16^2$ .

Assuming the variates to be independent,  $Y = X_1 + X_2 + X_3$  is distributed normally with mean  $m = 51 + 53 + 46 = 150$  and  $\sigma^2 = 15^2 + 12^2 + 16^2 = 625 = 25^2$ .

$$\therefore S.N.V. Z = \frac{Y - m}{\sigma} = \frac{Y - 150}{25}$$

$$\text{When } Y = 180, Z = \frac{180 - 150}{25} = \frac{30}{25} = 1.2.$$

$$\therefore P(Y \geq 180) = P(Z \geq 1.2)$$

$$\begin{aligned} &= \text{Area to the right of } Z = 1.2 \\ &= 0.5 - (\text{area between } Z = 0 \text{ and } Z = 1.2) \\ &= 0.5 - 0.3849 = 0.1151. \end{aligned}$$

$$\text{When } Y = 80, Z = \frac{80 - 150}{25} = \frac{-70}{25} = -2.4.$$

$$\therefore P(Y \leq 80) = P(Z \leq -2.4)$$

$$\begin{aligned} &= \text{Area to the left of } Z = -2.4 \\ &= 0.5 - \text{area from } Z = 0 \text{ to } Z = -2.4 \\ &= 0.5 - 0.4918 = 0.0082. \end{aligned}$$

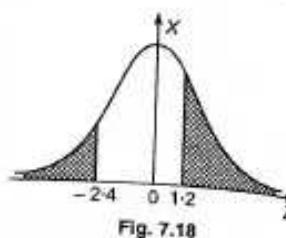


Fig. 7.18

## Type V

**Example 1 :** The incomes of a group of 10,000 persons were found to be normally distributed with mean ₹ 520 and standard deviation ₹ 60. Find (i) the number of persons having incomes between ₹ 400 and 550, (ii) the lowest income of the richest 500.

$$\text{Sol. : S.N.V. } Z = \frac{X - m}{\sigma} = \frac{X - 520}{60}$$

$$(i) \text{ When } X = 400, Z = \frac{400 - 520}{60} = -2. \text{ When } X = 550, Z = \frac{550 - 520}{60} = 0.5$$

$$\therefore P(400 \leq X \leq 550) = \text{Area (from } z = -2 \text{ to } z = 0.5\text{)}$$

But, area (from  $z = -2$  to  $z = 0$ )

$$\begin{aligned} &= \text{Area (from } z = 0 \text{ to } z = 2\text{)} \\ &= 0.4772. \end{aligned}$$

And area (from  $z = 0$  to  $z = 0.5$ ) = 0.1915.

$$\therefore P(400 \leq X \leq 550) = \text{Area (from } z = -2 \text{ to } z = 0.5\text{)} \\ = 0.4772 + 0.1915 = 0.6687.$$

$\therefore$  The number of persons whose incomes are between ₹ 400 and ₹ 550 =  $Np = 10,000 \times 0.6687 = 6687$ .

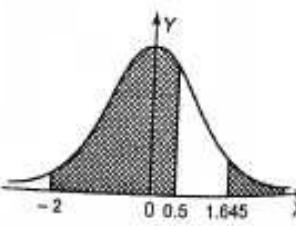


Fig. 7.19

(ii) If we have to consider the richest 500 persons then the probability that a person selected at random will be one of them

$$= \frac{500}{10,000} = 0.05$$

This is a reverse problem. So far we have found the probability for a given value of  $Z$ . Here, we have to find the value of  $Z$  for a given probability. We have to find the value of  $Z$  to the right of which the area is 0.05. But area to the right of  $Z = 0$  is 0.5.

$$\therefore \text{Area from } (Z = 0 \text{ to } Z = \text{this value}) = 0.5 - 0.05 = 0.45$$

From the table we find that the area from  $Z = 0$  to  $Z = 1.645$  is 0.45

$$\therefore \text{The required value of } Z = 1.645$$

$$\text{But } Z = \frac{X - 520}{60} \quad \therefore 1.645 = \frac{X - 520}{60}$$

$$\therefore X - 520 = 60 \times 1.645 \quad \therefore X = 520 + 98.7 = ₹ 618.7.$$

$\therefore$  The lowest income of the richest 500 is ₹ 618.7.

**Example 2 :** The income of a group of 10,000 persons was found to be normally distributed with mean of ₹ 750 and standard deviation of ₹ 50. What is the lowest income of richest 250?

$$\text{Sol. : S.N.V. } Z = \frac{X - m}{\sigma} = \frac{X - 750}{50}$$

If we have to consider the richest 250 persons then the probability that a person selected at random will be one of them is  $= \frac{250}{10,000} = 0.025$ .

This again is a reverse problem. So far we have found the probability for a given value of  $Z$ . Here, we have to find the value of  $Z$  for a given probability. We have to find the value of  $Z$  to the right of which the area is 0.025. But the area to the right of  $Z = 0$  is 0.5.

$$\therefore \text{Area from } (Z = 0 \text{ to } Z = \text{this value}) = 0.5 - 0.025 = 0.475$$

From the table we find that the area from  $Z = 0$  to  $Z = 1.96$  is 0.475.

$$\therefore \text{The required value of } Z = 1.96$$

$$\text{When } Z = 1.96, 1.96 = \frac{X - 750}{50}$$

$$\therefore X - 750 = 1.96 \times 50 \quad \therefore X = 848$$

$\therefore$  The lowest income of richest 250 persons = ₹ 848.

**Example 3 :** In a competitive examination the top 15% of the students appeared will get grade A, while the bottom 20% will be declared fail. If the grades are normally distributed with mean % of marks 75 and S.D. 10, determine the lowest % of marks to receive grade A and the lowest % of marks that passes.

(M.U. 2014)

Sol. : This is a reverse problem as above.

$$\text{We have } Z = \frac{X - m}{\sigma} = \frac{X - 75}{10}$$

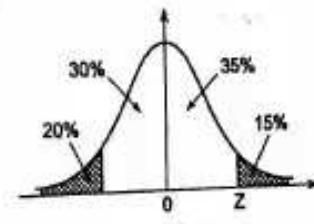


Fig. 7.20

- (i) Grade A is given for 15%. We have to find the value of  $Z$  to the right of which the area is 0.15.  
 But the area to the right of  $Z = 0$  is 0.5.  
 $\therefore$  Area from ( $Z = 0$  to  $Z = \text{this value}$ ) =  $0.5 - 0.15 = 0.35$ .  
 From the table, we find that the area between  $Z = 0$  to  $Z = 1.04$  is 0.35.  
 $\therefore$  The required value of  $Z = 1.04$ .  
 But  $Z = \frac{X - 75}{10} \therefore 1.04 = \frac{X - 75}{10} \therefore X = 75 + 10 \cdot 4 = 85.4$
- (ii) Lowest 20% students are declared fail. We have to find the value of  $Z$  to the left of which the area is 0.20. But the area to the left of  $Z = 0$  is 0.5.  
 $\therefore$  Area from ( $Z = 0$  to  $Z = \text{this value}$ ) =  $0.5 - 0.2 = 0.3$ .  
 From the table we find that the area between  $Z = 0$  and  $Z = 0.84$  is 0.3.  
 But this ordinate is on the left and hence negative.  
 $\therefore$  The required value of  $Z = -0.84$ .  
 But  $Z = \frac{X - 75}{10} \therefore -0.84 = \frac{X - 75}{10} \therefore X = 75 - 8.4 = 66.6$ .

**Example 4 :** If the actual amount of coffee which a filling machine puts into 6 ounce jars is a random variable having normal distribution with standard deviation 0.05 ounce and if only 3% of the jars are to contain less than 6 ounce of coffee what must be the mean fill of these jars ?

$$\text{Sol. : Let } Z = \frac{X - m}{\sigma}$$

$$\text{We have } \sigma = 0.05, X = 6 \therefore Z = \frac{6 - m}{0.05}$$

We want  $Z$  such that

$$P(Z \leq 3) = P\left(\frac{6 - m}{0.05}\right) = 0.03$$

From the table for area to be 0.47

$$z_1 = 1.808 \quad \therefore z_2 = -1.808$$

$$\therefore \frac{6 - m}{0.05} = -1.808$$

$$\therefore m = 6 + 0.05 \times 1.808 = 6.09 \text{ ounce.}$$

#### Type VI

**Example 1 :** Find the mean and the standard deviation of a normal distribution of marks in an examination where 58 % of the candidates obtained marks below 75, 4 % got above 80 and the rest  $z = \pm 1.8$  is 92%.

**Sol. :** Let  $m$  and  $\sigma$  be the mean and the standard deviation of the variate.

Since 58 % students are below 75,  $58 - 50 = 8$  % students are between 75 and  $m$ .

Since 4 % students are above 80,  $50 - 4 = 46$  % students are between  $m$  and 80.

We are given that area between  $Z = \pm 0.2$  is 0.16 and that between  $Z = \pm 1.8$  is 9.2%.

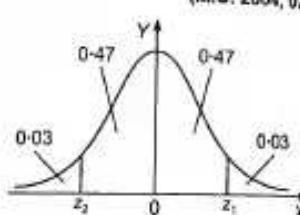


Fig. 7.21

Hence, the area between  $Z = 0$  and  $Z = 0.2$  is  $\frac{0.16}{2} = 0.08$  and that between  $Z = 0$  and  $Z = 1.8$  is  $\frac{0.92}{2} = 0.46$ .  
 In other words for area 0.08 (8 %),  $Z = 0.2$  and for area 0.46 (46 %),  $Z = 1.8$ .  
 $\therefore \frac{75 - m}{\sigma} = 0.2$  and  $\frac{80 - m}{\sigma} = 1.8$   
 $\therefore 75 - m = 0.2 \sigma$  and  $80 - m = 1.8 \sigma$   
 $\therefore 75 - m = -1.6 \sigma \therefore \sigma = \frac{5}{1.6} = 3.125$   
 Subtracting 5  $\therefore m = 75 - 3.125 \times 0.2 = 74.4$  mark.

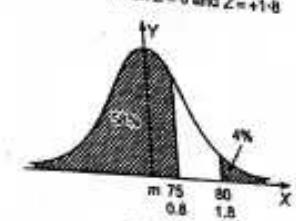


Fig. 7.22

**Example 2 :** Marks obtained by students in an examination follow normal distribution. If 30% of students got below 35 marks and 10% got above 60 marks, find the mean and standard deviation. (M.U. 2016)

**Sol. :** Let  $m$  and  $\sigma$  be the mean and the standard deviation of the distribution.

Since 30% students are below 35, 20% students are between 35 and  $m$ .

Since 10% students are above 60, 40% students are between  $m$  and 60.

From the table we find that,

0.2 area corresponds to  $Z = 0.525$

and 0.4 area corresponds to  $Z = 1.283$

But 0.2 area is to the left of  $m$  hence  $Z = -0.525$ .

$$\therefore \frac{35 - m}{\sigma} = -0.525; \quad \frac{60 - m}{\sigma} = 1.283$$

$$\therefore 35 - m = -0.525 \sigma$$

$$\therefore 60 - m = 1.283 \sigma$$

..... (1)

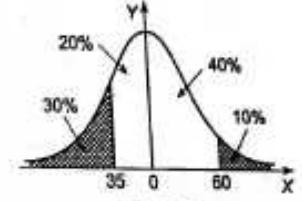


Fig. 7.23

$$\text{By subtraction, we get } 25 = 1.808 \sigma \therefore \sigma = \frac{25}{1.808} = 13.83.$$

Putting this value of  $\sigma$  in (1), we get

$$35 - m = -0.525 (13.83)$$

$$\therefore m = 35 + 0.525 (13.83) = 42.26$$

Hence, mean = 42.26 and standard deviation,  $\sigma = 13.83$ .

**Example 3 :** In a distribution exactly normal 7 % of items are under 35 and 89 % are under 63. What are the mean and standard deviation ? (M.U. 2004)

**Sol. :** Since 7 % items are below 35,  $50 - 7 = 43$  % items are between 35 and  $m$ , and since 89 % items are below 63,  $89 - 50 = 39$  % items are between  $m$  and 63.

For area 0.43,  $Z = 1.48$ .

Since  $35 < m$ ,  $Z = -1.48$  and for area 0.39,  $Z = 1.23$ .

$$\begin{aligned} \therefore \frac{35-m}{\sigma} &= -1.48 \text{ and } \frac{63-m}{\sigma} = 1.23 \\ \therefore 35-m &= -1.48\sigma \\ \text{and } 63-m &= 1.23\sigma \\ \text{Subtracting } 28 &= 2.71\sigma \\ \therefore \sigma &= \frac{28}{2.71} = 10.33 \\ \therefore m &= 35 + 1.48\sigma = 35 + 1.48 \times 10.33 \\ &= 35 + 15.3 = 50.3. \end{aligned}$$

**Example 4 :** In a distribution exactly normal 7% of items are under 35 and 89 % of the items are under 63. Find the probability that an item selected at random lies between 45 and 56.

**Sol. :** As in the above example  $m = 50.3$  and  $\sigma = 10.33$ .

$$\text{Now, } Z = \frac{X-m}{\sigma} = \frac{X-50.3}{10.33}$$

$$\text{When } X = 45, Z = \frac{45-50.3}{10.33} = -0.51$$

$$\text{When } X = 56, Z = \frac{56-50.3}{10.33} = 0.55$$

$$\therefore P(45 \leq X \leq 56) = P(-0.51 \leq Z \leq 0.55)$$

= area between  $(Z = -0.51 \text{ to } Z = 0.55)$

= area from 0 to 0.51 + area from 0 to 0.55

$$= 0.1950 + 0.2088 = 0.4038$$

**Example 5 :** A large number of automobile batteries have average life of 24 months. If 34 percent of them average between 22 and 26 months and 272 of them last longer than 29 months how many were in the group tested? Assume the distribution to be normal. (For a normal curve 17 % and 36.4 % values lie between the mean and respective distance of 0.44 and 1.1 times standard deviation from the mean).

**Sol. :** Because of symmetry of the normal distribution and because  $m = 24$ , the area between 22 and 24 is equal to that between 24 and 26. This area is equal to  $34/2 = 17\%$  which corresponds to S.N.V.  $Z = 0.44$  by data and  $X = 26$ .

$$\therefore \frac{26-24}{\sigma} = 0.44 \quad \therefore \sigma = \frac{2}{0.44} = \frac{50}{11}$$

$$\text{Now when } X = 29, Z = \frac{X-m}{\sigma} = \frac{29-24}{50/11} = \frac{11}{10} = 1.1.$$

By data area between  $Z = 0$  and  $Z = 1.1$  is 0.364.

$\therefore$  The area to the right of  $Z = 1.1$  i.e.  $X = 29$  is  $= 0.5 - 0.364 = 0.136$  which is the probability that a battery will last longer than 29 months.

$$\text{But } p = \frac{f}{N} \text{ and } f = 272, p = 0.136. \quad \therefore N = \frac{f}{p} = \frac{272}{0.136} = 2000$$

Hence, 2000 batteries were tested.

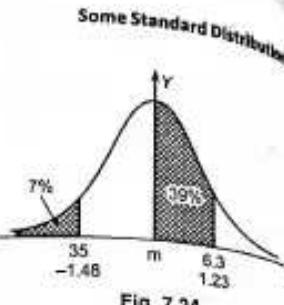


Fig. 7.24

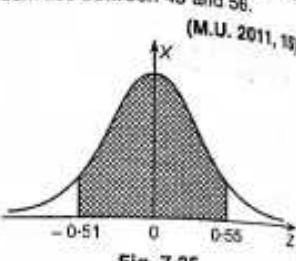


Fig. 7.25

## Type VII

**Example 1 :** The probability that an electronic component will fail in less than 1200 hours of continuous use is 0.25. Using normal approximation to Binomial distribution, find the probability that among 200 such components fewer than 45 will fail in less than 1200 hours of continuous use. (M.U. 2005)

**Sol. :** While using continuous variate in place of discrete variate we must "spread" its values over a continuous scale. This we do by taking each integer  $k$  to represent the interval  $k - (1/2)$  to  $k + (1/2)$ . Now, we have  $n = 200, p = 0.25, q = 0.75$ .

$$\begin{aligned} \therefore m &= np = 200 \times 0.25 = 50 \\ \sigma &= \sqrt{npq} = \sqrt{200 \times 0.25 \times 0.75} = 6.12 \\ Z &= \frac{X-np}{\sqrt{npq}} = \frac{X-50}{6.12} \end{aligned}$$

When  $X = 44.5$  (i.e.  $k - (1/2)$ )

$$Z = \frac{44.5-50}{6.12} = -0.9886 = -0.9$$

For  $Z = 0.9, p = 0.3159$ .

$$\therefore P(X \leq 44.5) = P(Z \leq -0.9) = 0.5 - 0.3159 = 0.1841.$$

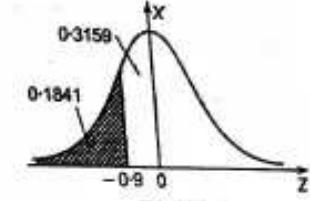


Fig. 7.26

**Example 2 :** Determine in two different ways, the probability that by guess-work a student can correctly answer 25 to 30 questions in a multiple choice quiz consisting of 80 questions. Assume that in each question with four choices only one is correct and the student has no knowledge. (M.U. 2004)

**Sol. :** (a) By using Normal approximation to Binomial Distribution

$$\text{Mean} = m = np = 80 \times (1/4) = 20$$

$$\text{S.D., } \sigma = \sqrt{npq} = \sqrt{80 \times \frac{1}{4} \times \frac{3}{4}} = 3.873$$

$$\therefore Z = \frac{X-m}{\sigma} = \frac{X-20}{3.873}$$

Since from discrete (Binomial Distribution) we are approximating to continuous (Normal distribution) we extend the range 25 to 30 by half units on either side i.e. we take the range as 24.5 to 30.5.

$$\text{When } X = 24.5, Z = \frac{24.5-20}{3.873} = 1.16. \quad \text{When } X = 30.5, Z = \frac{30.5-20}{3.873} = 2.71$$

$$\therefore P(24.5 \leq X \leq 30.5) = P(1.16 \leq Z \leq 2.71) = (\text{area from } Z = 0 \text{ to } Z = 2.71) - (\text{area from } Z = 0 \text{ to } Z = 1.16) = 0.4966 - 0.6770 = 0.1196$$

(b) By using Binomial Distribution

$$\text{We have } p = \frac{1}{4}, q = \frac{3}{4}, n = 80$$

**Applied Mathematics - IV**

(7-63)

**Some Standard Distributions**

$$\begin{aligned} P(X=x) &= {}^n C_x p^x q^{n-x} = {}^{80} C_x \left(\frac{1}{4}\right)^x \left(\frac{3}{4}\right)^{80-x} \\ \therefore \text{The required probability} &= \sum_{x=25}^{30} {}^{80} C_x \left(\frac{1}{4}\right)^x \left(\frac{3}{4}\right)^{80-x} \\ &= 0.0434 + 0.0306 + 0.0204 + 0.0129 + 0.0077 + 0.0043 \\ &= 0.1193 \end{aligned}$$

(Note that the two values differ only by 0.0003.)

**Example 3:** Using normal distribution, find the probability of getting 55 heads in the toss of 100 fair coins. (Compare the result with that obtained from Binomial distribution). (M.U. 2004)

Sol.: Since the coins are fair, we have  $p = 1/2$ ,  $q = 1/2$ . By data  $n = 100$ .

$$\therefore m = np = 100 \times \frac{1}{2} = 50, \quad \sigma = \sqrt{npq} = \sqrt{100 \times \frac{1}{2} \times \frac{1}{2}} = 5$$

$$\text{Hence, we have S.N.V. } Z = \frac{X - m}{\sigma} = \frac{X - 50}{5}$$

$$\text{When } X = 54.5, \quad Z = \frac{54.5 - 50}{5} = 0.9.$$

$$\text{When } X = 55.5, \quad Z = \frac{55.5 - 50}{5} = 1.1$$

$$\begin{aligned} \therefore P(0.9 < Z < 1.1) &= \text{area from } Z = 0.9 \text{ to } Z = 1.1 \\ &= (\text{area from } Z = 0 \text{ to } Z = 1.1) - (\text{area from } Z = 0 \text{ to } 0.9) \\ &= 0.3643 - 0.3159 = 0.0484 \end{aligned}$$

Now, for the second part, we have

$$P(X=x) = {}^n C_x p^x q^{n-x} = {}^{100} C_x \left(\frac{1}{2}\right)^x \left(\frac{1}{2}\right)^{100-x}$$

$$\therefore P(X=55) = {}^{100} C_{55} \left(\frac{1}{2}\right)^{55} \left(\frac{1}{2}\right)^{45} = 0.04847$$

**EXERCISE - III**
**Type I**

1. Find  $k$  and the mean and standard deviation of the normal distribution given by

$$(i) y = k e^{-\frac{x^2 - x + 9}{18}}$$

$$[ \text{Ans. : } k = \frac{1}{3\sqrt{2\pi}}, \quad m = 9, \quad \sigma = 3 ]$$

$$(ii) y = k e^{-\frac{x^2 - x + 3}{6}}$$

$$[ \text{Ans. : } k = \frac{1}{\sqrt{6\pi}}, \quad m = 3, \quad \sigma = \sqrt{3} ]$$

2. Write down the equation of the curve of the normal distribution with mean 50 and standard deviation 8. What is the first quartile of the distribution?

3. Write down the equation of the normal curve with mean 10 and variance 36. What is the quartile deviation of the distribution ?

[ Ans. : 4 ]

**Applied Mathematics - IV**

(7-64)

**Some Standard Distributions**

4. What is the Q.D. of a normal distribution with S.D. 9 ?

[ Ans. : 6 ]

**Type II**

1. If  $X$  is normally distributed with mean 10 and standard deviation 2, find  $P(-3 \leq X \leq 12)$ .

[ Ans. : 0.8413 ]

2. If  $X$  is normally distributed with mean 15 and standard deviation 6, find  $P(-3 \leq X \leq 18)$  and  $P(|X| \geq 16.02)$ .

[ Ans. : 0.6902; 0.5675 ]

3. If  $X$  is normally distributed with mean and standard deviation 4, find (i)  $P(5 \leq X \leq 10)$ ,

- (ii)  $P(X \geq 15)$ , (iii)  $P(10 \leq X \leq 15)$ , (iv)  $P(X \leq 5)$ .

[ Ans. : (i) 0.3326, (ii) 0.003, (iii) 0.1557, (iv) 0.05967 ]

4. A normal distribution has mean 5 and standard deviation 3. What is the probability that the deviation from the mean of an item taken at random will be negative ?

[ M.U. 2004 ]

[ Ans. : 0.0575 ]

**Type III**

1. If  $Z$  is a S.N.V., find  $c$  such that (i)  $P(-c < Z < c) = 0.98$ , (ii)  $P(|Z| > c) = 0.04$ .

[ Ans. : (i)  $c = 2.33$ , (ii)  $c = 2.05$  ]

2. If  $X$  is a normal variate with mean 30 and standard deviation 6, find the value of  $X = x_1$  such that  $P(X \geq x_1) = 0.05$ .

[ Ans. :  $x_1 = 1.64, x_1 = 39.84$  ]

3. If  $X$  is a normal variate with mean 25 and standard deviation 5, find the value of  $X = x_1$  such that  $P(X \leq x_1) = 0.01$ .

[ Ans. :  $x_1 = -2.33, x_1 = 13.35$  ]

**Type IV**

1. The first and third quartiles of a normal distribution are respectively 92 and 128. Find the mean and the standard deviation.

[ Ans. : 110, 27 ]

2. For a normal distribution the first quartile is 46 and the variance is 144. Find the (i) mode, (ii) limits of central 50% items, (iii) mean deviation.

[ Ans. : (i) 54, (ii) 46; 62, (iii) 9.6 ]

3. The mean and the standard deviation of a normal distribution are 70 and 15. Find the quartile deviation and mean deviation.

[ Ans. : (i) 10, (ii) 12 ]

**Type V**

1. The weights of 4000 students are found to be normally distributed with mean 50 kgs. and standard deviation 5 kgs. Find the probability that a student selected at random will have weight (i) less than 45 kgs., (ii) between 45 and 60 kgs.

[ Ans. : (i) 0.1587, (ii) 0.8185 ]

2. The sizes of 10,000 items are normally distributed with mean 20 cms and standard deviation 4 cm. Find the probability that an item selected at random will have size between (i) 18 cms and 23 cms, (ii) above 26 cms.

[ Ans. : (i) 0.4649, (ii) 0.0668 ]

3. The daily sales of a firm are normally distributed with mean ₹ 8000 and variance of ₹ 10,000. (i) What is the probability that on a certain day the sales will be less than ₹ 8210 ? (ii) What is % of days on which the sales will be between ₹ 8100 and ₹ 8200 ?

[ M.U. 1999, 2001 ] [ Ans. : (i) 0.5832, (ii) 14% ]

**Type VI**

1. Mean and standard deviation of chest measurements of 1200 soldiers are 85 cms and 5 cms respectively. How many of them are expected to have their chest measurements exceeding 95 cms. assuming the measurements to follow the normal distribution ? (Area for S.N.V.  $z$  from  $z = 0$  to  $z = 2$  is 0.4772)

[ Ans. : 27 ]

2. The height of 22 year old boys is distributed normally with mean 63" and standard deviation 2.5". A boy is eligible if his height is between 62" and 56". Find the expected number of boys out of 180 who will be ineligible because of excess height. (Area for S.N.V.  $z$  from  $z = 0$  to  $z = 0.4$  is 0.1554 and that from  $z = 0$  to  $z = -0.8$  is 0.2861). [Ans. : 38]
3. The mean height of soldiers is 68.22" with variance 10.8". Find the expected number of soldiers in a regiment of 1000 whose height will be more than 6 feet. (Area from  $z = 0$  to  $z = 1.15$  is 0.3749). [M.U. 1997, 2009] [Ans. : 125]
4. The heights of 1000 soldiers in a regiment are distributed normally with mean of 172 cms. and a standard deviation of 5 cms. How many soldiers have height greater than 180 cms? (Area from  $z = 0$  to  $z = 1.6$  is 0.4452). [Ans. : 55]

5. The weights of 1000 students were found to be normally distributed with mean 40 kgs. and standard deviation 4 kgs. Find the expected number of students with weights (i) less than 36 kgs. (ii) more than 45 kgs. [Ans. : (i) 159, (ii) 106]

6. If the heights of 500 students is normally distributed with mean 68 inches and standard deviation 4 inches, estimate the number of students having heights (i) greater than 72 inches, (ii) less than 62 inches, (iii) between 65 and 71 inches. [Ans. : (i) 79, (ii) 33, (iii) 273]

## Type VII

1. The mean I.Q. of a large number of children of age 14 is 100 with S.D. 16. Assuming the distribution of I.Q. to be normal, find the percentage of the children having I.Q. between 70 and 120. (Area for S.N.V.  $z$  from  $z = 0$  to  $z = 1.875$  is 0.4896 and that from  $z = 0$  to  $z = 1.25$  is 0.3944). [Ans. : 86.4 %]

2. A sample of 100 dry battery cells is tested to find the length of life, produced the following results.

$$\bar{x} = 12 \text{ hours}, \sigma = 3 \text{ hrs.}$$

- Assuming normal distribution what percentage of cells is expected to have life (i) more than 15 hours, (ii) between 10 and 14 hours. [M.U. 2007] [Ans. : (i) 15.87%, (ii) 49.72 %]

3. The daily sales of a certain item are normally distributed with mean ₹ 8000 and variance ₹ 10,000. (i) What is the probability that on a certain day the sales will be less than ₹ 8210? (ii) What percentage of the days will the sales be between ₹ 8100 and ₹ 8210?

- (Given : Area for S.N.V.  $z$  from  $z = 0$  to  $z = 2.1$  is 0.4821; that between  $z = 0$  and  $z = 1$  is 0.3413). [Ans. : (i) 0.9821, (ii) 14.08 %]

4. The average selling price of houses in a city is ₹ 50,000 with standard deviation of ₹ 10,000. Assuming the distribution of selling price to be normal find (i) the percentage of houses that sell for more than ₹ 55,000, (ii) the percentage of houses selling between ₹ 45,000 and ₹ 60,000. (Area between  $t = 0$  and  $t = 1$  is 0.3413 and between  $t = 0$  and  $t = 0.5$  is 0.1915).

- [Ans. : (i) 30.85 %, (ii) 53.28 %]

## Type VIII

1. The income distribution of workers in a certain factory was found to be normal with mean of ₹ 500 and standard deviation equal to ₹ 50. There were 228 persons above ₹ 600. How many persons were there in all? (Area under the S.N. curve between height at 0 and 2 is 0.4772).

- [M.U. 2000] [Ans. : 10,000]

2. In a factory a large number of workers have average daily income of ₹ 120. If 38.3% of them have income between ₹ 100-140 and 528 of them get more than ₹ 170, how many workers were interrogated? (Area for S.N.V. between  $z = 0$  and  $z = 1.15$  is 0.5 and that between  $z = 0$  and  $z = 1.25$  is 0.3944). (Hint : Find  $a$ ) [Ans. : 5,000]
3. The arithmetic mean of purchases per day by a customer in a large store is ₹ 25 with a standard deviation of ₹ 10. If on a particular day, 100 customers purchased for ₹ 37.80 or more estimate the total number of customers who purchased from the store that day. (Given that the normal area between  $t = 0$  and  $t = 1.28$  is 0.4000 where  $t$  is the S.N.V.) [Ans. : 1,000]
4. The arithmetic mean of the weights of a group of boys is 105 lbs with standard deviation of 5 lbs. If there were 456 boys having weights more than 115 lbs, how many students were there in the group? (Given : For S.N.V.  $z$  area from  $z = 0$  to  $z = 2$  is 0.4772). [Ans. : 20,000]

## Type IX

1. The heights of 1000 cakes baked with certain mix have a normal distribution with a mean of 5.75 cms. and a standard deviation of 0.75 cms. Find the number of cakes having heights between 5 cms. and 6.25 cms. Also find the maximum height of the flattest 200 cakes.

- (For a standard variate  $t$ , the area between  $t = -1$  and  $t = 1$  is 0.6288, that between  $t = 0$  and  $t = 0.67$  is 0.2486 and that between  $t = 0$  and  $t = 0.84$  is 0.3). [Ans. : 562-9, 5-12]

2. The life of army shoes is normally distributed with mean 8 months and standard deviation 2 months. If 5000 pairs are issued, how many pairs would be expected to need replacement after 12 months? [M.U. 2001] [Ans. : 2386]

3. In an intelligence test administered to 1000 students the average was 42 and standard deviation was 24. Find the number of students (i) exceeding 50, (ii) between 30 and 54, (iii) the least score of top 100 students. [M.U. 2003] [Ans. : (i) 371, (ii) 383, (iii) 72-72]

4. 1000 light bulbs with an average life of 120 days are installed in streets of Mumbai. Their length of life is normally distributed with variance 400 days. (i) How many will expire in less than 90 days? (ii) If it is decided to replace all the bulbs together what interval should be allowed between replacements if not more than 10 percent should expire before replacement?

- (Area between  $z = 0$  and  $z = 1.5$  is 0.4332 and 80% of the area lies between  $z = \pm 1.28$ ). [Ans. : (i) 67, (ii) 94-4]

5. Monthly salaries of 1000 workers have a normal distribution with mean of ₹ 575 and a standard deviation of ₹ 75. Find the number of workers having salaries between ₹ 500 and ₹ 625 p.m. Also find the minimum salary of the highest paid 200 workers.

- (Given : For a standard normal variate  $t$  (i) area between  $t = 0$ ,  $t = 1$  is 0.3413, (ii) area between  $t = 0$  and  $t = 0.67$  is 0.2486, (iii) area between  $t = 0$  and  $t = 0.84$  is 0.3). [Ans. : ₹ 590, ₹ 638]

6. The marks obtained by students in a class are normally distributed with mean 75 and standard deviations. If top 5% got grade A and bottom 25% got grade B, what are the marks of the lowest of A and what are the marks of the highest of B? Also find the percentage of students who got marks between 60 and 70. [M.U. 2004] [Ans. : (i) 83, (ii) 72, (iii) 15.74 %]

## Type X

1. The local authorities in a certain city installed 10,000 electric lamps in the streets of the city. If these lamps have average life of 1000 burning hours with a standard deviation of 200 hours, what number of lamps might be expected to fail (i) in the first 800 hours, (ii) between 800 and 1200 hours? After what period of burning hours would you expect that (i) 10% of the lamps would fail,

(ii) 10% of the lamps would be still burning? (The area between the ordinates corresponding to S.N.V.  $z = 0$  and  $z = 1$  is 0.34134 and 80% of the area lies between the ordinate corresponding to  $z = \pm 1.25$ ).  
 (M.U. 2004) [Ans. : (i) 1587, (ii) 6827, (i) 750 hrs., (ii) 1250 hrs.]

2. The distribution of monthly income of 3000 primary teachers confirms to a normal curve with mean equal to ₹ 600 and standard deviation equal to ₹ 100. Find (i) the percentage of teachers having monthly income of more than ₹ 800, (ii) the number of teachers having monthly income less than ₹ 400, (iii) the highest monthly income among the lowest paid 100 teachers, and (iv) the lowest monthly income of the highest paid 100 teachers. (For a S.N.V.  $t$  = the area under the curve between  $t = 0$  and  $t = \pm 2$  is 0.4772 and that between  $t = \pm 1.83$  is 0.4667).  
 [Ans. : (i) 2.28%, (ii) 68.4, (iii) ₹ 417, (iv) ₹ 783]

3. In an examination the arithmetic mean of marks scored by 10,000 students is 50 and the standard deviation is 15. Assuming the distribution to be normal find (i) the number of students who scored more than 65 marks, (ii) the number of students who scored marks between 35 and 65, (iii) the limits between which the marks of the middle 50% students lie.

(For a standard normal variate the area under the curve between  $t = 0$  and  $t = 1$  is 0.3413).  
 [Ans. : (i) 1587, (ii) 6826, (iii) 40-60]

4. In a test of 2000 electric bulbs, it was found that the life of a particular make was normally distributed with an average of life of 2040 hours and standard deviation of 60 hours.

Estimate the number of bulbs likely to burn for (i) more than 2150 hours, (ii) less than 1950 hours.  
 (M.U. 2004) [Ans. : (i) 67, (ii) 184]

5. Assuming that the diameters of 1000 brass plugs taken consecutively from a Normal distribution with mean 0.7515 cm. and standard deviation 0.0020 cm. how many plugs are likely to be rejected if the approved diameter is  $0.752 \pm 0.004$  cms?  
 (M.U. 2003, 05) [Ans. : 53]

#### Type XI

1. If  $X$  is normally distributed with unknown mean and standard deviation  $\sigma = 4$ . Find the mean if (i) not more than 6% values of  $X$  are to exceed 30. (ii) not more than 5% values of  $X$  are to be less than 20.  
 [Ans. : (i) 23.8, (ii) 26.56]

2. The quantity filled in small medicine bottles is normally distributed with standard deviation of 0.04 c.c. If less than 2% of the bottles are to contain less than 4 c.c. medicine, find the mean quantity to which the machine be set up.  
 [Ans. :  $z_1 = -2.05, m = 4.082$ ]

3. The qualifying marks for a certain examination are 35 and to secure distinction one has to score more than 74. If 25% of the students fail, whereas 6.681% obtained distinction, determine the mean and the standard deviation assuming that the distribution of marks is normal. (Semi-interquartile range in a normal distribution is two-third of standard deviation and in a normal distribution 43.319% items lie between the mean and 1.5 times the standard deviation from the mean).  
 [Ans. :  $m = 47, \sigma = 18$ ]

4. In a large institution 2.28% employees receive income below ₹ 4500 and 15.87% employees receive income above ₹ 7500.

Assuming the income to be normally distributed, find the mean and the S.D. (M.U. 2006)

[Ans. :  $m = 6500, \sigma = 1000$ ]  
 5. In a normal distribution 31% items are under 45 and 8% are over 64. Find the mean and standard deviation. Find also the percentage of items lying between 30 and 75.  
 (Given : For S.N.V.  $Z$  area from  $Z = 0$  to  $Z = 0.5$  is 0.19 and that from  $Z = 0$  to  $Z = 1.4$  is 0.42).  
 (M.U. 1995, 98, 2003, 04) [Ans. :  $m = 50, \sigma = 10 ; 0.957$ ]

6. Of a large group of men 5% are under 60 inches in height and 40% are between 60 and 65 inches. Assuming a normal distribution, find the mean and standard deviation of the distribution.  
 (M.U. 2004) [Ans. :  $\mu = 65.43, \sigma = 3.29$ ]

7. The distribution of marks in a certain examination was found to be normal with 23% of the candidates scoring above 60 marks and 21% candidates scoring below 40. Find the mean and standard deviation of the distribution.  
 (Given : For S.N.V.  $Z$  area from  $Z = 0$  to  $Z = 0.74$  is 0.27 and area from  $Z = 0$  to  $Z = 0.81$  is 0.29).  
 (M.U. 1999) [Ans. :  $m = 50$  nearly and  $\sigma = 13$  nearly]

8. For a normal distribution 30% items are below 45 and 8% items are above 64. Find the mean and variance of the normal distribution.  
 (M.U. 1998, 2001, 05) [Ans. :  $m = 50, \sigma = 10$ ]

9. Of a large group of men 5% are under 60 inches in height and 40% are between 60 and 65 inches in height. Assuming the distribution to be normal, find the mean and variance.  
 (M.U. 1998) [Ans. :  $m = 65.42, \sigma = 3.29$ ]

10. Marks obtained by students in an examination follow a normal distribution. If 30% of students got below 35 marks and 10% got above 60 marks find the mean and the % of students who got marks between 40 and 50.  
 (M.U. 2003) [Ans. :  $m = 42.25, \sigma = 13.81, 28\%$ ]

#### Type XII

1. The mean and standard deviation (s.d.) of marks obtained by students in Mathematics and Physics are given below.

	Mean	S.D.
Maths	50	10
Physics	55	12

Assuming the marks in the two subjects to be independent normal variates obtain the probability that a student scores marks between 100 and 130 marks in the two subjects taken together.

[Ans. : 0.5707]

2. In an examination marks obtained by students in Mathematics, Physics and Chemistry are distributed normally about means 40, 46, 44 with standard deviations 13, 11, 10 respectively. Find the probability of a student securing total marks (i) 180 or above, (ii) 90 or below.

[Ans. : (i) 0.0057, (ii) 0.0217]

#### Type XIII

1. A random variable has a Binomial distribution with  $n = 30$  and  $p = 0.60$ . Using normal approximation to Binomial distribution, find the probabilities that it will take (i) the value 14, (ii) a value less than 12.

[Ans. : (i) 0.0486, Find  $P(13.5 \leq X \leq 14.5)$ , (ii) 0.0078, Find  $P(X \leq 11.5)$ ]

2. A random variable has a Binomial distribution with  $n = 100$ ,  $p = 0.2$ . Using normal approximation to Binomial distribution, find the probabilities that it will take (i) a value less than 15.5, (ii) the value 15.

(Hint : For (i) Find  $P(X \leq 15.5)$  take (i) a value less than 16.)

[Ans. : (i) 0.1292, (ii) 0.0454. For (ii) find  $P(14.5 \leq X \leq 15.5)$ ]

3. A sample of 100 items is known to contain 40 defective items. Find in two different ways the probability that the sample will contain exactly 44 defective.

(M.U. 2007)

[Ans. : (i) Binomial Distribution  $p = 0.40$ ,  $q = 0.6$ .

$$P(x=44) = {}^{100}C_{44} (0.40)^{44} (0.60)^{56} = 0.0576.$$

(ii) Normal Distribution,  $m = np = 100 (0.4) = 40$ ,  $\sigma = \sqrt{npq} = 4.0$

$$Z = \frac{x-m}{\sigma} + P(43.5 < X < 44.5) = 0.060. ]$$

## Type XIV (Miscellaneous)

1. Find the probability of getting 30 to 35 diamond cards when cards are drawn with replacement from 100 pack of cards which is well-shuffled every time before a card is drawn, using (i) Normal distribution, (ii) Binomial distribution.

[Ans. : (i) By Normal Approximation : 0.141, (ii) By Binomial : 0.140]

2. Using normal distribution find the probability that in a group of 100 person there will be 55 males, assuming that the probability of a person being male is 1/2. [Ans. : 0.0484]

3. Using normal distribution find the probability that 65 students will pass in a group of 100 students if the probability of student's passing is 0.6. [Ans. : 0.0678]

4. Two independent random variates  $X$  and  $Y$  have normal distributions with means 46 and 45 and standard deviations 2 and 2.5 respectively. Find the probability that a randomly chosen pair of values of  $X$  and  $Y$  will (i) differ by 1.5 or more, (ii) add up to 100 or more.

[Ans. : (i) 0.6541, (ii) 0.0025]

5. If  $X$  and  $Y$  are two independent normal variates both with mean 0 and standard deviations 4, find the probability that the point  $(X, Y)$  lies between the lines  $4X + 3Y = 6$  and  $4X + 3Y = 14$ . [Ans. : 0.1401]

6. The time when a city-bus arrives at a certain bus-stop is distributed normally with a mean of 8.25 a.m., and standard deviation of 4 minutes. What is the least time one should arrive at the bus-stop and still have a probability of 0.99 of catching the bus?

(Hint : If  $T$  is the time in minutes past 8 a.m. then  $T$  follows  $N(25, 4)$ .  $z = \frac{T-25}{4}$  is S.N.V. For probability 0.99/2 = 0.495 table value of  $z = 2.575$ . For  $T$  least,  $z = -2.575 \therefore T = 14.3$  i.e. 15. He should arrive at 8.15.)

7. If  $X$  and  $Y$  are independent normal variates with the same mean  $\mu$  but with variances 4 and 48 such that  $P(X+2Y \geq 4) = P(2X-Y \leq 3)$ , find  $\mu$ .

[Ans. :  $U = X+2Y$  is  $N(3\mu, 10)$

and  $V = 2X - Y$  is  $N(\mu, 6)$ .  $P(U \geq 4) = P(V \leq 3)$

$$P\left(\frac{U-3\mu}{10} \geq \frac{4-10\mu}{10}\right) = P\left(\frac{V-\mu}{6} \leq \frac{3-\mu}{6}\right)$$

$$\therefore -\frac{4-10\mu}{10} = \frac{3-\mu}{6} \therefore \mu = \frac{27}{35}.$$

8. The number of words in a book are normally distributed with mean 800 and standard deviation 50. If 3 pages are selected at random what is the probability that none of them has between 830 and 845 words?

9. A factory turns out tubes by mass production methods. It was found that 20 tubes in a batch of 100 are defective. Find the variance of the defective tube in a batch. Also find the probability that the number of defective tubes in a batch is greater than 30.

[Ans. : var. = 16;  $P(X > 30) = 0.0062$ ]

10. Suppose that the length in hours, say  $X$  of light bulbs manufactured by a company A are normally distributed with mean 800 hours and standard deviation of 120 hours and those of B with mean 850 hours and standard deviation of 50 hours. One bulb is selected from the production of each company and is burned till "death". Find the probability that the length of life of the bulb from company A exceeds the length of the bulb from the company B at least by 15 hours.

(M.U. 2005) [Ans. : 0.2979]

## EXERCISE - IV

## Theory

- Define Binomial distribution and state its uses.
- Explain Binomial distribution.
- Find the first two moments about origin of Binomial distribution and hence, find mean and variance. (M.U. 2003)
- State whether the following statements are true or false. Give justification.
  - If for a Binomial distribution  $np$  is an integer then the mean and mode both are equal to  $np$ .
  - For a Binomial distribution mean is always greater than the variance.
  - For a Poisson variate mean and variance are equal.
  - If  $X$  is a Poisson variate with  $P(X=2) = 3P(X=4) + 45P(X=6)$  then the variance of  $X$  is 2.
- [Ans. : All are correct statements.]
- Show that for a Poisson distribution the mean and variance are same. (M.U. 1997)
- Prove for the Binomial distribution that  $\sum p(x) = 1$ . (M.U. 1998)
- For a Binomial distribution, prove that the mean and variance are  $np$  and  $npq$ . (M.U. 1997, 99)
- Find the mean and variance of Binomial distribution. (M.U. 1994, 98, 2007)
- Obtain the recurrence relation for Poisson distribution. (M.U. 2001)
- State the conditions under which Binomial distribution approximates to Poisson distribution. (M.U. 1999)
- Find moment generating function of Binomial distribution and hence, find its mean and variance. (M.U. 2002, 04, 15)
- Define Poisson distribution and state its uses.
- Find the mean and variance of the following distribution

$$f(x) = \frac{1}{n}, \quad x = 1, 2, 3, \dots, n$$

[Ans. : (i)  $\frac{n+1}{2}$  (ii)  $\frac{n^2-1}{12}$ ]

- Define Poisson distribution. What are its uses ?
- Define Poisson distribution and obtain it as the limiting case of Binomial distribution. (M.U. 2004)
- Derive Poisson distribution. (M.U. 2009)
- Find the mean and variance of Poisson distribution. (M.U. 2001, 03, 04, 06, 07, 09, 10)

18. State and prove additive property of Binomial distribution.
19. State and prove additive property of Poisson distribution.
20. Find the m.g.f. of Binomial distribution.
21. Derive Poisson distribution as a limiting case of binomial distribution.
22. Find the moment generating function of a Poisson distribution. Hence, find its mean and variance. (M.U. 1998)
23. Define Normal distribution and state its important properties. (M.U. 1998, 2004)
24. Define Normal distribution and find its mean and variance. (M.U. 2001, 04)
25. Find m.g.f. of Normal distribution about origin.
26. Define normal distribution and mention some of its important characteristics.
27. Explain importance of normal distribution.
28. Define Normal distribution. Define standard normal variate. Show that for standard normal variate mean is zero and standard deviation is 1. (M.U. 1998)
29. If  $X$  and  $Y$  are independent random variates having  $N(2, 1)$  and  $N(3, 2)$  respectively, find the distribution of (i)  $2X + 3Y$  and (ii)  $2X - 3Y$ . [Ans.: (i)  $N(13, \sqrt{40})$ , (ii)  $N(-5, \sqrt{40})$ ]
30. Obtain the m.g.f. of Normal Variate. (M.U. 2004)
31. Obtain the m.g.f. of Standard Normal variate and hence, find its mean and variance. (M.U. 2004)
32. Find the mean and variance of standard normal variate. (M.U. 1998, 2001, 04)
33. Define moment generating function. Obtain the same for Normal distribution. (M.U. 2000, 04)
34. Obtain moments of Normal distribution. (M.U. 2003, 07)
35. Define Standard Normal Variate. State its properties and uses. (M.U. 2002)
36. Prove that for a normal variate moments of odd power are zero and  $\mu_{2n} = 1 \cdot 3 \cdot 5 \dots (2n-1) \sigma^{2n}$ . (M.U. 2003, 04)
37. What is the moment generating function of a Normal variate? Also find the moment generating function of standard normal variates. (M.U. 2004)
38. State the purpose for which Normal distribution is widely used. (M.U. 2004, 05)



CHAPTER  
**8**

## Large Sample Tests

### 1. Introduction

One of the aims of statistical study of a problem is to be able to predict some characteristics concerning the problem. For example, we may be interested to know the average life or average income of an Indian. To obtain such values, information is collected from the group of the objects of study. In statistical language collecting information for statistical analysis is called collection of data and the aggregate of the objects of study is called the population or universe. There are two methods of collecting data (1) **Census Method** and (2) **Sampling Method**. In census method information is collected from every member of the population and in sampling method information is collected from members of a group selected from the universe by some technique. This group is called a sample.

#### A Parameter and A Statistic

A statistical measure such as mean, standard deviation calculated from the whole universe is called a parameter. On the other hand a statistical measure obtained from the values of a sample is called a statistic. Since in general, an universe is large, we use sampling method, obtain a sample, calculate from it a statistic and from the statistic we estimate the parameter.

### 2. Methods of Sampling

There are various methods of selecting a sample from the population. Choice of the method depends upon the information available about the population, nature of data and the object of inquiry. The methods are grouped into two classes. (1) Non-random Sampling or Non-probability Sampling, (2) Random Sampling or Probability Sampling.

#### (a) Non-probability Sampling

In non-probability sampling an item is included in the sample on the basis of personal judgement of the investigator. We shall study only the following method.

**Deliberate Sampling also called Judgement Sampling or Purposive Sampling :** The deliberate sampling is highly subjective in nature because the investigator chooses those members of the population in the sample that he thinks are the best representatives of the population. For example, if he wants to investigate expenditure pattern of students of a college having 800 students on roll he will select, say 100 students for the study at his will. There is no other rule for selection except his own will.

As is evident, although the method is very simple and easy to apply, it suffers from the drawback that it is highly subjective. Let us suppose that an investigator is studying wages of workers of a firm. If he is biased towards the workers, he will choose low paid workers and if he is biased towards the owner, he will choose highly paid workers to find out the average salary.

However, this method is useful if immediate results are required. If this is applied with proper care and skill by an experienced statistician, reliable results can be obtained.

#### (b) Probability Sampling

In probability sampling selection of an item in the sample is done with a certain rule. We shall study only one method.

**Simple Random Sampling :** Random sampling is a scientific and objective method of selection in which every item has an equal opportunity of being selected in the sample. If sample is random and sufficiently large in size then it is likely to represent population more accurately. The following methods are commonly used for random selection.

(i) **Lottery Method :** The method is simple and therefore popular for taking a random sample. The numbers or the names of all the members of the population are written on separate pieces of paper of the same size, shape and colour. The pieces are folded in the same manner, mixed up thoroughly in a drum and the required number of pieces are drawn blindly. All this ensures that each member of the population has equal opportunity of being selected in the sample.

Suppose we want to select a sample of 100 boys from a class of 800 boys. If lottery method is to be used the names of all the 800 boys are written on separate pieces of paper, they are folded, mixed and 100 of them are drawn from the drum blindly.

The method is used for drawing the prizes of a lottery and hence the name.

(ii) **Table of random numbers :** The lottery method is tedious to follow if the population is large. An alternative method is the method of random numbers. In this method all the items are given numbers. Then a book of random numbers is consulted. The book is opened at random and the numbers appearing on the page are read. The items bearing these numbers are included in the sample.

A number of statisticians have constructed tables of random numbers but Tippett's random numbers are commonly used. The table contains 10,400 numbers all in four digits arranged in a random manner. One question can be legitimately asked. Are these numbers really random? No proof can be given, but the experience has shown that we can rely upon the tables for all practical purposes.

### 3. Central Limit Theorem

Central limit theorem is a very important theorem in Statistical analysis. We give below the central limit theorem in two forms, one known as Liapounoff's Form and other known as Lindberg-Levy form.

#### Central Limit Theorem (Liapounoff's Form)

\*If  $X_1, X_2, \dots, X_n$  are independent random variates with  $E(X_i) = \mu_i$  and  $\text{Var}(X_i) = \sigma_i^2$ ,  $i = 1, 2, \dots, n$  then under certain general conditions  $S_n = X_1 + X_2 + \dots + X_n$  is a normal variate with  $\mu = \sum \mu_i$  and variance  $\sigma^2 = \sum \sigma_i^2$  as  $n$  tends to infinity. (meaning  $n$  is large.)

A particular form of the above theorem is of interest to us. The following form of the central limit theorem is known as Lindeberg-Levy theorem.

#### Central Limit Theorem (Lindeberg-Levy Theorem)

\*If  $X_1, X_2, \dots, X_n$  are independently and identically distributed random variates such that  $E(X_i) = \mu$  and  $\text{Var}(X_i) = \sigma^2$ ,  $i = 1, 2, \dots, n$  then  $S_n = X_1 + X_2 + \dots + X_n$  is a normal variate with mean  $\mu$  and variance  $n\sigma^2$  as  $n$  tends to infinity.

**Corollary :** From the above theorem, we get a very important corollary as follows:

If  $\bar{X}$  the mean of the sample of size  $n$ , taken from a population having the mean  $\mu$  and variance  $\sigma^2$  i.e. of

$$\bar{X} = \frac{X_1 + X_2 + \dots + X_n}{n}$$

$$\text{then } E(\bar{X}) = \frac{n\mu}{n} = \mu \text{ and } \text{Var}(\bar{X}) = \frac{1}{n^2}(n\sigma^2) = \frac{\sigma^2}{n}$$

In other words, we get the following important result as a corollary of Central Limit Theorem.

If  $\bar{X}$  is the mean of the sample of size  $n$  drawn from the population with mean  $\mu$  and standard deviation  $\sigma$  then  $\bar{X}$  is normally distributed with mean  $\mu$  and standard deviation  $\sigma/\sqrt{n}$  i.e.

$$Z = \frac{\bar{X} - \mu}{\sigma/\sqrt{n}}$$

is a S.N.V. as  $n \rightarrow \infty$ .

### 4. Sampling Distribution of Means ( $\sigma$ known)

If we are required to estimate a population mean, we can take a sample and use the sample mean as the estimate. Although we know that the sample mean will be close to the population mean we do not know what our error will be. We need therefore some way to know how much sample means will deviate from the population mean.

Suppose we take 1000 samples each of size 100 from the population. The difference between (i) the number of samples (1000) and (ii) the number of items in a sample i.e. sample size (100) should be carefully noted.

Now for each of these 1000 samples we can calculate a separate mean  $\bar{X}$ , thus getting 1000 values of  $\bar{X}$ , the sample mean. Most of these sample means will be close to the population mean although occasionally by chance, we may get a value considerably above or below the population mean.

By constructing a histogram from the sample means, we can obtain a frequency curve. The curve will look very much like a normal curve, a 'thin' one but all the same a normal curve. Moreover, it can be proved that the mean of such a distribution i.e. the mean of the sample means is equal to the true population mean. This distribution is called the sampling distribution of the sample means.

**The standard deviation of the mean :** We saw above that the sample mean  $\bar{X}$  is distributed normally with mean  $\mu$  where  $\mu$  is the mean of the population. But what is the standard deviation of the distribution of the sample mean? It can be shown that the standard deviation of the sample means, called standard error denoted by  $\sigma_{\bar{X}}$  is equal to  $\sigma/\sqrt{n}$  where  $\sigma$  is standard deviation of the population and  $n$  is the size of the sample.

Thus,  $\sigma_{\bar{X}} = \sigma/\sqrt{n}$

i.e.,

$$\text{V}(\bar{X}) = \sigma^2/n$$

Now, look at the whole thing again. If  $\bar{X}$  is the mean of the sample of size  $n$  drawn from the population with mean  $\mu$  and standard deviation  $\sigma$  then  $\bar{X}$  is normally distributed with mean  $\mu$  and standard deviation  $\sigma/\sqrt{n}$ .

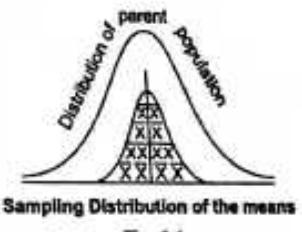


Fig. 8.1

If we put,  $Z = \frac{\bar{X} - \mu}{\sigma/\sqrt{n}}$ , then  $Z$  is a standard normal variate with the mean zero and standard deviation one.

### 5. Critical Region

$$\text{The fact that } Z = \frac{\bar{X} - \mu}{\sigma/\sqrt{n}}$$

is a S.N.V. is highly useful to us in drawing statistical inference. We know that for a S.N.V. 95% area under the curve lies between  $-1.96$  and  $+1.96$ , 99% between  $-2.58$  and  $+2.58$  and 99.73% between  $+3$  and  $-3$ . In other words, only 5% area under the curve lies beyond  $\pm 1.96$ , 1% beyond  $\pm 2.58$  and 0.27% beyond  $\pm 3$ . But the areas are also the probabilities that the S.N.V.  $Z$  will exceed these values i.e. the probability that  $Z$  will exceed  $1.96$  numerically is 0.05.

$$\therefore P(Z < -1.96 \text{ or } Z > 1.96) = 0.05$$

$$\therefore P(|Z| > 1.96) = 0.05$$

This means the probability that  $Z$  will lie in the shaded area is 0.05 - is very small.

$$\text{Similarly, } P(|Z| > 2.58) = 0.01 \text{ and } P(|Z| > 3) = 0.0027.$$

Suppose, we know the population mean is  $\mu$ , the population standard deviation is  $\sigma$  and we take a sample of size  $n$  from this population. Let the mean of this sample be  $\bar{X}_1$ , and let  $\frac{\bar{X}_1 - \mu}{\sigma/\sqrt{n}} = z_1$ .

Now, 95 out of 100 values of  $z_1$  will be between  $-1.96$  and  $+1.96$ . If  $z_1 > 1.96$  or  $z_1 < -1.96$ , a rare event has taken place because the probability of such an event is very small (0.05). The relative deviation of  $\bar{X}_1$  from  $\mu$  is so significant that it cannot be due to sampling fluctuations alone. Similarly, if  $z_1 > 2.58$  or  $-2.58 < z_1$ . A very unusual event has taken place because the probability of such an event is very remote (0.01). We again say that the deviation of  $\bar{X}_1$  from  $\mu$  is significant that it cannot be due to sampling fluctuations alone. The levels marked by probabilities 0.05 or 0.01 which decide the significance of an event are called **levels of significance** and are expressed in percentages as 5% level of significance or 1% level of significance. The corresponding regions are called **critical regions**.

The limits within which we expect  $z$  to lie with specified probabilities are called **confidence limits**. Thus,  $P(|z| > 1.96) = 0.05$  the bounding values  $\pm 1.96$  are the confidence limits, also called **fiducial limits**. This means we are confident that in 95 cases out of 100, the sample mean  $\bar{X}$  will be such that  $z$  lies between  $-1.96$  and  $1.96$ .

### 6. Procedure of Testing A Hypothesis

#### (1) To set up a hypothesis

A hypothesis is a statement supposed to be true till it is proved false. The hypothesis may be based on previous experience or may be derived theoretically. But a statistical hypothesis in the problems referred to above is a statement about parameters. A hypothesis can be stated in various

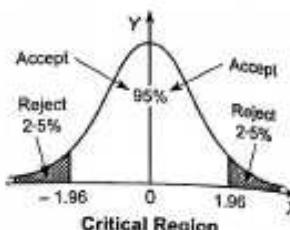


Fig. 8.2

ways e.g. the parameter is equal to a given value or the parameter is greater than the given value or the parameter is not equal to the given value etc.

A statistician generally sets up two hypothesis instead of one. They are called (i) Null Hypothesis and (ii) Alternative Hypothesis. They are set up in such a way that if one is true the other is false.

(i) **The Null Hypothesis**: The approach here is to set up the hypothesis, or assumption, that there is no contradiction between the believed result and the sample result and that the difference therefore can be ascribed solely to chance. Such a hypothesis is called a null hypothesis. The object of the test is to see whether the null hypothesis should be rejected or accepted.

(ii) **Alternative Hypothesis**: For example, if it is assumed that the mean of the weights of a population of boys in a college is 110 lbs., then the null hypothesis will be that the mean of the population is 110 lbs. The null hypothesis is denoted by  $H_0$ . In addition to this, one more hypothesis is stated. It is called an **alternative hypothesis** and is denoted by  $H_a$ . The alternative hypothesis generally specifies a range of values rather than one value. In the present example we may make an alternative hypothesis that the population mean is not equal to 110 lbs. These are denoted as:

$$H_0 : \mu = 110 \text{ lbs. (Null Hypothesis)}$$

$$H_a : \mu \neq 110 \text{ lbs. (Alternative Hypothesis)}$$

#### (2) To set up levels of significance

After setting up the null hypothesis we set up the limits within which we expect the null hypothesis to lie. The idea in setting up the hypothesis is to ensure that the difference between the sample value and the hypothesis should arise due to sampling fluctuations alone. If the difference does not exceed the limits the sample supports the hypothesis and it is accepted. If it exceeds the limits the sample does not support the hypothesis and it is rejected.

The limits are fixed depending upon the accuracy desired. Generally, the limits are fixed such that the probability that the difference will exceed the limits is 0.05 or 0.01. The probability that a random value of a statistic will lie in the critical region is called the **level of significance** (and is expressed in percentage as  $\alpha = 5\%$  or  $1\%$  level of significance)  $\alpha = 5\%$  level of significance means the probability of rejecting a true hypothesis is 0.05 and 1% level of significance means the probability of rejecting a true hypothesis is 0.01.

It should be noted that when a hypothesis is rejected it does not mean that the hypothesis is disproved. It only means that the sample value does not support the hypothesis. Similarly, when a hypothesis is accepted it does not mean that the hypothesis is proved. It means that the sample value supports the hypothesis.

#### (3) Confidence Limits

The limits within which an hypothesis should lie with specified probability are called **confidence limits** or **fiducial limits**. Generally, the confidence limits are set up with 5% or 1% level of significance. If the sample value lies between the confidence limits the hypothesis is accepted, if it does not, the hypothesis is rejected at the specified level of significance.

#### (4) Test Statistic

After setting up the hypothesis and after fixing the level of significance we need to calculate a statistic from sample values to test the hypothesis. Depending upon the nature of the data and the nature of the problem we use normal distribution, t-distribution,  $\chi^2$ -distribution, etc. From the sample we calculate sample mean or sample proportion etc. and from these we calculate the test statistic. Test statistic can be defined as the statistic calculated on the basis of appropriate probability

distribution for testing a hypothesis. Different probability distributions are used to calculate the test statistic depending upon the size and the nature of data.

The most commonly used test statistics are :-

**Z-distribution :** If the parent population can be considered at least approximately as normal distribution and if the sample is large ( $n \geq 30$ ), then we calculate the test statistic as

$$Z = \frac{\bar{X} - \mu}{\sigma / \sqrt{n}}$$

where,  $\bar{X}$  is the sample mean,  $\mu$  is the population mean to be tested,  $\sigma$  is the standard deviation of the population,  $n$  is the size of the sample.

**t-distribution :** If the sample size is small ( $n < 30$ ), then we calculate the test statistic as

$$t = \frac{\bar{X} - \mu}{s / \sqrt{n-1}}$$

where,  $\bar{X}$  is the sample mean,  $\mu$  is the population mean to be tested,  $s$  is the standard deviation of the sample,  $n$  is the size of the sample ( $< 30$ ).

**$\chi^2$ -distribution :** To test the goodness of fit, to test independence of attributes etc. we calculate  $\chi^2$ -statistic as

$$\chi^2 = \sum \left( \frac{(O-E)^2}{E} \right)$$

where,  $O$  is the observed frequency and  $E$  is the expected frequency of an event or a cell.

#### (5) Selection of test-statistic and its distribution

After setting up the null hypothesis and the alternative hypothesis and after deciding significance level, we construct a test criterion. Depending upon the nature of the population and size of the sample we decide the nature of the statistic and its probability distribution.

The following table shows the conditions under which z-test and t-tests are used. (t-distribution is discussed in the next chapter).

Sample size	Population s.d. $\sigma$ known	Population s.d. $\sigma$ unknown
$n \geq 30$ (Any population)	z-test	z-test
$n < 30$ (Population Normal or Approximately Normal)	z-test	t-test

#### (6) Making Decision

The next step is to compute the value of the statistic from given information and compare it with the table value for the chosen level of significance. The value of the sample statistic which separates the regions of acceptance and rejection, is called the critical value or significant value and denoted by  $z_\alpha$  (or  $t_\alpha$  or  $\chi^2_\alpha$ ) where  $\alpha$  denotes the level of significance. The region of rejection is called the critical region. The critical region may lie on one side or both sides of the sampling distribution of the test statistic. The area of a critical region (which actually gives the probability) in the tails is equal to the level of significance.

#### (7) Two Tailed and One Tailed Tests

The probability distribution of a sample statistic is a normal distribution. The z-curve is symmetrical as we know and the parts of the curve at the two ends are called the two tails of the curve. If the rejection area lies on the two sides i.e. on the two tails the test is called the two tailed test. If on the other hand the rejection area lies on one side only the test is called one tailed test.

**(i) Two Tailed Test :** In a two tailed hypothesis the rejection area lies on the two tails of the distribution curve. For example, while testing,

Null Hypothesis  $H_0 : \mu = \mu_0$

Alternative Hypothesis :  $\mu \neq \mu_0$

(i.e.  $\mu < \mu_0$  or  $\mu > \mu_0$ )

We use areas on both sides and hence, it is a two tailed test.

**(ii) One Tailed Test :** In one tailed test we use area lying on one side of the normal curve. When an alternative hypothesis is one sided for example,

$\mu > \mu_0$  or  $\mu < \mu_0$ , the test is one sided.

**(a) Right Tailed Test :** If the region of rejection lies on the right side of the normal curve, the test is called the right tailed test. For example, the test for  $\mu > \mu_0$  is a right tailed test.

**(b) Left Tailed Test :** If the region of rejection lies on the left side of the normal curve, the test is called the left tailed test. For example, the test  $\mu < \mu_0$  is a left tailed test.

**(c) Relation between the critical values for one-tailed test and two tailed test :** Let  $z_\alpha$  be the critical value of  $Z$  corresponding to the level of significance  $\alpha$  in the right-tailed test then

$$P(Z \geq z_\alpha) = \alpha$$

By symmetry of the standard normal distribution

$$P(Z < -z_\alpha) = \alpha$$

$$\therefore P(|Z| > z_\alpha) = P((Z < -z_\alpha) + (Z > z_\alpha))$$

$$= P(Z < -z_\alpha) + P(Z > z_\alpha)$$

$$= 2\alpha$$

Thus, the critical value of  $Z$  for a one-tailed test (right or left) at level of significance (LOS)  $\alpha$  is the same as that for a two-tailed test at the level of significance  $2\alpha$ .

In other words, this means for the same critical value  $z_\alpha$  the critical region i.e. the level of significance i.e. percentage of area for two tailed test is double that of one tailed test. This means for the same critical value, say, 1.64 or 2.33 for one tailed test, the critical regions (i.e. the probabilities) are 5% and 1% while the critical regions for two-tailed test are 10% and 2% respectively.

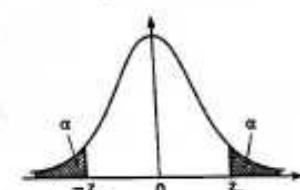


Fig. 8.3

Name of the test	Level of significance $\alpha$			
	1 %	2 %	5 %	10 %
Two tailed test	$ z_\alpha  = \pm 2.576$	$ z_\alpha  = \pm 2.326$	$ z_\alpha  = \pm 1.960$	$ z_\alpha  = \pm 1.645$
Right tailed test	$z_\alpha = +2.326$	$z_\alpha = +2.054$	$z_\alpha = +1.645$	$z_\alpha = +1.282$
Left tailed test	$z_\alpha = -2.326$	$z_\alpha = -2.054$	$z_\alpha = -1.645$	$z_\alpha = -1.282$

The same table is recast from different point of view below.

Table of Critical Values (Normal Distribution)

Name of the test	Critical Value			
	$z_{\alpha} = 1.64$	$z_{\alpha} = 1.96$	$z_{\alpha} = 2.33$	$z_{\alpha} = 2.58$
Two tailed test (LOS)	$\alpha = 10\%$	$\alpha = 5\%$	$\alpha = 2\%$	$\alpha = 1\%$
Right tailed test (LOS)	$\alpha = 5\%$	$\alpha = 2.5\%$	$\alpha = 1\%$	$\alpha = 0.5\%$
Left tailed test (LOS)	$\alpha = 5\%$	$\alpha = 2.5\%$	$\alpha = 1\%$	$\alpha = 0.5\%$

It may be noted again that the critical value of  $z_{\alpha}$  for single-tailed test (left or right) at a level of significance  $\alpha$  is the same as critical value of  $z_{\alpha}$  for a two-tailed test at a level of significance  $2\alpha$  as discussed earlier.

$\alpha = 10\%$  level of significance

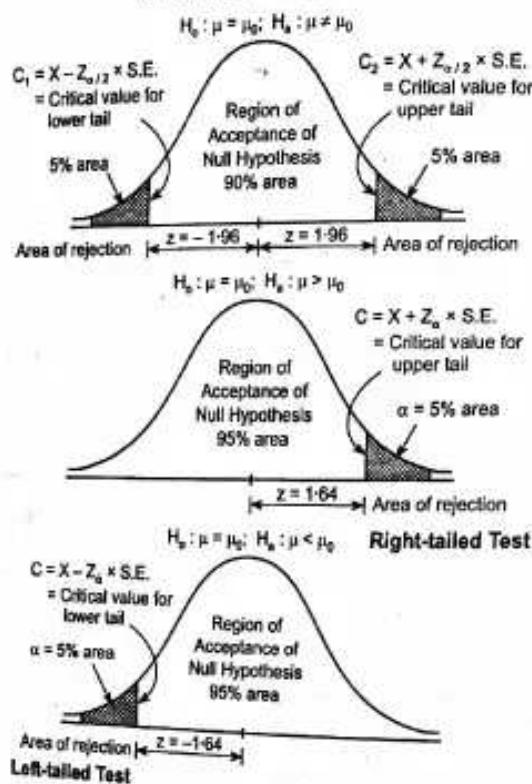


Fig. 8.4

### 7. Errors in Testing of Hypothesis

When a statistical hypothesis is tested there are only two results either we accept it or we reject it. We never know whether the hypothesis is true or false. Hence there arise four possibilities:

- A true hypothesis is rejected,
- A true hypothesis is accepted,
- A false hypothesis is rejected,
- A false hypothesis is accepted.

Obviously, if the outcome of the test leads to the possibilities (i) and (iv) then we are committing an error of (a) rejecting a true hypothesis or (b) accepting a false one. The possibility (a) is called type I error and the possibility (b) is called type II error.

#### Type I Error

Type I error arises when a true hypothesis is rejected i.e. when the difference between the sample value and hypothetical value exceeds the confidence limits. The error can be minimised by increasing the confidence limits. But then because of this the error of type II i.e. of accepting a false hypothesis is increased, because we do not know whether the hypothesis is true or false in reality.

#### Type II Error

Type II error arises when a false hypothesis is accepted i.e. when the difference between the sample value and the hypothetical value lies within the limits. The error can be minimised by decreasing the confidence limits. But then the error of type I i.e. of rejecting a true hypothesis is increased, because we again do not know whether the hypothesis is true or false in reality.

Thus, it seems that when error of one type is decreased that of the other is increased. The statistician therefore has to decide, depending upon the nature of the problem, as to which type of error he wishes to avoid. In certain problems type I error may prove to be serious and in certain other problems type II error may prove to be serious. Hence, the levels of significance will have to be decided on considering the practical consequences of the errors of both the types.

The four situations arising in the process of decision making can be described in the form of a table as

	$H_0$ is accepted	$H_0$ is rejected
$H_0$ is true	Correct decision	Type I error
$H_0$ is false	Type II error	Correct decision

Fig. 8.5

We shall now see how to test a hypothesis. We shall consider only two types of samples (i) Sampling of Variables, (ii) Sampling of Attributes.

### 8. Sampling of Variables

We have already seen that the sample mean  $\bar{X}$  is normally distributed with mean  $\mu$  and standard deviation  $\sigma / \sqrt{n}$  where  $\mu$  is the mean of the population and  $\sigma$  is the standard deviation of the population. This result is going to help us in testing a hypothesis about the population mean.

**9. Testing the Hypothesis that the Population Mean =  $\mu$** 

Suppose that the standard deviation  $\sigma$  of the population is known and let the null hypothesis to be tested be

$$H_0 : \text{mean} = \mu$$

If  $\bar{X}$  is the sample mean, then  $\bar{X}$  is distributed normally with mean  $\mu$  and standard deviation  $\sigma/\sqrt{n}$ . Hence,  $Z = \frac{\bar{X} - \mu}{\sigma/\sqrt{n}}$  is a standard normal variate with mean zero and standard deviation one.

Now we take a sample and find its mean  $\bar{X}$ . If this observed mean  $\bar{X}$  is such that  $|Z| = \left| \frac{\bar{X} - \mu}{\sigma/\sqrt{n}} \right|$  (called relative deviation of sample mean  $\bar{X}$  from the population mean  $\mu$ ) exceeds 1.96 numerically then a rare event has occurred because the probability of  $|Z| = \left( \frac{\bar{X} - \mu}{\sigma/\sqrt{n}} \right) > 1.96$  is very small. As can be seen from the table  $P(|Z| > 1.66) = 0.05$ . If from the sample chosen we get the value of  $\bar{X}$  such that

$$|Z| = \left| \frac{\bar{X} - \mu}{\sigma/\sqrt{n}} \right| > 1.96$$

we say that relative deviation of  $\bar{X}$  from  $\mu$  is significant and not due to sampling fluctuations alone. We, therefore, reject the hypothesis at 5% level of significance if  $|Z| > 1.96$ . Similarly, we define other levels.

Note ...

If the standard deviation  $\sigma$  of the population is not known and if the sample size  $n$  is large ( $\geq 30$ ) then we use the standard deviation  $s$  of the sample in place of  $\sigma$ .

**Example 1 :** A random sample of 50 items gives the mean 6.2 and variance 10.24. Can it be regarded as drawn from a normal population with mean 5.4 at 5% level of significance? (M.U. 1998, 2015)

Sol. : (i) Null Hypothesis  $H_0 : \mu = 5.4$

Alternative Hypothesis  $H_a : \mu \neq 5.4$

(ii) Test Statistic : Since the population S.D. is unknown but sample S.D.  $s$  is known and since sample is large

$$Z = \left| \frac{\bar{X} - \mu}{s/\sqrt{n}} \right| = \left| \frac{6.2 - 5.4}{\sqrt{10.24}/\sqrt{50}} \right| = \left| \frac{0.8}{3.2/7.07} \right| = 1.77$$

$$\therefore |Z| = 1.77$$

(iii) Level of significance :  $\alpha = 0.05$

(iv) Critical value : The value of  $z_\alpha$  at 5% level of significance from the table = 1.96.

(v) Decision : Since the computed value of  $|Z| = 1.77$  is less than the critical value  $z_\alpha = 1.96$ , the null hypothesis is accepted.

∴ The sample is drawn from the population with mean 5.4.

**Example 2 :** A random sample of 400 members is found to have a mean of 4.45 cms. Can it be reasonably regarded as a sample from a large population whose mean is 5 cms and variance is 4 cms. (M.U. 2016)

Sol. : (i) Null Hypothesis  $H_0 : \mu = 5$

Alternative Hypothesis  $H_a : \mu \neq 5$

(ii) Test Statistic :  $Z = \left| \frac{\bar{X} - \mu}{\sigma/\sqrt{n}} \right|$

Since we are given standard deviation of the population, we put

$$\bar{X} = 4.45, \mu = 5, \sigma = 2, n = 400$$

$$\therefore Z = \left| \frac{4.45 - 5}{2/\sqrt{400}} \right| = \left| \frac{0.55}{2/20} \right| = 5.5$$

(iii) Level of Significance :  $\alpha = 0.05$ .

(iv) Critical value : The value of  $z_\alpha$  at 5% level of significance from the table = 1.96.

(v) Decision : Since the computed value of  $Z = 5.5$  is greater than the critical value  $z_\alpha = 1.96$ , the null hypothesis is rejected and the alternative hypothesis is accepted.

∴ The sample is not drawn from the above population.

**Example 3 :** Can it be concluded that the average life-span of an Indian is more than 70 years, if a random sample of 100 Indians has an average life span of 71.8 years with standard deviation of 8.9 years? (M.U. 2004)

Sol. : (i) Null Hypothesis  $H_0 : \mu = 70$  years.

Alternative Hypothesis  $H_a : \mu \neq 70$  years

(ii) Test Statistic :  $Z = \left| \frac{\bar{X} - \mu}{\sigma/\sqrt{n}} \right|$

Since we are given standard deviation of the sample, we put

$$\bar{X} = 71.8, \mu = 70, \sigma = 8.9, n = 100$$

$$\therefore Z = \frac{71.8 - 70}{8.9/\sqrt{100}} = 2.02$$

(iii) Level of Significance :  $\alpha = 0.05$ .

(iv) Critical value : The value of  $z_\alpha$  at 5% level of significance is 1.96.

(v) Decision : Since the computed value of  $|Z| = 2.02$  is greater than the critical value  $z_\alpha = 1.96$ , the null hypothesis is rejected.

∴ The hypothesis is rejected.

**Example 4 :** A tyre company claims that the lives of tyres have mean 42,000 kms with S.D. of 4000 kms. A change in the production process is believed to result in better product. A test sample of 81 new tyres has a mean life of 42,500 kms. Test at 5% level of significance that the new product is significantly better than the old one. (M.U. 2006, 09)

Sol. : (i) Null Hypothesis  $H_0 : \mu = 42000$

Alternative Hypothesis  $H_a : \mu \neq 42000$

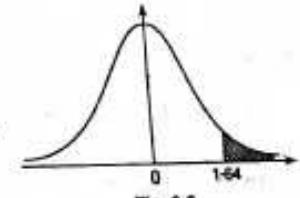


Fig. 9.6

- (i) **Test Statistic :** Since the population S.D. is unknown but sample S.D.  $s$  is known and since the sample is large

$$Z = \frac{\bar{X} - \mu}{\sigma/\sqrt{n}} = \frac{42500 - 42000}{4000/\sqrt{61}} = 1.125$$

$$\therefore |Z| = 1.125$$

- (ii) **Level of Significance :**  $\alpha = 0.05$

- (iv) **Critical value :** The value of  $z_{\alpha}$  at 5% level of significance is 1.96.

- (v) **Decision :** Since the computed value of  $|Z| = 1.125$  is less than the critical value  $z_{\alpha} = 1.96$ , the null hypothesis is accepted.

$\therefore$  There is no improvement.

### EXERCISE - I

1. A machine is claimed to produce nails of mean length 5 cm. and standard deviation of 0.45 cm. A random sample of 100 nails gave 5.1 cm. as their average length. Does the performance of the machine justify the claim? Mention the level of significance you apply.

(M.U. 2014) [Ans. :  $|Z| = 2.2$ , No, at 5%]

2. The mean height of random sample of 100 individuals from a population is 160. The S.D. of the sample is 10. Would it be reasonable to suppose that the mean height of the population is 165?

(M.U. 2005) [Ans. :  $|Z| = 5$ , No]

3. A sample of 50 pieces of certain type of string was tested. The mean breaking strength turned out to be 14.5 pounds. Test whether the sample is from a batch of a string having a mean breaking strength of 15.6 pounds and standard deviation of 2.2 pounds. [Ans. :  $|Z| = 3.53$ , No]

4. The mean breaking strength of cables supplied by a manufacturer is 1800 with standard deviation 100. By a new technique in the manufacturing process it is claimed that the breaking strength of the cable has increased. In order to test the claim a sample of 50 cables is tested. It is found that the mean breaking strength is 1850. Can we support the claim at 1% level of significance.

(M.U. 2007, 09) [Ans. :  $|Z| = 3.54$ . Right tail test, Yes]

5. A random sample of size 36 has 53 as mean and sum of squares of deviations from mean is 150. Can this sample be regarded as drawn from the population having 54 as mean?

[Ans. :  $s = 2.04$ ,  $|Z| = 2.94$ , Yes at 0.27%]

6. A distribution with unknown  $\mu$  has variance 1.5. Use central limit theorem to find how large a sample should be taken from the distribution in order that the probability will be at least 0.95 that the sample will be within 0.5 of the population mean.

(M.U. 2004)

$$\text{Hint: } \frac{\bar{X} - \mu}{\sigma/\sqrt{n}} = 1.96 \quad i.e., \quad \frac{0.5}{\sqrt{1.5}/\sqrt{n}} = 1.96$$

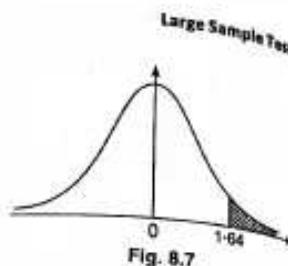
[Ans. :  $n = 23$ ]

7. A random sample of 900 items is found to have a mean of 65.3 cms. Can it be regarded as a sample from a large population whose mean is 66.2 cms. and standard deviation is 5 cms. at 5% level of significance?

(M.U. 2014) [Ans. :  $|Z| = 5.4$ , No]

8. A machine is set to produce metal plates of thickness 1.5 cms with standard deviation of 0.2 cms. A sample of 100 plates produced by the machine gave an average thickness of 1.52 cms. Is the machine fulfilling the purpose?

[Ans. :  $|Z| = 1$ , Yes]



### 10. Testing the Difference Between Means

Sometimes we may have two distinct populations and we may want to test whether they have equal means. For example, we may want to know whether the average I.Q. of students of Mumbai University is equal to average I.Q. of students of Pune University. If we actually take samples from two populations, it is unlikely that the two sample means would be identical. Even if they are equal, how are we to know whether the two samples came from populations having equal means or that the two samples came from the same population? In other words, how can we test the hypothesis that the two populations have equal means? The procedure to test this hypothesis is discussed below.

#### (i) Distribution of the difference between means

Suppose two populations have equal means. Suppose further we draw a large number of pairs of samples from the two populations. Let us take difference between the pairs of sample means for all these pairs, always subtracting the sample mean of the second population from the sample mean of the first population. If these differences are graphed we would find that the distribution would follow a normal curve. If  $\bar{X}_1$  and  $\bar{X}_2$  denote the means of the samples drawn from the first and the second population respectively having means  $\mu_1$ ,  $\mu_2$  and standard deviations  $\sigma_1$ ,  $\sigma_2$  and if the sizes of the samples are  $n_1$  and  $n_2$ . Then we can prove that the distribution of the difference between the means  $\bar{X}_1 - \bar{X}_2$  is normally distributed with mean  $\mu_1 - \mu_2$  and standard deviation given by

$$s = \sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}$$

$$\text{i.e., } Z = \frac{(\bar{X}_1 - \bar{X}_2) - (\mu_1 - \mu_2)}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}} \text{ is a S.N.V.}$$

Further, under the hypothesis  $\mu_1 = \mu_2$  we see that

$$Z = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}} \text{ is a S.N.V.} \quad (i)$$

If the samples are drawn from the same population, so that  $\sigma_1 = \sigma_2 = \sigma$ , we see from the above expression, that

$$Z = \frac{\bar{X}_1 - \bar{X}_2}{\sigma \sqrt{(1/n_1) + (1/n_2)}} \text{ is a S.N.V.} \quad (ii)$$

(i) If samples are large then  $\sigma_1^2 = s_1^2$ ,  $\sigma_2^2 = s_2^2$  asymptotically and

$$\text{S.E.} = \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}$$

(ii) If samples are large and  $\sigma_1 = \sigma_2 = \sigma$ , then the combined standard deviation of the two samples is given by

$$s^2 = \frac{\sum (x_{1i} - \bar{x}_1)^2 + \sum (x_{2i} - \bar{x}_2)^2}{n_1 + n_2}$$

But  $\frac{\sum(x_i - \bar{x}_1)^2}{n_1} = s_1^2$  and  $\frac{\sum(x_i - \bar{x}_2)^2}{n_2} = s_2^2$

$$\therefore s^2 = \frac{n_1 s_1^2 + n_2 s_2^2}{n_1 + n_2}$$

$s^2$  is asymptotically unbiased estimator of  $\sigma^2$ .

$$\begin{aligned} \text{S.E.} &= \sqrt{\frac{n_1 s_1^2 + n_2 s_2^2}{n_1 + n_2} \cdot \frac{1}{n_1 + n_2}} \\ &= \sqrt{\frac{n_1 s_1^2 + n_2 s_2^2}{n_1 + n_2} \cdot \frac{n_1 + n_2}{n_1 + n_2}} = \sqrt{\frac{s_1^2 + s_2^2}{n_1 + n_2}}. \end{aligned}$$

#### (2) Procedure to test the hypothesis : $\mu_1 = \mu_2$ :

Suppose we take two samples of size  $n_1$  and  $n_2$  with means  $\bar{X}_1$  and  $\bar{X}_2$  from the populations with means  $\mu_1$ ,  $\mu_2$  and standard deviation  $\sigma_1$ ,  $\sigma_2$ . To test the hypothesis that  $\mu_1 = \mu_2$ .

(i) we calculate  $\bar{X}_1 - \bar{X}_2$

(ii) then we calculate the standard error,

$$\text{S.E. } s = \sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}} \quad \dots \dots \dots (1)$$

(iii) Then we calculate,  $|Z| = \left| \frac{\bar{X}_1 - \bar{X}_2}{s} \right|$  and take the decision as explained in 2 (i) above.

#### Remarks ...

- If the samples are drawn from the populations with common S.D.  $\sigma$  i.e. if  $\sigma_1 = \sigma_2 = \sigma$  (known) then standard error

$$\text{S.E. } s = \sigma \sqrt{\frac{1}{n_1} + \frac{1}{n_2}} \quad \dots \dots \dots (2)$$

In this case we calculate the value of

$$|Z| = \left| \frac{\bar{X}_1 - \bar{X}_2}{\sigma \sqrt{\frac{1}{n_1} + \frac{1}{n_2}}} \right|$$

- If population standard deviations  $\sigma_1$  and  $\sigma_2$  are not known ( $\sigma_1 \neq \sigma_2$ ) and if the sample sizes  $n_1$  and  $n_2$  are sufficiently large, (since sample standard deviation  $s$  is asymptotically unbiased estimator of standard deviation of the population) we replace  $\sigma_1$  by  $s_1$  and  $\sigma_2$  by  $s_2$  and find the S.E.  $s$  from,

$$\text{S.E. } s = \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}} \quad \dots \dots \dots (3)$$

In this case  $|Z| = \left| \frac{\bar{X}_1 - \bar{X}_2}{s} \right|$

3. If the standard deviations of the two populations  $\sigma_1$  and  $\sigma_2$  are equal to  $\sigma$ , say, and are unknown and if  $s_1$  and  $s_2$  are the standard deviations of the samples of sizes  $n_1$  and  $n_2$ , then

$$\text{S.E. } s = \sqrt{\frac{s_1^2}{n_2} + \frac{s_2^2}{n_1}} \quad \dots \dots \dots (4)$$

Carefully note the difference between the denominators of the formulae (3) and (4).

Note ...

Formulae for  $s$  given in (1), (2), (3) and (4) are to be taken into consideration for testing the hypothesis  $\mu_1 > \mu_2$  as well as for estimating the interval of  $\mu_1 - \mu_2$ .

#### Testing of Hypothesis

Example 1 : The means of two samples of sizes 1000 and 2000 respectively are 67.50 and 68.0 inches. Can the samples be regarded as drawn from the same population of standard deviation 2.5 inches ?

(M.U. 2015)

Sol. (i) Null Hypothesis  $H_0 : \mu_1 = \mu_2$

Alternative Hypothesis  $H_A : \mu_1 \neq \mu_2$

(ii) Calculation of Statistic :  $\bar{X}_1 - \bar{X}_2 = 67.5 - 68.0 = -0.5$

Since S.D. of the population is known,

$$\text{S.E. } s = \sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}} = \sigma \sqrt{\frac{1}{n_1} + \frac{1}{n_2}}$$

$$= (2.5) \sqrt{\frac{1}{1000} + \frac{1}{2000}} = 0.097$$

$$\therefore Z = \frac{\bar{X}_1 - \bar{X}_2}{s} = \frac{-0.5}{0.097} = -5.15 \quad \therefore |Z| = 5.15.$$

(iii) Level of significance :  $\alpha = 0.27\%$

(iv) Critical Value : The value of  $z_{\alpha}$  at 0.27% level of significance from the table is 3.

(v) Decision : Since the computed value of  $|Z| = 5.15$  is greater than the critical value  $z_{\alpha} = 3$ , the hypothesis is rejected.

∴ The samples cannot be regarded as drawn from the same population.

Example 2 : The average of marks scored by 32 boys is 72 with standard deviation 8 while that of 36 girls is 70 with standard deviation 6. Test at 1% level of significance whether the boys perform better than the girls.

(M.U. 2004, 09, 10, 15, 16)

Sol. (i) Null Hypothesis  $H_0 : \mu_1 = \mu_2$

Alternative Hypothesis  $H_A : \mu_1 \neq \mu_2$

(ii) Calculation of Statistic :  $\bar{X}_1 - \bar{X}_2 = 72 - 70 = 2$

$$\text{S.E. } s = \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}} = \sqrt{\frac{64}{32} + \frac{36}{36}} = \sqrt{3}$$

$$\therefore Z = \frac{\bar{X}_1 - \bar{X}_2}{s} = \frac{2}{\sqrt{3}} = 1.15 \quad \therefore |Z| = 1.15$$

(We assume that the standard deviations  $\sigma_1$  and  $\sigma_2$  of the two populations are not equal.)

- (iii) Level of significance :  $\alpha = 1\%$   
 (iv) Critical Value : The value of  $z_{\alpha}$  at 1% level of significance from the table is 2.58.  
 (v) Decision : Since the computed value of  $|Z| = 1.15$  is less than the critical value  $z_{\alpha} = 2.58$ , the hypothesis is accepted.  
 $\therefore$  Boys do not perform better than the girls.

Example 3 : Test the significance of the difference between the means of two normal populations with the same standard deviation from the following data.

	Size	Mean	S.D.
Sample I	100	64	6
Sample II	200	67	8

Sol. : (i) Null Hypothesis  $H_0 : \mu_1 = \mu_2$

Alternative Hypothesis  $H_a : \mu_1 \neq \mu_2$

(ii) Calculation of Statistic :  $\bar{X}_1 - \bar{X}_2 = 67 - 64 = 3$

Since the standard deviations of the two populations are equal but unknown

$$\begin{aligned} S.E.s &= \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}} = \sqrt{\frac{36}{200} + \frac{64}{100}} \\ &= \sqrt{0.18 + 0.64} = \sqrt{0.82} = 0.91 \\ \therefore Z &= \frac{\bar{X}_1 - \bar{X}_2}{S.E.s} = \frac{3}{0.91} = 3.3 \quad \therefore |Z| = 3.3 \end{aligned}$$

(iii) Level of Significance :  $\alpha = 5\%$

(iv) Critical value :  $z_{\alpha}$  at 5% LOS is 1.96.

(v) Decision : Since the computed value of  $|Z| = 3.3$  is greater than the critical value  $z_{\alpha} = 1.96$ , the null hypothesis is rejected.

$\therefore$  The samples do not support the hypothesis that the two populations have the same mean although they may have the same standard deviation.

Example 4 : Two samples drawn from two different populations gave the following results.

	Size	Mean	S.D.
Sample I	125	340	25
Sample II	150	380	30

Test the hypothesis at 5% LOS that the difference of the means of the two populations is 45.

Sol. : (i) Null Hypothesis  $H_0 : \mu_1 - \mu_2 = 45$

Alternative Hypothesis  $H_a : \mu_1 \neq \mu_2$

(ii) Calculation of Statistic :  $\bar{X}_1 - \bar{X}_2 = 40$ ,  $\mu_1 - \mu_2 = 35$

$$\begin{aligned} S.E.s &= \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}} = \sqrt{\frac{25^2}{125} + \frac{30^2}{150}} = 3.32 \\ \therefore Z &= \frac{(\bar{X}_1 - \bar{X}_2) - (\mu_1 - \mu_2)}{S.E.s} = \frac{40 - 35}{3.32} = 1.5 \quad \therefore |Z| = 1.5 \end{aligned}$$

(iii) Level of Significance :  $\alpha = 5\%$

(iv) Critical value :  $z_{\alpha}$  at 5% LOS is 1.96.

(v) Decision : Since the computed value of  $|Z| = 1.5$  is less than the critical value  $z_{\alpha} = 1.96$ ,  
 $\therefore$  The data supports the hypothesis that the difference between the means of the two populations may be 45.

Example 5 : Two populations have the same mean but the standard deviation of one is twice that of the other. Show that in samples, each of size 500, drawn under simple random conditions the difference of the means, in all probability, will not exceed  $0.3\sigma$ , where  $\sigma$  is the smaller standard deviation.

(M.U. 2007)

Sol. : We have  $\mu_1 = \mu_2 = \mu$ ,  $\sigma_1 = \sigma$ ,  $\sigma_2 = 2\sigma$ ;  $n_1 = 500$ ,  $n_2 = 500$ .

$$\begin{aligned} S.E.s &= \sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}} = \sqrt{\frac{\sigma^2}{500} + \frac{4\sigma^2}{500}} \\ &= \sqrt{\frac{5\sigma^2}{500}} = \sqrt{\frac{\sigma^2}{100}} = \frac{\sigma}{10} \end{aligned}$$

We want  $|\bar{X}_1 - \bar{X}_2| < 0.3\sigma$

Dividing both sides by S.E.,

$$\left| \frac{\bar{X}_1 - \bar{X}_2}{S.E.s} \right| < \frac{0.3\sigma}{\sigma/10} \quad [\because \sigma \text{ is positive}]$$

$$\therefore \left| \frac{\bar{X}_1 - \bar{X}_2}{S.E.s} \right| < 3$$

For S.N.V.  $Z = 3$ , 99.73% area lies under the curve. The event is almost impossible. Hence, for  $\mu_1 = \mu_2$ ,  $|\bar{X}_1 - \bar{X}_2|$  in all probability will be  $< 0.3\sigma$ .

## EXERCISE - II

1. A sample of 200 fish of a particular kind taken at random from one end of a lake had mean weight of 20 lbs. and standard deviation of 2 lbs. At the other end of the lake, a sample of 80 fish of the same kind had mean weight of 20.5 lbs. and standard deviation of 2 lbs. also. Is the difference between the mean weights significant ?

[Ans. :  $|Z| = 1.89$ , No]

2. A man buys 100 electric bulbs of each of two well-known makes taken at random from stock for testing purpose. He finds that 'make A' has a mean life of 1300 hours with a S.D. of 82 hours, and 'make B' has a mean life of 1248 hours with S.D. of 93 hours. Discuss the significance of these results.

[Ans. :  $|Z| = 4.19$ , Significant]

3. The mean consumption of food grains among 400 sampled middle class consumers is 380 grams per day per person with a standard deviation of 120 grams. A similar sample survey of 600 working class consumers gave a mean of 410 grams with standard deviation of 80 grams. Are we justified in saying that the difference between the averages of the two classes is 40 ? Use 5% level of significance.

[Ans. :  $|Z| = 5.86$ , No]

4. Two groups consisting of 400 and 500 persons have mean heights 68.5 inches and 66.1 inches and variance 6.4 and 6.0 respectively. Examine whether the difference is significant.

[Ans. :  $|Z| = 14.54$ , Yes]

**Applied Mathematics - IV**

(8-18)

**Large Sample Tests**

5. A potential buyer of light bulbs bought 50 bulbs each of 2 brands. Upon testing the bulbs, he found that brand A had a mean life of 1,282 hours with a S.D. of 80 hours; brand B had a mean life of 1,208 hours with S.D. of 94 hours. Can the buyer be quite certain that the means of the two brands do differ in quality ? [Ans. :  $|z| = 4.24$ , Yes]

6. Average height of a sample of 6400 persons from one population was found to be 67.85 inches with a S.D. of 2.56 inches. Average height of a sample of 1600 persons from another population was found to be 68 inches with a S.D. of 2.52 inches. Is the difference between the mean heights of the two samples significant ? [Ans. :  $|z| = 2.12$ , No at 1%]

7. Intelligence tests of two groups of boys and girls obtained from two normal populations having the same standard deviations gave the following results.

	Mean	S.D.	No.
Girls	84	10	121
Boys	81	12	81

Is the difference between the means significant ? [Ans. :  $|Z| = 1.93$ , No]

8. The mean life of a sample of 100 electric light bulbs was found to be 1456 hours with S.D. 400. A second sample of 225 bulbs chosen from a different batch showed a mean life of 1400 hours with standard deviation of 144 hours. Assuming that the two populations have same standard deviation find, if there any significant difference between the mean of two batches ? [Ans. :  $|Z| = 1.84$ , No]

**EXERCISE - III****Theory**

- Distinguish between :-  
 (i) Census Survey and Sample Survey.  
 (ii) Sample and population.  
 (iii) Standard deviation and standard error.  
 (iv) Null Hypothesis and Alternative Hypothesis.  
 (v) Type I error and type II error.  
 (vi) Point estimation and Interval estimation.  
 (vii) Statistic and parameter  
 (viii) One tailed test and two tailed test. (M.U. 2007)
- Explain the following terms  
 (i) Statistic and Parameter. (ii) Test Statistic.  
 (iii) Level of Significance. (iv) Null of Hypothesis. (M.U. 1998)
- What are the principles of sampling ?
- What are the principles of sampling ?
- Explain simple random sampling method. State its merits and demerits. (M.U. 2005)
- Explain the use of random numbers in selection of a sample. Indicate the method used and the principles adopted. (M.U. 1997)
- Define the following terms  
 (i) Sampling. (ii) Standard Error. (iii) Level of Significance. (M.U. 2002)
- Define finite population correction factor.

**Applied Mathematics - IV**

(8-19)

**Large Sample Tests**

- If  $\bar{X}$  is the mean of a random sample of size  $n$  taken from the population of size  $n$  having mean  $\mu$  and variance  $\sigma^2$  then, prove that the mean of  $\bar{X}$  is  $m$  and the variance of  $\bar{X}$  is  $\sigma/\sqrt{n}$ . (M.U. 2005)
- Prove that the sample mean  $\bar{X}$  is an unbiased estimator of the population mean  $\mu$ .
- Prove that sample variance  $s^2 = \frac{\sum(x_i - \bar{x})^2}{n}$  is not an unbiased estimator of population variance  $\sigma^2$ . (M.U. 2005)
- If  $S^2 = \frac{1}{n-1} \sum(x_i - \bar{x})^2$  then prove that  $S^2$  is an unbiased estimator of  $\sigma^2$ . (M.U. 2006)
- Explain the following terms : (i) Critical Region, (ii) Fiducial Limits. (M.U. 2006)
- Write short note on  
 (i) Null Hypothesis and alternative hypothesis.  
 (ii) Type I error and type II error.  
 (iii) Level of significance and Confidence interval.  
 (iv) One tailed and two tailed tests. (M.U. 2004, 07)
- Summarise various steps in testing a statistical hypothesis in a systematic manner. (M.U. 2004)
- Describe briefly the steps used in testing of a statistical hypothesis. (M.U. 2003)
- (See § 6, page 8-4)
- State Central Limit Theorem. (M.U. 2001)
- Derive the formulae for sample size for testing (i) mean and (ii) proportion. (M.U. 2004)
- Describe the test of significance of difference between sample mean and population mean. (M.U. 2004)



## CHAPTER 9

# Small Sample Tests

### 1. Introduction

In the previous chapter we have seen that if the samples are large ( $\geq 30$ ) then the sampling distribution of a statistic is normal. But if the samples are small ( $< 30$ ) then the above result does not hold good and for estimation of the parameter as well as for testing a hypothesis we cannot use the above methods.

If we take a large number of samples of small ( $< 30$ ) size, calculate the mean of each sample, plot the frequencies and obtain the frequency curve we will find that the resulting sampling distribution of the mean is not normal but is the student's  $t$ -distribution.

### 2. Student's $t$ -distribution

Theoretical work on  $t$ -distribution was done by Irish Statistician W. S. Gosset. W. S. Gosset was working with Guinness Brewery in Dublin which did not allow its employees to publish their research work under their own names. So he adopted the pen-name "Student" and published his research work under that name in early period of 20th century. Hence, this distribution is known as Student's  $t$ -distribution or simply  $t$ -distribution.

The  $t$ -distribution is used when (i) the sample size is 30 or less and (ii) population standard deviation is not known.

The " $t$ -statistic" is defined as

$$t = \frac{\bar{X} - \mu}{S/\sqrt{n}} \quad \text{where, } S = \sqrt{\frac{\sum (X_i - \bar{X})^2}{n-1}}$$

The curve is given by

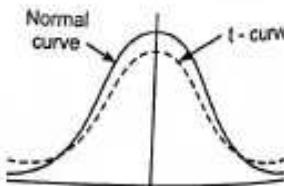
$$y = C \left(1 + \frac{t^2}{v}\right)^{-\frac{(v+1)}{2}} \quad \text{where, } t = \frac{\bar{X} - \mu}{S/\sqrt{n}}$$

$C$  = constant required to make the area under the curve unity,  
 $v = n - 1$ , the number of degrees of freedom.

The  $t$ -distribution has been derived mathematically under the hypothesis that parent population is distributed normally.

### 3. Properties of $t$ -distribution

- (i) As the normal curve, this curve also extends from  $-\infty$  to  $+\infty$ .
- (ii) The constant  $C$  depends upon the  $v$  (pronounced as 'nu'), the degrees of freedom.



### Applied Mathematics - IV

(9-2)

### Small Sample Tests

- (iii) Like the normal distribution, the  $t$ -distribution also is symmetrical and has a mean zero.
- (iv) The variance of  $t$ -distribution is greater than unity and approaches unity as the number of degrees of freedom and therefore the size of the sample becomes large.

1. Assumptions for  $t$ -test : (i) Samples are drawn from normal population and they are random.

(ii) For testing the equality of means of two populations their variances are assumed to be equal.

2.  $t$ -table : An interval estimate of the population mean is given by  $\bar{X} \pm t \sigma_{\bar{X}}$ . It should be noted that  $t$  table gives the probability that population parameter will not lie within the desired confidence interval i.e. the parameter will lie outside the confidence interval. For making an estimate, say, at 95% confidence level we consult the column under the head 0.05 (100% - 95% = 5% = 0.05) of the Table. Similarly for 98%, 99% confidence level we consult the column under the head 0.02 and 0.01.

3. Degree of freedom : Degree of freedom means the number of values we are free to choose. Suppose the sum of three numbers is 15. How many numbers we are free to choose such that the sum is 15? Certainly not all the three. We can choose two numbers at our will but the third will be given by 15 - (sum of the two chosen numbers). Thus, we are free to choose only two numbers. Hence, the degrees of freedom here are two.

4. Uses of  $t$ -distribution : The  $t$ -distribution has a wide number of applications. Some important of them are :

- (i) To estimate the population mean  $\mu$  from the sample mean  $\bar{X}$ .
- (ii) To test the hypothesis that the population mean is  $\mu$  with the help of the sample mean  $\bar{X}$ .
- (iii) To test the hypothesis that two populations have the same mean with the help of the sample means.

### 4. Distribution of Sample Mean

If  $\bar{X}$  is the sample mean and  $\mu$  is the population mean then

$$t = \frac{\bar{X} - \mu}{S/\sqrt{n}} \quad \text{where, } S^2 = \frac{\sum (X_i - \bar{X})^2}{n-1}$$

follows Student's  $t$ -distribution with  $n - 1$  degrees of freedom.

Remark ...

We know that the sample variance is given by

$$s^2 = \frac{\sum (X_i - \bar{X})^2}{n} \quad \therefore ns^2 = \sum (X_i - \bar{X})^2 = (n-1)S^2$$

$$\therefore \frac{S^2}{n-1} = \frac{s^2}{n-1} \quad \therefore \frac{S}{\sqrt{n-1}} = \frac{s}{\sqrt{n-1}}$$

$$\text{Hence, } t = \frac{\bar{X} - \mu_0}{S/\sqrt{n-1}} \quad \dots \quad (1) \quad \text{or} \quad t = \frac{\bar{X} - \mu_0}{s/\sqrt{n-1}} \quad \dots \quad (2)$$

We use (2) when sample standard deviation  $s$  is given and use (1) when sample values  $x_1, x_2, \dots, x_n$  are given or when  $S^2 = \sum (X_i - \bar{X})^2 / (n-1)$  is obtained or an unbiased estimates of standard deviation  $\sigma$  is given.

Thus, we have the following results when sample is small.

## For Small Samples

1. If the standard deviation  $\sigma$  of the parent population is known, then  $Z = \frac{\bar{X} - \mu}{\sigma/\sqrt{n}}$  is a S.N.V.
  2. If the standard deviation of the parent population is not known and the parent population is normal, then  $t = \frac{\bar{X} - \mu}{s/\sqrt{n}}$  is a  $t$ -distribution where  $s^2 = \frac{\sum (X_i - \bar{X})^2}{n-1}$ .
  3. If the standard deviation of the parent population is not known and if the parent population is normal, then  $t = \frac{\bar{X} - \mu}{s/\sqrt{n-1}}$  is a  $t$ -distribution where  $s^2 = \frac{\sum (X_i - \bar{X})^2}{n}$ .
- [ Note the cases (2) and (3) carefully.]

5. Testing the Hypothesis that the Population Mean is  $\mu$ .

To test the hypothesis that the population mean is  $\mu$  when the sample is small we follow the steps as for large sample but use the  $t$ -distribution instead of normal distribution and use the unbiased estimator  $s/\sqrt{n-1}$  of the standard deviation of the population and not  $s/\sqrt{n}$ .

**Example 1:** A soap manufacturing company was distributing a particular brand of soap through a large number of retail shops. Before a heavy advertisement campaign, the mean sales per week per shop was 140 dozens. After the campaign a sample of 26 shops was taken and the mean sale was found to be 147 dozens with standard deviation of 16. Can you consider the advertisement effective?

Sol.: (i) The null Hypothesis  $H_0 : \mu = 140$

Alternative Hypothesis  $H_a : \mu \neq 140$

(ii) Calculation of test statistic : Since the sample is small and S. D. of the population is not known, we use  $t$ -distributions.

$$t = \frac{\bar{X} - \mu}{s/\sqrt{n-1}} = \frac{147 - 140}{16/\sqrt{26-1}} = 2.19 \quad \therefore |t| = 2.19.$$

(iii) Level of significance :  $\alpha = 0.05$ .

(iv) Critical value : The value of  $t_{\alpha/2}$  for 5% level of significance and degrees of freedom  $v = 26 - 1 = 25$  from the table is  $t = 2.06$ .

(v) Decision : Since the computed value of  $|t| = 2.19$  is greater than the critical value  $t_{\alpha/2} = 2.06$  the null hypothesis is rejected.

$\therefore$  The advertisement may have changed the average sales.

**Example 2 :** A random sample of size 16 from a normal population showed a mean of 103.75 cm. and sum of squares of deviations from the mean 843.75 cm<sup>2</sup>. Can we say that the population has a mean of 108.75 cm?

Sol. : We first calculate sample standard deviation

$$s^2 = \frac{\sum (x_i - \bar{x})^2}{n} = \frac{843.75}{16} = 52.73$$

(i) The null hypothesis  $H_0 : \mu = 108.75$

Alternative hypothesis  $H_a : \mu \neq 108.75$

## Calculation of test statistic :

$$t = \frac{\bar{X} - \mu}{s/\sqrt{n-1}} = \frac{103.75 - 108.75}{\sqrt{52.73 / 15}} = -\frac{5}{1.875} = -2.67 \quad \therefore |t| = 2.67$$

(ii) Level of significance :  $\alpha = 0.05$ .

(iii) Critical value : The value of  $t_{\alpha/2}$  for 5% level of significance and degrees of freedom  $v = 16 - 1$

$= 15$  from the table is 2.131.

(iv) Decision : Since the computed value of  $|t| = 2.67$  is greater than the table value  $t_{\alpha/2} = 2.131$ , the null hypothesis is rejected.

$\therefore$  We cannot say that the population mean is 108.75.

**Example 3 :** Nine items of a sample had the following values

45, 47, 50, 52, 48, 47, 49, 53, 51

Does the mean of 9 items differ significantly from the assumed population mean 47.5?

(M.U. 2002, 10)

Sol. : We first calculate sample mean  $\bar{X}$  and sample standard deviation  $s^2$  (by assumed mean method).

Calculation of  $\bar{X}$  and  $s^2$ 

X	45	47	50	52	48	47	49	53	51	Sum
$d_i = x_i - 48$	-3	-1	2	4	0	-1	1	5	3	10
$d_i^2 = (x_i - 48)^2$	9	1	4	16	0	1	1	25	9	66

$$\bar{X} = a + \frac{\sum d_i}{n} = 48 + \frac{10}{9} = 49.11$$

$$\sum (X_i - \bar{X})^2 = \sum d_i^2 - \frac{(\sum d_i)^2}{n} = 66 - \frac{100}{9} = 54.89$$

$$\therefore s^2 = \frac{\sum (X_i - \bar{X})^2}{n} = \frac{54.89}{9} = 6.099$$

(i) The null hypothesis  $H_0 : \mu = 47.5$

Alternative hypothesis  $H_a : \mu \neq 47.5$

(ii) Calculation of test statistic : Since the sample size is small, we use  $t$ -distribution.

$$t = \frac{\bar{X} - \mu}{s/\sqrt{n-1}} = \frac{49.11 - 47.5}{\sqrt{6.099 / 8}} = 1.84 \quad \therefore |t| = 1.84$$

(iii) Level of significance :  $\alpha = 0.05$ .

(iv) Critical value : The value of  $t_{\alpha/2}$  at 5% level of significance for  $v = 9 - 1 = 8$  degrees of freedom is 2.306.

(v) Decision : Since the calculated value of  $|t| = 1.84$  is less than the table value  $t_{\alpha/2} = 2.306$ , the null hypothesis is accepted.

$\therefore$  The mean of nine items does not differ significantly from assumed population mean 47.5.

**Example 4 :** Ten individuals are chosen at random from a population and their heights are found to be 63, 63, 64, 65, 66, 69, 70, 70, 71 inches. Discuss the suggestion that the mean height of the universe is 65 inches. (M.U. 2003, 18, 19)

Sol.: We first calculate sample mean  $\bar{X}$  and sample standard deviation  $s^2$ .

Calculation of  $\bar{X}$  and  $s^2$ 

$X$	63	63	64	65	66	69	69	70	70	71	Sum
$d_i = x_i - 66$	-3	-3	-2	-1	0	3	3	4	4	5	10
$d_i^2 = (x_i - 66)^2$	9	9	4	1	0	9	9	16	16	25	98

$$\bar{X} = a + \frac{\sum d_i}{n} = 66 + \frac{10}{10} = 67$$

$$\sum (X_i - \bar{X})^2 = \sum d_i^2 - \frac{(\sum d_i)^2}{n} = 98 - \frac{100}{10} = 88$$

$$\therefore s^2 = \frac{\sum (X_i - \bar{X})^2}{n} = \frac{88}{10} = 8.8$$

(i) The null hypothesis  $H_0 : \mu = 65$

Alternative hypothesis  $H_a : \mu \neq 65$

(ii) Calculation of test statistic

$$t = \frac{\bar{X} - \mu}{s/\sqrt{n-1}} = \frac{67 - 65}{\sqrt{8.8}/\sqrt{9}} = \frac{6}{2.97} = 2.02 \quad \therefore |t| = 2.02.$$

(iii) Level of significance :  $\alpha = 0.05$ .

(iv) Critical value : The value of  $t_{\alpha}$  at 5% level of significance for  $v = 10 - 1 = 9$  degrees of freedom is 2.26.

(v) Decision : Since the calculated value of  $t = 2.02$  is less than the table value  $t_{\alpha} = 2.26$ , the null hypothesis is accepted.

∴ The mean height of the universe may be 65 inches.

**Example 5 :** Tests made on breaking strength of 10 pieces of a metal wire gave the following results.

578, 572, 570, 568, 572, 570, 570, 572, 596 and 584 in kgs.

Test if the breaking strength of the metal wire can be assumed to be 577 kg. ?

Sol.: First we calculate the mean and standard deviation  $s^2$  of the sample.

Calculation of  $\bar{X}$  and  $s^2$ 

$X$	578	572	570	568	572	570	570	572	596	584	Sum
$d_i = x_i - 580$	-2	-8	-10	-12	-8	-10	-10	-8	6	4	-48
$d_i^2 = (x_i - 580)^2$	4	64	100	144	64	100	100	64	256	16	864

$$\bar{X} = a + \frac{\sum d_i}{n} = 580 + \frac{48}{10} = 575.2$$

$$\sum (X_i - \bar{X})^2 = \sum d_i^2 - \frac{(\sum d_i)^2}{n} = 912 - \frac{(-48)^2}{10} = 633.6$$

$$\therefore s^2 = \frac{\sum (X_i - \bar{X})^2}{n} = \frac{633.6}{10} = 63.36$$

(i) The null hypothesis  $H_0 : \mu = 577$

Alternative hypothesis  $H_a : \mu \neq 577$

Calculation of test statistic

$$t = \frac{\bar{X} - \mu}{s/\sqrt{n-1}} = \frac{575.2 - 577}{\sqrt{63.36}/\sqrt{9}} = -0.65 \quad \therefore |t| = 0.65$$

(ii) Level of significance :  $\alpha = 0.05$ .

(iv) Critical value : The value of  $t_{\alpha}$  at 5% level of significance for  $v = 10 - 1 = 9$  degrees of freedom is 2.25.

(v) Decision : Since the calculated value of  $|t| = 0.65$  is less than the table value  $t_{\alpha} = 2.25$ , the null hypothesis is accepted.

∴ The mean is 577.

## EXERCISE - I

1. Vanaspati oil is marketed in tins of 10 kgs. A sample of 20 tins showed the mean weight as 9.5 kg. with standard deviation of 3 kgs. Does the sample justify the claim that the mean weight is 10 kg. Mention the level of significance, you use. [Ans. :  $t = 0.726$ , Yes at 5%]

2. A random sample of 18 observations has mean 103.75 cm. The sum of the squares of the deviations from the mean is 843.75 cm. Can this sample be regarded as coming from the population having 108.75 cm as the mean? ( $t_{15} = 2.131$  and  $t_{16} = 2.120$  at 5% level.)

(M.U. 2004) [Ans. :  $t = 2.67$ , No]

3. A machine is designed to pack edible oil in tins of 5 kgs. A random sample of 10 tins gave the average weight of a tin as 4.8 kg. and standard deviation of 2 kgs. Is the machine working properly ? Value of  $t$  for 9 degrees of freedom at 5% level of significance is 2.262. [Ans. :  $t = 3$ , No]

4. A company supplies tooth-paste in a packing of 100 gm. A sample of 10 packings gave the following weights in gms.

100.5, 100.3, 100.1, 99.8, 99.7, 99.7, 100.3, 100.4, 99.2, 99.3.

Does the sample support the claim of the company that the packing weighs 100 gms ?

[Ans. :  $\bar{X} = 99.93$ ,  $s^2 = 0.2112$ ,  $t = 0.48$ , Yes]

5. A machine is designed to produce insulating washers for electrical devices of average thickness of 0.025 cms. A random sample of 10 washers was found to have average thickness of 0.024 cms., with standard deviation of 0.002 cms. Test the significance of the deviation. (M.U. 2004) [Ans. :  $|t| = 1.5$ ; Accept  $H_0$ ]

6. A certain drug administered to 12 patients resulted in the following change in their Blood Pressure.

5, 2, 8, -1, 3, 0, 6, -2, 1, 5, 0, 4

Can we conclude that the drug increases the blood pressure ? (M.U. 2005, 09, 10, 14)

[Ans. :  $t = 2.89$ , One tailed test  $\bar{X} > \mu$  is to be accepted. There is increase in B.P.]

**6. Testing the Difference Between Means**

We have seen how to test the difference between the means of two samples when they are large. We shall now see how to test the difference between the means of two samples when the samples are small.

**(a) Case I : Independent Samples**

If the sample size ( $n_1 + n_2 - 2$ ) is small, an unbiased estimate of the common population standard deviation  $\sigma$  is obtained by pooling the data with the help of the following formula.

$$s_p = \sqrt{\frac{\sum (x_{ij} - \bar{x}_1)^2 + \sum (x_{ij} - \bar{x}_2)^2}{n_1 + n_2 - 2}} \quad (1)$$

If we are given unbiased standard deviations of the two samples,

$$S_1 = \sqrt{\frac{\sum (x_{ij} - \bar{x}_1)^2}{n_1 - 1}} \quad \text{and} \quad S_2 = \sqrt{\frac{\sum (x_{ij} - \bar{x}_2)^2}{n_2 - 1}}$$

then, we get, from (1)

$$s_p = \sqrt{\frac{(n_1 - 1) S_1^2 + (n_2 - 1) S_2^2}{n_1 + n_2 - 2}} \quad (2)$$

On the other hand, if we are given standard deviations of the two samples

$$s_1 = \sqrt{\frac{\sum (x_{ij} - \bar{x}_1)^2}{n_1}} \quad \text{and} \quad s_2 = \sqrt{\frac{\sum (x_{ij} - \bar{x}_2)^2}{n_2}}$$

then, we get, from (1)

$$s_p = \sqrt{\frac{n_1 s_1^2 + n_2 s_2^2}{n_1 + n_2 - 2}} \quad (3)$$

The standard error of the difference between the two means is then given by

$$\text{S.E.} = s_p \times \sqrt{\frac{1}{n_1} + \frac{1}{n_2}}$$

The test statistic is then computed as

$$t = \frac{\bar{x}_1 - \bar{x}_2}{\text{S.E.}}$$

The statistic  $t$  so computed follows Student's  $t$ -distribution.

Note ...

It is assumed that the two populations have the same standard deviation  $\sigma$ . If we cannot assume that  $\sigma_1 = \sigma_2$ , then the problem is beyond the scope of this book.

**Example 1 :** If two independent random samples of sizes 15 and 8 have respectively the following means and population standard deviations,

$$\begin{aligned} \bar{x}_1 &= 980 & \bar{x}_2 &= 1012 \\ \sigma_1 &= 75 & \sigma_2 &= 80 \end{aligned}$$

Test the hypothesis that  $\mu_1 = \mu_2$  at 5% level of significance.

(Assume the population to be normal.)

(M.U. 2016)

Sol. : When population standard deviations  $\sigma_1$  and  $\sigma_2$  are known, we can assume  $\bar{x}_1 - \bar{x}_2$  to be normal with mean zero and S.E. =  $\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}$  and hence, use Z-distribution. (See page 8-13).

**(i) Null Hypothesis  $H_0 : \mu_1 = \mu_2$** **Alternative Hypothesis  $\mu_1 \neq \mu_2$** **(ii) Calculation of test statistic :**

$$\begin{aligned} \text{S.E.} &= \sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}} = \sqrt{\frac{75^2}{15} + \frac{80^2}{8}} = \sqrt{375 + 800} = \sqrt{1175} = 34.28 \\ \therefore z &= \frac{\bar{x}_1 - \bar{x}_2}{\text{S.E.}} = \frac{980 - 1012}{34.28} = -0.93 \quad \therefore |z| = 0.93 \end{aligned}$$

**(iii) Level of significance :  $\alpha = 0.05$** **(iv) Critical value :** The table value of  $z$  at  $\alpha = 0.05$  is  $z_{\alpha/2} = 1.96$ .

(We use Z-test because we have assumed the population to be normal and population S.D. is known. See table on page 8-6.)

**(v) Decision :** Since the computed value  $|z| = 0.93$  is less than the table value 1.96, the hypothesis is accepted.

$\therefore$  The population means are equal  $\mu_1 = \mu_2$ .

**Example 2 :** A sample of 8 students of 16 years each shown up a mean systolic blood pressure of 118.4 mm of Hg with S.D. of 12.17 mm. While a sample of 10 students of 17 years each showed the mean systolic B.P. of 121.0 mm with S.D. of 12.68 during an investigation. The investigator feels that the systolic B.P. is related to age.

Do you think that the data provides enough reasons to support investigator's feeling at 5% LOS? (Assume the distribution of systolic B.P. to be normal.)

(M.U. 2014)

Sol. : We are given  $n_1 = 8$ ,  $n_2 = 10$ ;  $\bar{x}_1 = 118.4$ ,  $\bar{x}_2 = 121.0$ ;  $s_1 = 12.17$ ,  $s_2 = 12.68$ .

**(i) Null Hypothesis  $H_0 : \mu_1 = \mu_2$** **Alternative Hypothesis  $\mu_1 \neq \mu_2$** **(ii) Calculation of test statistic :**

$$s_p = \sqrt{\frac{n_1 s_1^2 + n_2 s_2^2}{n_1 + n_2 - 2}} = \sqrt{\frac{8(12.17)^2 + 10(12.68)^2}{8 + 10 - 2}}$$

$$\therefore s_p = \sqrt{\frac{1184+87+1658+94}{16}} = 13.33$$

$$\text{S.E.} = s_p \sqrt{\frac{1}{n_1} + \frac{1}{n_2}} = 13.33 \sqrt{\frac{1}{8} + \frac{1}{10}} = 6.32$$

$$t = \frac{\bar{x}_1 - \bar{x}_2}{\text{S.E.}} = \frac{118.4 - 121.0}{6.32} = -0.41 \quad \therefore |t| = 0.41$$

- (iii) Level of significance :  $\alpha = 0.05$   
 (iv) Critical value : The table value of  $t$  at  $\alpha = 0.05$  for  $v = 8 + 7 - 2 = 13$  d.f.  
 (v) Decision : Since the computed value  $|t| = 0.41$  is less than the table value  $t_{0.05} = 2.12$ , the hypothesis is accepted.  $\mu_1 = \mu_2$   
 (Although the population is normal, since the population S.D. is not known, we use  $t$ -test. See table on page 8-6.)

**Example 3 :** The means of two random samples of size 9 and 7 are 196.42 and 198.92 respectively. The sum of the squares of the deviations from the means are 26.94 and 18.73 respectively. Can the samples be considered to have been drawn from the same population?

Sol. (i) Null Hypothesis  $H_0 : \mu_1 = \mu_2$

Alternative Hypothesis  $H_a : \mu_1 \neq \mu_2$

(ii) Calculations of test statistic : Unbiased estimate of common population standard deviation is

$$s_p = \sqrt{\frac{\sum (X_i - \bar{X})^2 + \sum (Y_i - \bar{Y})^2}{n_1 + n_2 - 2}} = \sqrt{\frac{26.94 + 18.73}{9 + 7 - 2}} = \sqrt{\frac{45.67}{14}} = 1.81$$

Standard error of the difference between the means

$$S.E. = s_p \times \sqrt{\frac{1}{n_1} + \frac{1}{n_2}} = 1.81 \sqrt{\frac{1}{9} + \frac{1}{7}} = 0.91$$

$$\therefore t = \frac{\bar{X}_1 - \bar{X}_2}{S.E.} = \frac{196.42 - 198.92}{0.91} = -2.64 \quad \therefore |t| = 2.64$$

(iii) Level of significance :  $\alpha = 0.05$ ,

(iv) Critical value : The table value of  $t$  at  $\alpha = 0.05$  for  $v = 9 + 7 - 2 = 14$  degrees of freedom is 2.145.

(v) Decision : Since the computed value of  $|t| = 2.64$  is greater than the table value  $t_{0.05} = 2.145$ , the null hypothesis is rejected.  
 ∴ The samples cannot be considered to have been drawn from the same population.

**Example 4 :** Six guinea pigs injected with 0.5 mg. of a medication took on an average 15.4 secs. to fall asleep with an unbiased standard deviation 2.2 secs., while six other guinea pigs injected with 1.5 mg. of the medication took on an average 11.2 secs. to fall asleep with an unbiased standard deviation 2.6 cms. Use 5% level of significance to test the null hypothesis that the difference in dosage has no effect.

Sol. We have  $\bar{X}_1 = 15.4$ ,  $\bar{X}_2 = 11.2$ ,  $S_1 = 2.2$ ,  $S_2 = 2.6$ ,  $n_1 = 6$ ,  $n_2 = 6$ .

(i) Null Hypothesis  $H_0 : \mu_1 = \mu_2$

Alternative Hypothesis  $H_a : \mu_1 \neq \mu_2$

(ii) Calculation of test statistic : We are given unbiased standard deviations.  
 ∴ The unbiased estimate of the common population is given by

$$s_p = \sqrt{\frac{(n_1 - 1)S_1^2 + (n_2 - 1)S_2^2}{n_1 + n_2 - 2}} = \sqrt{\frac{5 \times (2.2^2) + 5 \times (2.6^2)}{6 + 6 - 2}}$$

$$\therefore s_p = \sqrt{\frac{56}{10}} = \sqrt{5.6} = 2.408$$

The standard error of the difference between the two means is given by

$$S.E. = s_p \times \sqrt{\frac{1}{n_1} + \frac{1}{n_2}} = 2.408 \times \sqrt{\frac{1}{6} + \frac{1}{6}} = 1.39$$

$$\therefore t = \frac{\bar{X}_1 - \bar{X}_2}{S.E.} = \frac{15.4 - 11.2}{1.39} = 3.02 \quad \therefore |t| = 3.02$$

- (iii) Level of significance :  $\alpha = 0.05$ ,  
 (iv) Critical values : The table value of  $t$  at  $\alpha = 0.05$  for  $v = 6 + 6 - 2 = 10$  degrees of freedom is  $t_{0.05} = 2.228$ ,  
 (v) Decision : Since the computed value of  $|t| = 3.02$  is greater than the table value  $t_{0.05} = 2.228$  the null hypothesis is rejected.  
 ∴ The difference is significant.

**Example 5 :** Samples of two types of electric bulbs were tested for length of life and the following data were obtained.

	Type I	Type II
No. of samples	8	7
Mean of the samples (in hours)	1134	1024
Standard deviation (in hours)	35	40

Test at 5% level of significance whether the difference in the sample means is significant.  
 (Table value of  $t$  for 13 d.f. is 2.16, for 14 d.f. is 2.15 and for 15 d.f. is 2.13). (M.U. 2004, 06)

Sol. We have  $\bar{X}_1 = 1134$ ,  $\bar{X}_2 = 1024$ ,  $s_1 = 35$ ,  $s_2 = 40$ ,  $n_1 = 8$ ,  $n_2 = 7$ .

(i) Null Hypothesis  $H_0 : \mu_1 = \mu_2$

Alternative Hypothesis  $H_a : \mu_1 \neq \mu_2$

(ii) Calculation of test statistic : Since the sizes of the samples are small we use  $t$ -distribution. The unbiased estimate of the common population is given by

$$s_p = \sqrt{\frac{n_1 S_1^2 + n_2 S_2^2}{n_1 + n_2 - 2}} = \sqrt{\frac{8 \times 35^2 + 7 \times 40^2}{8 + 7 - 2}} = \sqrt{\frac{21000}{13}} = \sqrt{1615.38} = 40.19$$

The standard error of the difference between the two means is given by

$$S.E. = s_p \times \sqrt{\frac{1}{n_1} + \frac{1}{n_2}} = 40.19 \sqrt{\frac{1}{8} + \frac{1}{7}} = 20.8$$

$$\therefore t = \frac{\bar{X}_1 - \bar{X}_2}{S.E.} = \frac{1134 - 1024}{20.8} = \frac{110}{20.8} = 5.388 \quad \therefore |t| = 5.388$$

(iii) Level of significance :  $\alpha = 0.05$ ,

(iv) Critical value : The table value of  $t$  at  $\alpha = 0.05$  for  $v = 8 + 7 - 2 = 13$  degrees of freedom is  $t_{0.05} = 2.16$ .

(v) Decision : Since the computed value  $|t| = 5.388$  is greater than the table value  $t_{0.05} = 2.16$ , the hypothesis is rejected.

∴ The difference is significant.

**Example 6 :** The heights of six randomly chosen sailors are in inches : 63, 65, 68, 69, 70, 71, 72 and 73. The heights of ten randomly chosen soldiers are : 61, 62, 65, 66, 69, 69, 70, 71, 72 and 73. Discuss in the light that these data throw on the suggestion that the soldiers on an average are taller than sailors.

**Sol. :** We first calculate the mean and standard deviation of the heights of both sailors and soldiers.

Sailors			Soldiers		
Height $X_1$	$d_i$ $(x_i - \bar{x}_1)$	$d_i^2$ $(x_i - \bar{x}_1)^2$	Height $X_2$	$d_i$ $(x_i - \bar{x}_2)$	$d_i^2$ $(x_i - \bar{x}_2)^2$
63	-5	25	61	-6.8	46.24
65	-3	9	62	-5.8	33.64
68	0	0	65	-2.8	7.84
69	1	1	66	-1.8	3.24
71	3	9	69	1.2	1.44
72	4	16	69	1.2	1.44
			70	2.2	4.84
			71	3.2	10.24
			72	4.2	17.64
			73	5.2	27.04
$\Sigma x_1$	0	$\Sigma (x_1 - \bar{x}_1)^2$ = 60	$\Sigma x_2$	0	$\Sigma (x_2 - \bar{x}_2)^2$ = 163.60
= 408			= 678		

$$\text{Now, } \bar{X}_1 = \frac{\sum \bar{X}_1}{N} = \frac{408}{6} = 68, \bar{X}_2 = \frac{\sum X_2}{N} = \frac{678}{10} = 67.8$$

The unbiased estimate of the common population

$$s_p = \sqrt{\frac{\sum (X_1 - \bar{X}_1)^2 + \sum (X_2 - \bar{X}_2)^2}{n_1 + n_2 - 2}} = \sqrt{\frac{60 + 153.60}{6 + 10 - 2}} = \sqrt{\frac{213.6}{14}} = \sqrt{15.26} = 3.9$$

(i) Null Hypothesis  $H_0 : \mu_1 = \mu_2$

Alternative Hypothesis  $H_a : \mu_1 \neq \mu_2$

(ii) Calculation of test statistic

$$t = \frac{\bar{X}_1 - \bar{X}_2}{S.E.}, \quad \text{Now, } \bar{X}_1 = 68, \bar{X}_2 = 67.8$$

$$\therefore S.E. = s_p \times \sqrt{\frac{1}{n_1} + \frac{1}{n_2}} = 3.9 \times \sqrt{\frac{1}{6} + \frac{1}{10}} = 2.014$$

$$\therefore t = \frac{\bar{X}_1 - \bar{X}_2}{S.E.} = \frac{68 - 67.8}{2.014} = 0.099$$

(iii) Level of significance :  $\alpha = 0.05$ ,

(iv) Critical value : The table value of  $t$  at  $\alpha = 0.05$  for  $v = 6 + 10 - 2 = 14$  degrees of freedom is  $t_c = 2.145$ .

(v) Decision : Since the computed value  $|t| = 0.099$  is smaller than the table value  $t_c = 2.145$ , the hypothesis is accepted.

$\therefore$  The means are equal i.e. the suggestion that the soldiers on the average are taller than sailors cannot be accepted.

**EXERCISE - II**

1. Two independent samples of sizes 8 and 7 gave the following results.

Sample 1 : 19, 17, 15, 21, 16, 18, 16, 14

Sample 2 : 15, 14, 15, 19, 15, 18, 16

Is the difference between sample means significant ?

[ Ans. :  $\bar{X}_1 = 17, \bar{X}_2 = 16, s_1 = 2.12, s_2 = 1.69$ , (M.U. 2003, 04, 14) ]

$$s_p = \sqrt{\frac{n_1 s_1^2 + n_2 s_2^2}{n_1 + n_2 - 2}}, \quad S.E. = s_p \times \sqrt{\frac{1}{n_1} + \frac{1}{n_2}} = 1.073$$

$\therefore t = 0.93$ . Accept  $H_0$

2. The mean and standard deviation of heights of 8 randomly chosen soldiers are 166.9 cms. and 8.29 cms. respectively. The corresponding values for 8 randomly chosen sailors are 170.3 cms. and 8.5 cms. respectively. Based on this data can we conclude that the soldiers, in general, are shorter than the sailors ? Find 95% confidence limits for the statistic used. (M.U. 2006)

[ Ans. :  $|t| = 0.8967$ , No ]

3. Two independent random samples of sizes 8 and 10 have the means 950 and 1000. The standard deviations of the two populations are 80 and 100. Test the hypothesis that the populations have the same mean.

[ Ans. :  $|z| = 1.178$ , Accepted ]

4. Two independent random sample have the following data

$$\bar{X}_1 = 110, \sigma_1 = 25, n_1 = 16$$

$$\bar{X}_2 = 120, \sigma_2 = 30, n_2 = 9$$

If  $\sigma_1$  and  $\sigma_2$  are the standard deviations of the populations. Test the hypothesis that  $\mu_1 = \mu_2$  at 5% level of significance. (State the assumption you make if any.)

[ Ans. :  $|z| = 0.848$ , Accepted ]

5. Samples of electric tubes of two companies were tested for lengths of their life and the following information was obtained,

No. of sample	Company A	Company B
Mean life (in hrs.)	1210	1314
Standard deviation (in hrs.)	36	42

Test at 5% level of significance whether the difference in the sample means is significant. (Table value of  $t$  for  $v = 13$  is 2.16, for  $v = 14$  is 2.15 and for  $v = 15$  is 2.13)

[ Ans. :  $|t| = 4.81$ , Reject ]

6. A medicine was found to be effective for 9 patients in 8 days on an average with standard deviation of 2.2 days. Another medicine administered to another group of 8 patients was found to be effective in 6 days on an average with standard deviation of 2.6 days. Use 5% level of significance to test the null hypothesis that the two medicines are equally effective.

[ Ans. :  $|t| = 1.614$ , Accept ]

7. Two types of anti-biotics were tested on two groups of patients for curing a particular disease and the following data were obtained.

	Type A	Type B
No. of patients	6	6
Mean period (in days)	13.55	10.10
Unbiased standard deviation (in days)	3.2	2.8

Use 5% level of significance to test the null hypothesis that the difference in the mean period of the two drugs is significant.

8. Two kinds of manures were used in seventeen plots of the same size other conditions being the same. The yields in quintals are given below.

Manure I : 35, 42, 40, 42, 34, 24, 42.

Manure II : 34, 44, 32, 40, 52, 41, 50, 40, 42, 45.

Test at 5% level of significance whether the two manures differ as regards their mean yield. (Table value of  $t$  at 5% level of significance for 15 degrees of freedom is 2.131).

[Ans. :  $|t| = 1.68$ . Difference is not significant]

9. The following are the gain in weights of cows fed on two types of diets X and Y.

Diet X : 30, 37, 35, 37, 29, 19, 37.

Diet Y : 29, 39, 27, 35, 47, 37, 45, 35, 37, 40.

Test at 5% level of significance whether the two diets differ as regards their effect on mean increase in weight. (Table value of  $t$  for 15 degrees of freedom at 5% level of significance is 2.131).

[Ans. :  $|t| = 1.62$ . Do not differ]

10. The means of two random samples of size 9 and 7 are 196 and 199 respectively. The sum of the squares of the deviations from the mean are 27 and 19 respectively. Can the samples be regarded to have been drawn from the same normal population?

[Ans. :  $|t| = 3.30$ , No]

#### (b) Case II : Samples not independent

In the previous test it was assumed that the two samples were independent. For example, guinea pigs to which sleeping drugs were administered in the two groups were different. The cows fed on two diets were different. The plots on which two different manures were used were different. But in some cases the samples may not be different. We may test the effectiveness of a drug on the same group of persons. We may test the effectiveness of coaching on the same batch of students. In such cases the sample is the same for two tests. The samples are not independent and the above formula for testing of hypothesis cannot be used. In such cases we calculate the  $t$ -statistic as explained below.

We first find the differences of the corresponding values of the two sets of data then find the mean difference  $\bar{X}$  and standard deviation of the differences  $s$ . We then define

$$t = \frac{\bar{X} - \mu}{s/\sqrt{n-1}} = \frac{\bar{X} - 0}{s/\sqrt{n-1}} \quad \text{or} \quad t = \frac{\bar{X} - \mu}{S/\sqrt{n}} = \frac{\bar{X}}{S/\sqrt{n}}$$

where,  $\mu = 0$  is the null hypothesis,  $s$  = S.D. of the sample,  
 $S$  = unbiased estimator of  $\sigma$ .

Note ...

Taking the null hypothesis  $\mu = 0$  for differences amounts to the null hypothesis of equality of means  $\mu_1 = \mu_2$  of the two populations.

Example 1 : A certain injection administered to 12 patients resulted in the following changes of blood pressure :

5, 2, 8, -1, 3, 0, 6, -2, 1, 5, 0, 4

Can it be concluded that the injection will be in general accompanied by an increase in blood pressure?

Sol. : We first calculate  $\bar{X}$  and  $s^2$ .

#### Calculation of $\bar{X}$ and $s^2$

X	5	2	8	-1	3	0	6	-2	1	5	0	4
$d_i = x_i - 2$	3	0	6	-3	1	-2	4	-4	-1	3	-2	2
$d_i^2 = (x_i - 2)^2$	9	0	36	9	1	4	16	16	1	9	4	4

$$\bar{X} = a + \frac{\sum d_i}{n} = 2 + \frac{7}{12} = 2.58$$

$$\sum (X_i - \bar{X})^2 = \sum d_i^2 - \frac{(\sum d_i)^2}{n} = 109 - \frac{49}{12} = 104.92$$

$$\therefore s^2 = \frac{\sum (X_i - \bar{X})^2}{n} = \frac{104.92}{12} = 8.74$$

i) The null hypothesis  $H_0 : \mu = 0$

Alternative hypothesis  $H_a : \mu \neq 0$

ii) Calculation of test statistic : Since the sample size is small, we use student's  $t$ -distribution.

$$t = \frac{\bar{X} - \mu}{s/\sqrt{n-1}} = \frac{2.58 - 0}{\sqrt{8.74}/\sqrt{11}} = 2.89 \quad \therefore |t| = 2.89$$

iii) Level of significance :  $\alpha = 0.05$ .

iv) Critical value : The value of  $t_{\alpha/2}$  at 5% level of significance for  $v = 12 - 1 = 11$  degrees of freedom = 2.201.

v) Decision : Since the calculated value of  $t = 2.89$  is greater than the critical value  $t_{\alpha/2} = 2.201$ , the hypothesis is rejected.

∴ There is rise in B.P.

Example 2 : Ten school boys were given a test in Statistics and their scores were recorded. They were given a months special coaching and a second test was given to them in the same subject at the end of the coaching period. Test if the marks given below give evidence to the fact that the students are benefitted by coaching.

Marks in Test I : 70, 68, 56, 75, 80, 90, 68, 75, 56, 58.

Marks in Test II : 68, 70, 52, 73, 75, 78, 80, 92, 54, 55.

(M.U. 2004)

Sol. : We first calculate the differences between marks in test II and marks in test I =  $X$  and from these we calculate  $\bar{X}$  and  $s^2$ .

Calculation of  $\bar{X}$  and  $s^2$ 

$X$	-2	2	-4	-2	-5	-12	12	17	-2	-3
$d_1 = x_i - 2$	-4	0	-6	-4	-7	-14	10	15	-4	-5
$d_1^2 = (x_i - 2)^2$	16	0	36	16	49	196	100	225	16	25

$$\bar{X} = a + \frac{\sum d_1}{n} = 2 + \left( -\frac{19}{10} \right) = 0.1$$

$$\begin{aligned} \sum (X_i - \bar{X})^2 &= \sum d_1^2 - \frac{(\sum d_1)^2}{n} \\ &= 679 - \frac{0.01}{10} = 678.999 \end{aligned}$$

$$s^2 = \frac{\sum (X_i - \bar{X})^2}{n} = 67.90$$

(i) The null hypothesis  $H_0 : \mu = 0$

Alternative hypothesis  $H_a : \mu \neq 0$

(ii) Calculation of test statistic : Since the sample size is small, we use students t-distribution.

$$t = \frac{\bar{X} - \mu}{s / \sqrt{n-1}} = \frac{0.1 - 0}{\sqrt{67.90 / 9}} = 0.036$$

$$\therefore |t| = 0.036.$$

(iii) Level of significance :  $\alpha = 0.05$ .

(iv) Critical value : The value of  $t_{\alpha/2}$  at 5% level of significance for  $v = 10 - 1 = 9$  degrees of freedom = 2.262.

(v) Decision : Since the calculated value of  $|t| = 0.036$  is less than the critical value  $t_{\alpha/2} = 2.262$ , the hypothesis is accepted.

$\therefore$  The students are not benefitted by coaching.

**Example 3 :** In a certain experiment to compare two types of pig-foods A and B, the following results of increasing weights were obtained.

Pig Number	: 1 2 3 4 5 6 7 8
Increase in weight X kg by A	: 49 53 51 52 47 50 52 53
Increase in weight Y kg by B	: 52 55 52 53 50 54 54 53

(i) Assuming that the two sample of pigs are independent, can we conclude that food B is better than food A.

(ii) Examine the case if the same set of pigs were used in both the cases.

(M.U. 2004, 08)

Sol. : (a) We first calculate  $\bar{X}_1$  and  $\bar{X}_2$ .

Calculation of  $\bar{X}_1$  and  $\bar{X}_2$  etc.

Food A			Food B		
$X_1$	$d_1 = x_1 - 51$	$d_1^2 = (x_1 - 51)^2$	$X_2$	$d_2 = x_2 - 53$	$d_2^2 = (x_2 - 53)^2$
49	-2	4	52	-1	1
53	2	4	55	2	4
51	0	0	52	-1	1
52	1	1	43	0	0
47	-4	16	50	-3	9
50	-1	1	54	1	1
52	1	1	54	1	1
53	2	4	53	0	0
	-1	31		-1	17

$$\bar{X}_1 = a + \frac{\sum d_1}{n} = 51 + \frac{-1}{8} = 50.875$$

$$\sum (X_1 - \bar{X}_1)^2 = \sum d_1^2 - \frac{(\sum d_1)^2}{n} = 31 - \frac{(-1)^2}{8} = 30.875$$

$$\text{and } \bar{X}_2 = a + \frac{\sum d_2}{n} = 53 - \frac{1}{8} = 52.875$$

$$\sum (X_2 - \bar{X}_2)^2 = \sum d_2^2 - \frac{(\sum d_2)^2}{n} = 17 - \frac{(-1)^2}{8} = 16.875$$

(i) The null hypothesis  $H_0 : \mu_1 = \mu_2$

Alternative hypothesis  $H_a : \mu_1 \neq \mu_2$

(ii) Calculation of test statistic

$$s_p = \sqrt{\frac{\sum (X_1 - \bar{X}_1)^2 + \sum (X_2 - \bar{X}_2)^2}{n_1 + n_2 - 2}} = \sqrt{\frac{30.875 + 16.875}{8 + 8 - 2}} = \sqrt{3.41}$$

$$\text{S.E.} = s_p \times \sqrt{\frac{1}{n_1} + \frac{1}{n_2}} = \sqrt{3.41} \times \sqrt{\frac{1}{8} + \frac{1}{8}} = 0.92$$

$$\therefore t = \frac{\bar{X}_1 - \bar{X}_2}{\text{S.E.}} = \frac{50.875 - 52.875}{0.92} = -2.17 \quad \therefore |t| = 2.17$$

(iii) Level of significance :  $\alpha = 0.05$ .

(iv) Critical value : The value of  $t$  at  $\alpha = 0.05$  for  $v = 8 + 8 - 2 = 14$  degrees of freedom = 2.145.

(v) Decision : Since computed value  $t = 2.17$  is greater than the table value  $t_{\alpha/2} = 2.145$ , the hypothesis is rejected at 5% level of significance.

$\therefore$  Food B is superior to food A.

(b) If the same set of pigs were used in the two tests : We first calculate the differences between the weights in the two tests and from these we calculate  $\bar{X}$  and  $s^2$ .

Calculation of  $\bar{X}$  and  $s^2$ 

$X_i$	49	53	51	52	47	50	52	53	Total
$X_j$	52	55	52	53	50	54	54	53	
$X$	-3	-2	-1	-1	-3	-4	-2	0	
$d_i = X_i - 2$	-5	-4	-3	-3	-5	-6	-3	-2	-32
$d_i^2 = (X_i - 2)^2$	25	16	9	9	25	36	16	4	140

$$\bar{X} = \mu + \frac{\sum d_i}{n} = 2 - \frac{32}{8} = -2$$

$$\Sigma (X_i - \bar{X})^2 = \Sigma d_i^2 - \frac{(\sum d_i)^2}{n} = 140 - \frac{(-32)^2}{8} = 12$$

$$\therefore s^2 = \frac{\Sigma (X_i - \bar{X})^2}{n} = \frac{12}{8} = 1.5$$

(i) The null hypothesis  $H_0 : \mu = 0$

Alternative hypothesis  $H_a : \mu \neq 0$

(ii) Calculation of test statistic

$$t = \frac{\bar{X} - \mu}{s/\sqrt{n-1}} = \frac{-2 - 0}{\sqrt{1.5/7}} = -4.32 \quad \therefore |t| = 4.32$$

(iii) Level of significance :  $\alpha = 0.05$ .

(iv) Critical value : The value of  $t_{\alpha/2}$  at 5% level of significance for  $v = 8 - 1 = 7$  degrees of freedom = 2.365.

(v) Decision : Since the calculated value of  $t = 4.32$  is greater than the critical value  $t_{\alpha/2} = 2.365$ , the hypothesis is rejected.

$\therefore$  Food B is superior to Food A.

**EXERCISE - III**

1. A drug was administered to 5 persons and the systolic blood pressure before and after was measured. The results are given below

Candidates : I, II, III, IV, V.  
B.P. before : 140, 130, 132, 150, 140  
B.P. after : 132, 126, 133, 144, 133.

Test whether the drug is effective in lowering the systolic blood pressure.

(M.U. 2007, 09) [Ans. :  $|t| = 3$ . Accept  $\mu_1 = \mu_2$ . The drug is not effective.]

2. A drug was administered to 10 patients and the changes in the sugar content in the blood was recorded as under 10, 8, -6, -4, 2, -8, 6, -5, -3, -6. Is it reasonable to believe that the drug has no effect on change of sugar? (Use 5% level of  $t$ . For 9 d.f.,  $t = 2.262$ .)

[Ans. :  $|t| = 0.289$ . Accept  $\mu_1 = \mu_2$ . Drug has no effect.]

3. Ten accountants were given intensive coaching and tests were conducted before and after coaching. The scores of tests are given below.

Sr. No. : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

Marks in test before coaching : 50, 42, 51, 42, 60, 41, 70, 55, 62, 38.

Marks in test after coaching : 62, 40, 61, 52, 68, 51, 64, 63, 72, 50.

Does the score show an improvement? Test at 5% level of significance. (The value of  $t$  for  $v = 9$  at 5% level for one tail test is 1.8333 and for two tail test is 2.262).

[Ans. :  $|t| = 3.72$ . Reject  $\mu_1 = \mu_2$ . There is improvement.]

4. Ten students were given intensive coaching for a month in Statistics. The scores obtained in tests are given below.

Sr. No. : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

Marks in 1<sup>st</sup> test : 50, 52, 53, 60, 65, 67, 48, 69, 72, 80.

Marks in 2<sup>nd</sup> test : 65, 55, 65, 65, 60, 67, 49, 82, 74, 86.

Does the score from test 1 to test 2 shows an improvement? Test at 5% level of significance. (The value of  $t$  for 9 d.f. at 5% level of significance is 1.833 for one tailed test and 2.262 for two tailed test.)

[Ans. :  $t = -2.57 < -1.833$  for one tailed test.  $t$  falls in rejection area. Hypothesis  $\mu_1 = \mu_2$  is rejected for one tailed test. Coaching is effective.]

5. The sales-data of an item in six shops before and after a special promotional campaign are as under.

Shops	A	B	C	D	E	F
Before campaign	53	28	31	48	50	42
After campaign	58	29	30	55	56	45

Can the campaign be judged to be a success at 5% level of significance?

(Use one tailed test.)

[Ans. :  $|t| = 3.14$ , Yes]

6. The following data relates to the marks obtained by 11 students in two tests, one held at the beginning of the year and the other at the end of the year after giving intensive coaching.

Test I : 19 23 16 24 17 18 20 18 21 19 20

Test II : 17 24 20 24 20 22 20 20 18 22 18

Do the data indicate that the students are benefited by coaching?

(M.U. 2004)

[Ans. :  $|t| = 1.20$ , No]

7. The following data represent the marks obtained by 12 students in 2 tests, one held before coaching and the other after coaching.

Test I : 55 60 65 75 49 25 18 30 35 51 61 72

Test II : 63 70 70 81 54 29 21 38 32 50 70 80

Do the data indicate that the coaching was effective in improving the performance of the students?

(M.U. 2004) [Ans. :  $t = 4$ , Yes]

8. An I.Q. test was administered to 5 persons before and after training. The results are given below.

	1	2	3	4	5
I.Q. Before Training	110	120	123	132	125
I.Q. After Training	120	118	125	136	121

Test whether there is any change in I.Q. after training programme. Use 1% level of significance. (M.U. 2006)

(Ans.:  $|t| = 0.82$ )

The value of  $t$  for  $v = 4$  at 1% level of significance = 4.6.  $H_0$  accepted.)

### 7. Non-parametric Tests

So far we have dealt with the problems of testing an hypothesis about a parameter. Such tests which deal with the parameter of the population are called parametric tests.

On the other hand tests which do not deal with the parameter are called non-parametric tests. One such test, which we are going to study is  $\chi^2$ -test (pronounced as 'ki' square test - 'ki' as in kite).

### 8. Definition of $\chi^2$

Suppose we are given a die and we want to know whether it is biased or unbiased. Or suppose in a cholera epidemic we inoculate a group and we want to know whether inoculation is effective in preventing the attack of cholera. In such situations Chi-square test is used to test the hypothesis e.g. the die is not biased or the inoculation is not effective.  $\chi^2$  is calculated on the assumption of status-quo i.e. there is no change.

To test such a hypothesis we toss the die for say, 138 times and observe how many times we got 1, 2, 3, 4, 5, 6. These are observed frequencies  $O$ . We can calculate expected frequencies of 1, 2, 3, 4, 5, 6 in 138 tosses. These are expected frequencies  $E$ . Then we find the value of Chi-square from the following.

The statistic  $\chi^2$ -pronounced as ki-square (ki as in 'kite') and first used by Karl Pearson is defined by

$$\chi^2 = \sum \left( \frac{(O - E)^2}{E} \right)$$

where,  $O$  = observed frequency,  $E$  = expected frequency.

We calculate expected frequencies on certain assumptions such as (i) the coin or a die is unbiased, (ii) there is no association between the attributes, (iii) the accident occur evenly on all days, (iv) errors occur evenly on all pages, (v) the events occur in the given ratio, (vi) the events occur according to the given distribution (Binomial, Poisson, Normal). This is called testing goodness of fit.

We now compare the calculated value of  $\chi^2$  with the table value for the given degrees of freedom and at a specified level of significance.

If the calculated value of  $\chi^2$  is greater than the table value we conclude that the difference between the observed values and expected frequencies is significant and the hypothesis is

rejected. If on the other hand the calculated value of  $\chi^2$  is less than the table value, we conclude that the difference between the observed values and the expected frequencies is not significant and the hypothesis is accepted.

Note ...

The value of  $\chi^2$  will be zero if the observed and expected frequencies coincide. The value of  $\chi^2$  is always positive. As observed frequencies depart from expected frequencies  $\chi^2$  goes on increasing.

#### (a) Analysis of $r \times c$ table (Contingency Table)

Chi-square criterion is based on observed frequencies  $O$  and expected frequencies  $E$ . Assuming that there is no association between the given attributes, we calculate frequencies in each cell. This frequency is called expected frequency of the cell. We denote the given frequency called observed frequency of the  $(i, j)$ th cell by  $O_{ij}$  and the expected frequency of  $(i, j)$ th cell by  $E_{ij}$ . If the table giving the observed frequencies of two attributes has  $r$ -rows and  $c$ -columns, there will be  $r \times c$  cells in the table. Such a table is called contingency table. If  $A_1, A_2, \dots, A_r$  are totals of  $r$ -rows and  $B_1, B_2, \dots, B_c$  are the totals of  $c$ -columns obtained from given frequencies, then expected frequency  $(i, j)$ th cell is given by

$$E_{ij} = \frac{(A_i \times B_j)}{N}$$

$$\text{i.e., } E_{1,1} = \frac{(A_1 B_1)}{N}, \quad E_{1,2} = \frac{(A_1 B_2)}{N}, \quad E_{1,3} = \frac{(A_1 B_3)}{N}, \dots \text{ etc.}$$

The statistic  $\chi^2$  is now defined by

$$\chi^2 = \sum \sum \left( \frac{(O_{ij} - E_{ij})^2}{E_{ij}} \right)$$

with  $(r-1) \times (c-1)$  degrees of freedom.

						Total
	$\frac{A_1 \times B_1}{N}$	$\frac{A_1 \times B_2}{N}$		$\frac{A_1 \times B_c}{N}$		$A_1$
Total	$B_1$	$B_2$		$B_c$		$A_2$
						$A_r$
						$N$

If calculated value of  $\chi^2$  is less than the table value of  $\chi^2$  the hypothesis that there is no association between the attributes is accepted.

### 9. Degrees of Freedom

While comparing the calculated value of  $\chi^2$  with the table value we must know the degrees of freedom. The term degrees of freedom means the number of values which can be chosen arbitrarily under the given restrictions. For example, if we have to choose 5 numbers whose sum is 50, we cannot choose all the five numbers arbitrarily because of the restriction. We can choose four numbers

arbitrarily and the fifth number will have to be 50 – (sum of four). Thus, the degrees of freedom are four and not five. If more restrictions are placed on the choice of number, the degrees of freedom will be less. In general if there are  $n$  numbers to be chosen and  $k$  independent constraints then the degrees of freedom denoted by d.f. are given by  $d.f. = n - k$ .

If the table has  $r$  rows and  $c$  columns then in each row we can select  $(c - 1)$  elements and in each column we can select  $(r - 1)$  elements freely. This means for each row we have  $(c - 1)$  degrees of freedom and for each column we have  $(r - 1)$  degrees of freedom. Hence, for the whole table we have  $(r - 1) \times (c - 1)$  degrees of freedom.

Thus, if there are two rows and two columns then  $d.f. = (2 - 1)(2 - 1) = 1$ . There is only one degree of freedom. If there are three rows and three columns then  $d.f. = (3 - 1)(3 - 1) = 4$ . There are four degrees of freedom and so on.

### 10. Conditions for $\chi^2$ Test

The following conditions should be satisfied while applying  $\chi^2$  test;

1.  $N$ , the total number of observations must be sufficiently large. Preferably  $N$  should be greater than 50.

2. Frequency of every cell must be greater than 10. If any frequency is less than 10 it is combined with neighbouring frequencies so that the combined frequency is greater than 10 and the degrees of freedom are reduced accordingly. (See Ex. 7 and 9, page 9-34 and 9-36)

3. The number of classes  $n$  must not be too small nor too large. Preferably we should have  $4 \leq n \leq 16$ .

**Note ...**

It may be noted that the  $\chi^2$ -test depends upon (i) the observed frequencies, (ii) the expected frequencies, (iii) the number of observations only. It does not make any assumption regarding the nature of parent population.

### 11. Yate's Correction

In a  $2 \times 2$  table the degrees of freedom is  $(2 - 1)(2 - 1) = 1$ . If any of the cell frequency is less than 5, we have to use pooling method. But this will result in  $\chi^2$  with zero degrees of freedom. This is meaningless. In this case Yates in 1934 suggested to use

$$\chi^2 = \sum \left[ \frac{(O - E)^2}{E} \right]$$

He showed that by taking  $\chi^2$  as defined above,  $\chi^2$  approximation is improved. (See Ex. 5, page 9-27).

### 12. Uses of $\chi^2$ Test

We shall consider only two uses of  $\chi^2$  distribution.

1. To test independence of attributes :  $\chi^2$ -test is widely used to test whether there is association between two or more attributes. For example,  $\chi^2$ -test can be used to determine whether there is association between the colour of mother's eye and daughter's eye, between inoculation and prevention of a disease. In such cases we proceed on the null hypothesis that there is no

association between the attributes. If the calculated value of  $\chi^2$  at a certain level of significance is less than the table value, the hypothesis is accepted otherwise rejected.

In the same way  $\chi^2$ -test is also used to test if a characteristic is dependent upon another characteristic. For example,  $\chi^2$ -test can be used to test whether the performance of workers in a factory is dependent on the training or to test whether performance of students in a particular subject is dependent on the performance in another subject. Using  $\chi^2$ -distribution in this way to test the independence of one attribute on another is called test of independence.

2. To test the goodness of fit :  $\chi^2$ -test is very commonly known as  $\chi^2$ -test of goodness of fit because it enables us to ascertain how well the theoretical distributions such as Binomial, Poisson or Normal fit the observed frequencies. In such cases we proceed on the null hypothesis that the theory supports the observations i.e. the fit is good. For example, suppose we toss 3 fair coins 200 times and observe the frequencies of 0, 1, 2, 3 heads. We can also calculate the expected frequencies by using Binomial Distribution.  $\chi^2$ -test can be used to ascertain whether Binomial distribution fits well. If the calculated value of  $\chi^2$  at a certain level of significance is less than the table value, the fit is supposed to be good otherwise the fit is supposed to be poor.

3. To test the discrepancies between observed frequencies and expected frequencies :  $\chi^2$ -test can also be used to ascertain whether the difference between observed frequencies and the expected frequencies is purely due to chance or whether due to inadequacy in the theory applied.

4. To test equality of several proportions :  $\chi^2$ -test can also be used to test whether the proportions  $p_1, p_2, p_3, p_4$  in different populations are equal i.e.  $\chi^2$ -test can also be used to test the null hypothesis that  $p_1 = p_2 = p_3 = p_4$ .

5. To test the hypothesis about  $\sigma^2$  :  $\chi^2$  is also used to test the population variance. (See Ex. 10, page 9-37)

#### Type I : Independence of Attributes

Example 1 : Investigate the association between the darkness of eye colour in father and son from the following data.

Colour of father's eyes

Colour of son's eyes			Total
	Dark	Not dark	
Dark	48	90	138
Not dark	80	782	862
Total	128	872	1000

(M.U. 2010)

Sol. : (i) Null Hypothesis  $H_0$  : There is no association between the darkness of eye colour in father and son.

Alternative Hypothesis  $H_a$  : There is an association.

(ii) Calculation of test statistic : On the basis of this hypothesis the expected frequency of dark eyed sons with dark eyed fathers

$$= \frac{A \times B}{N}$$

where,  $A$  = number of dark eyed fathers (total of first column)

$B$  = number of dark eyed sons (total of first row)

$N$  = total number of observations

$$\therefore \text{Expected frequency} = \frac{128 \times 128}{1000} = 18$$

(This is because if there is no association, since the ratio of dark eyed fathers to the total is  $128 / 1000$  out of 138 dark eyed sons there will be  $\frac{138 \times 128}{1000}$  dark eyed sons.)

Having obtained the expected frequency in the first cell, since the totals remain the same, the figures in other cells can be easily obtained as  $138 - 18 = 120$ ,  $128 - 18 = 110$ ,  $872 - 120 = 752$ . We thus get the following table.

Colour of father's eyes

Colour of son's eyes	Dark	Not dark	Total
Dark	18	120	138
Not dark	110	752	862
Total	128	872	1000

Calculation of  $(O - E)^2 / E$ 

O	E	$(O - E)^2$	$(O - E)^2 / E$
48	18	900	50.00
80	110	900	8.18
90	120	900	7.50
782	752	900	1.20
Total		$\chi^2 = 66.68$	

(iii) Level of significance :  $\alpha = 0.05$ .

Degrees of freedom =  $(r - 1)(c - 1) = (2 - 1)(2 - 1) = 1$ .

( $r$  = number of rows,  $c$  = number of columns.)

(iv) Critical value : For 1 d.f. at 5% level of significance the table value of  $\chi^2$  is 3.84.

(v) Decision : Since the calculated value of  $\chi^2 = 66.68$  is much greater than the table value of  $\chi^2 = 3.84$ , the null hypothesis is rejected.

$\therefore$  There is an association between darkness of colour of fathers and sons.

**Example 2 :** The following table gives the number of accounting clerks not committing errors among trained and untrained clerks working in an organisation.

	No. of clerks committing errors	No. of clerks not committing errors	Total
Trained	70	530	600
Untrained	155	745	900
Total	225	1275	1500

Test the effectiveness of training in preventing errors. (Table value of  $\chi^2$  for 1 d.f., 2 d.f., 3 d.f. 4 d.f. are 3.84, 5.99, 7.81, 9.29 respectively.)

Sol. (i) Null Hypothesis  $H_0$  : There is no association between training and errors.

Alternative Hypothesis  $H_A$  : There is an association between training and errors.

(ii) Calculation of test statistic : On the basis of this hypothesis, the number in the first cell

$$= \frac{A \times B}{N}$$

where,  $A$  = number of clerks committing error i.e. the total in the first column,  
 $B$  = number of trained clerks i.e. the total in the first row,  
 $N$  = Total number of observations.

(This is so because ratio of clerks committing errors to the total is  $\frac{225}{1500}$ . If there is no association out of total of 600 trained clerks  $\frac{225 \times 600}{1500}$  will commit errors.)

$\therefore$  The number in the first cell =  $\frac{225 \times 600}{1500} = 90$ .

Having obtained the expected frequency in the first cell, since the totals remain the same, the figures in the other cells are  $600 - 90 = 510$ ,  $225 - 90 = 135$ ,  $1275 - 510 = 765$ .

We, thus, get the following table.

Table of calculated frequencies

	No. of clerks committing errors	No. of clerks not committing errors	Total
Trained	90	510	600
Untrained	135	765	900
Total	225	1275	

Calculation of  $(O - E)^2 / E$ 

O	E	$(O - E)^2$	$(O - E)^2 / E$
70	90	400	4.44
530	510	400	0.78
155	135	400	2.96
745	765	400	0.52
Total		$\chi^2 = 8.7$	

(iii) Level of significance :  $\alpha = 0.05$ .

Degrees of freedom =  $(r - 1)(c - 1) = (2 - 1)(2 - 1) = 1$ .

(iv) Critical value : For 1 d.f. and 5% level of significance, the table value of  $\chi^2 = 3.81$ .

(v) Decision : Since the calculated value of  $\chi^2 = 8.7$  is greater than the table value of  $\chi^2 = 3.81$ , the null hypothesis is rejected.

$\therefore$  The training is effective in preventing errors.

**Example 3 :** A sample of 400 students of under-graduate and 400 students of post-graduate classes was taken to know their opinion about autonomous colleges. 290 of the under-graduate and 310 of the post-graduate students favoured the autonomous status. Present these facts in the form of a table and test at 5% level, that the opinion regarding autonomous status of colleges is independent of the level of classes of students. (M.U. 2016)



- (iii) Level of significance :  $\alpha = 0.05$ .  
 The number of degrees of freedom =  $(r-1)(c-1) = (2-1)(2-1) = 1$ .
- (iv) Critical value : For 1 d.f. at 5% level of significance the table value of  $\chi^2 = 3.84$ .
- (v) Decision : Since the calculated value of  $\chi^2 = 11.89$  is much greater than the table value of  $\chi^2 = 3.84$ , the null hypothesis is rejected.  
 ∴ There is association between education of fathers and intelligence of sons.

**Example 5 :** Two batches of 12 animals each are given test of inoculation. One batch was inoculated and the other was not. The number of dead and surviving animals are given in the following table for both cases. Can the inoculation be regarded as effective against the disease at 5% level of significance. (Make Yates correction)

	Dead	Surviving	Total
Inoculated	2	10	12
Not-Inoculated	8	4	12
Total	10	14	24

(M.U. 2004, 11)

- Sol. : (i) Null Hypothesis  $H_0$  : There is no association between inoculation and death.  
 Alternative Hypothesis  $H_a$  : There is association between inoculation and death.

- (ii) Calculation of test statistic : On the basis of this hypothesis the number in the first cell

$$= \frac{A \times B}{N}$$

where,  $A$  = total in the first column, $B$  = total in the first row, $N$  = Total number of observations.

$$\therefore \text{The number in the first cell} = \frac{10 \times 12}{24} = 5.$$

The remaining cell frequencies may be calculated in the same manner or may be obtained by subtracting this frequency from the row total and column total. We then apply Yates correction and prepare the table.

Calculation of  $\chi^2$ 

O	E	$ O-E  - 0.5$	$\frac{( O-E -0.5)^2}{E}$
2	$\frac{10 \times 12}{24} = 5$	2.5	$\frac{6.25}{5} = 1.25$
10	$12 - 5 = 7$	2.5	$\frac{6.25}{7} = 0.89$
8	$10 - 5 = 5$	2.5	$\frac{6.25}{5} = 1.25$
4	$12 - 5 = 7$	2.5	$\frac{6.25}{7} = 0.89$
	Total		$\chi^2 = 4.29$

- (i) Level of significance :  $\alpha = 0.05$ ,  
 Degree of freedom =  $(r-1)(c-1) = (2-1)(2-1) = 1$ ,  
 Critical value : For 1 degree of freedom at 5% level of significance the table value of  $\chi^2 = 3.81$ .  
 Decision : Since the calculated value of  $\chi^2 = 4.29$  is greater than the table value  $\chi^2 = 3.81$ , the hypothesis is rejected.  
 ∴ There is association between inoculation and death i.e. Inoculation is effective against the disease.

## Remark ...

We would arrive at the same conclusion even if Yates' correction is not made.

**Example 6 :** To test the effect of a new drug, a controlled experiment was conducted. 300 patients were given the new drug while 200 patients were given no drug. On the basis of examination of these persons, the following results were obtained.

	Cured	Condition worsened	No effect	Total
Given the new drug	200	40	60	300
Not given the drug	120	30	50	200
Total	320	70	110	500

Use  $\chi^2$  test to find the effect of the new drug.

- Sol. : (i) Null Hypothesis
- $H_0$
- : The drug is not effective.

- Alternative Hypothesis
- $H_a$
- : The drug is effective.

- (ii) On the basis of this hypothesis the number in the first cell

$$= \frac{A \times B}{N}$$

where,  $A$  = total in the first column, $B$  = total in the first row, $N$  = Total number of observations.

$$\therefore \text{The number in the first cell} = \frac{320 \times 300}{500} = 192.$$

$$\text{Similarly, the number in the second cell} = \frac{70 \times 300}{500} = 42.$$

Since the totals remain the same, the numbers in the remaining cells are

$$320 - 192 = 128,$$

$$70 - 42 = 28,$$

$$300 - (192 + 42) = 66,$$

$$110 - 66 = 44.$$

We, thus, get the following table.

Table of Calculated Frequencies

	Cured	Condition worsened	No effect	Total
Given the new drug	192	42	66	300
Not given the drug	128	28	44	200
Total	320	70	110	500

Calculation of  $(O - E)^2 / E$ 

O	E	O - E	$(O - E)^2$	$(O - E)^2 / E$
200	192	8	64	0.333
40	42	-2	4	0.095
60	66	-6	36	0.545
120	128	-8	64	0.500
30	28	2	4	0.143
50	44	6	36	0.816
Total			$\chi^2 = 2.434$	

(iii) Level of significance :  $\alpha = 0.05$ .Degrees of freedom =  $(r - 1)(c - 1) = (2 - 1)(3 - 1) = 2$ .(iv) Critical value : For 2 degrees of freedom at 5% level of significance, the table value of  $\chi^2 = 5.991$ .(v) Decision : Since the calculated value of  $\chi^2 = 2.434$  is less than the table value  $\chi^2 = 5.991$ , the hypothesis is accepted.

∴ The new drug is not effective.

**Example 7 :** The following table gives the result of opinion poll for three parties A, B and C. Test whether the age and the choice of the party are independent at 5% level of significance using  $\chi^2$  test.

Age	Party			Total
	A	B	C	
20 - 35	25	20	25	70
35 - 50	20	25	35	80
Above 50	25	25	30	80
Total	70	70	90	230

**Sol. :** (i) Null Hypothesis  $H_0$  : There is no relation between the age and the choice of the party.  
Alternative Hypothesis  $H_A$  : There is a relation between the two.

(ii) On the basis on this hypothesis the number in the first cell

$$= \frac{A \times B}{N}$$

where,  $A$  = total in the first column,  $B$  = total in the first row,  
 $N$  = Total number of observations.∴ The number in the first cell of the first row =  $\frac{70 \times 70}{230} = 21.3$ ,Similarly, the number in the second cell of the first row =  $\frac{70 \times 70}{230} = 21.3$ .The number in the first cell of the second row =  $\frac{70 \times 80}{230} = 24.3$ ,The number in the second cell of the second row =  $\frac{70 \times 80}{230} = 24.3$ .Since the totals remain the same, the numbers in the remaining cells are  
 $70 - (21.3 + 21.3) = 27.4$ ,  $80 - (24.3 + 24.3) = 31.4$ ,

We, thus, get the following table.

Table of Calculated Frequencies

Age	Party			Total
	A	B	C	
20 - 35	21.3	21.3	27.4	70.0
35 - 50	24.3	24.3	31.4	80.0
Above 50	24.4	24.4	31.2	80.0
Total	70.0	70.0	90.0	230.0

Calculation of  $(O - E)^2 / E$ 

O	E	O - E	$(O - E)^2$	$(O - E)^2 / E$
25	21.3	3.7	13.69	0.643
20	21.3	-1.3	1.69	0.079
25	27.4	-2.4	5.76	0.210
20	24.3	-4.3	18.49	0.685
25	24.3	0.7	0.49	0.020
35	31.4	-3.6	12.96	0.413
25	24.4	0.6	0.36	0.015
25	24.4	0.6	0.36	0.015
30	31.2	-1.2	1.44	0.046
Total			$\chi^2 = 2.126$	

(iii) Level of significance :  $\alpha = 0.05$ .Degrees of freedom =  $(r - 1)(c - 1) = (3 - 1)(3 - 1) = 4$ .(iv) Critical value : For 4 degrees of freedom at 5% level of significance, the table value of  $\chi^2 = 9.488$ .(v) Decision : Since the calculated value of  $\chi^2 = 2.126$  is less than the table value  $\chi^2 = 9.488$ , the hypothesis is accepted.

∴ There is no relation between the age and the choice of the party.

**Type II : Goodness of Fit**

**Example 1 :** The following table gives the number of accidents in a city during a week. Test whether the accidents are uniformly distributed over a week.

Day	Sun., Mon., Tue., Wed., Thu., Fri., Sat.	Total
No. of accidents	13, 15, 9, 11, 12, 10, 14	84

(M.U. 2017)

**Sol. :** (i) Null Hypothesis  $H_0$  : Accidents are equally distributed over all the days of a week.  
Alternative Hypothesis  $H_A$  : Accidents do not occur equally.

(ii) Calculation of test statistic : If the accidents occur equally on all days of a week, there will be  $84/7 = 12$  accidents per day.

$$\begin{aligned} \therefore \chi^2 &= \sum \frac{(O-E)^2}{E} = \frac{(13-12)^2}{12} + \frac{(15-12)^2}{12} + \frac{(9-12)^2}{12} \\ &\quad + \frac{(11-12)^2}{12} + \frac{(12-12)^2}{12} + \frac{(10-12)^2}{12} + \frac{(14-12)^2}{12} \\ &= \frac{1}{12} [1+9+9+1+0+4+4] = \frac{28}{12} = 2.33 \end{aligned}$$

(iii) Level of significance :  $\alpha = 0.05$ .

Degrees of freedom =  $n - 1 = 7 - 1 = 6$ ,

(iv) Critical value : For 6 degrees of freedom at 5% level of significance table value of  $\chi^2$  is 12.59.

(v) Decision : Since the calculated value of  $\chi^2$  is less than the table value. The hypothesis is accepted.

∴ The accidents occur equally on all working days.

**Example 2 :** A die was thrown 132 times and the following frequencies were observed.

No. obtained : 1, 2, 3, 4, 5, 6. Total

Frequency : 15, 20, 25, 15, 29, 28, 132

Test the hypothesis that the die is unbiased.

(M.U. 2010, 15, 17)

**Sol. :** (i) Null Hypothesis  $H_0$  : The die is unbiased.

Alternative Hypothesis  $H_A$  : The die is not unbiased.

(ii) Calculation of test statistic : On the hypothesis that the die is unbiased we should expect the frequency of each number to be  $132/6 = 22$ .

**Calculation of  $(O-E)^2/E$**

No.	O	E	$(O-E)^2$
1	15	22	49
2	20	22	4
3	25	22	9
4	15	22	49
5	29	22	49
6	28	22	36
	Total		196

$$\therefore \chi^2 = \sum \frac{(O-E)^2}{E} = \frac{196}{22} = 8.91$$

(i) Level of significance :  $\alpha = 0.05$ .

Number of degrees of freedom =  $n - 1 = 6 - 1 = 5$ .

(ii) Critical value : For 5 d.f. at 5% level of significance the table value of  $\chi^2$  is 11.07.

(iii) Decision : Since the calculated value of  $\chi^2 = 8.91$  is less than the table value of  $\chi^2 = 11.07$ , the null hypothesis is accepted.

∴ The die is unbiased.

**Example 3 :** The number of car accidents in a metropolitan city was found to be 20, 17, 12, 6, 7, 15, 8, 5, 16 and 14 per month respectively. Use  $\chi^2$ -test to check whether these frequencies are in agreement with the belief that occurrence of accidents was the same during 10 months period. Test at 5% level of significance. (Table value of  $\chi^2$  at 9 d.f. is 16.9) (M.U. 2001, 14)

**Sol. :** (i) Null Hypothesis  $H_0$  : Accidents occur equally on all months.

Alternative Hypothesis  $H_A$  : Accidents do not occur equally on all months.

(ii) Calculation of test statistic : On the basis of this hypothesis, the number of accidents per month = (total) / 10 =  $(20 + 17 + 12 + 6 + 7 + 15 + 8 + 5 + 16 + 14) / 10 = 120 / 10 = 12$ .

$$\begin{aligned} \therefore \chi^2 &= \sum \frac{(O-E)^2}{E} \\ &= \frac{(20-12)^2}{12} + \frac{(17-12)^2}{12} + \frac{(12-12)^2}{12} + \frac{(6-12)^2}{12} + \frac{(7-12)^2}{12} \\ &\quad + \frac{(15-12)^2}{12} + \frac{(8-12)^2}{12} + \frac{(5-12)^2}{12} + \frac{(16-12)^2}{12} + \frac{(14-12)^2}{12} \\ &= \frac{1}{12} [64 + 25 + 0 + 36 + 25 + 9 + 16 + 49 + 16 + 4] \\ &= \frac{244}{12} = 20.33. \end{aligned}$$

(iii) Level of significance :  $\alpha = 0.05$ .

Number of degrees of freedom =  $n - 1 = 10 - 1 = 9$ .

(iv) Critical value : For 9 d.f. at 5% level of significance, the table value of  $\chi^2$  is 16.92.

(v) Decision : Since the calculated value of  $\chi^2 = 20.33$  is greater than the table value of  $\chi^2 = 16.92$ , the null hypothesis is rejected.

∴ Accidents do not occur equally on all months.

**Example 4 :** 300 digits were chosen at random from a table of random numbers. The frequency of digits was as follows.

Digit	0	1	2	3	4	5	6	7	8	9	Total
Frequency	28	29	33	31	26	35	32	30	31	25	300

Using  $\chi^2$ -test examine the hypothesis that the digits were distributed in equal numbers in the table. (M.U. 1996)

Sol. : (i) Null Hypothesis  $H_0$  : The digits are distributed **equally**.  
 Alternative Hypothesis  $H_A$  : The digits are not distributed **equally**.

(ii) Calculation of test statistic : On the basis of the hypothesis the frequency of each digit.

$$\text{Total} = \frac{28 + 29 + 33 + 31 + 26 + 35 + 32 + 30 + 31 + 25}{10} = 30$$

$$\therefore E = \frac{300}{10} = 30.$$

$$\therefore \chi^2 = \sum \frac{(O - E)^2}{E}$$

$$= \frac{(28 - 30)^2}{30} + \frac{(29 - 30)^2}{30} + \frac{(33 - 30)^2}{30} + \frac{(31 - 30)^2}{30} + \frac{(26 - 30)^2}{30} + \frac{(35 - 30)^2}{30}$$

$$+ \frac{(32 - 30)^2}{30} + \frac{(30 - 30)^2}{30} + \frac{(31 - 30)^2}{30} + \frac{(25 - 30)^2}{30}$$

$$\therefore \chi^2 = \frac{1}{30} [4 + 1 + 9 + 1 + 16 + 25 + 4 + 0 + 1 + 25] = \frac{86}{30} = 2.87$$

(iii) Level of significance :  $\alpha = 0.05$ .

Number of degrees of freedom =  $n - 1 = 10 - 1 = 9$ .

(iv) Critical value : For 9 d.f. at 5% level of significance the table value of  $\chi^2$  is 16.92.

(v) Decision : Since the calculated value of  $\chi^2 = 2.87$  is less than the table value of  $\chi^2$ , the null hypothesis is accepted.

$\therefore$  Digits are equally distributed in the table.

Example 5 : Theory predicts that the proportion of beans in the four groups A, B, C, D should be 9 : 3 : 3 : 1. In an experiment among 1500 beans the numbers in the four groups were 882, 313, 287 and 118. Does the experimental results support the theory ? (M.U. 2001, 06)

Sol. : (i) Null Hypothesis  $H_0$  : The proportion of the beans in the four groups A, B, C, D is the given proportion 9 : 3 : 3 : 1.

Alternative Hypothesis  $H_A$  : The proportion is not as given above.

(ii) Calculation of test statistic : On the basis of the above hypothesis, since the sum is  $9 + 3 + 3 + 1 = 16$ , the number of beans in the four groups will be

$$A = \frac{9}{16} \times 1600 = 900, \quad B = \frac{3}{16} \times 1600 = 300$$

$$C = \frac{3}{16} \times 1600 = 300, \quad D = \frac{1}{16} \times 1600 = 100$$

$$\therefore \chi^2 = \sum \frac{(O - E)^2}{E} = \frac{(882 - 900)^2}{900} + \frac{(313 - 300)^2}{300} + \frac{(287 - 300)^2}{300} + \frac{(118 - 100)^2}{100}$$

$$= 0.36 + 0.56 + 0.56 + 3.24 = 4.72$$

(iii) Level of significance :  $\alpha = 0.05$ .

Degrees of freedom =  $n - 1 = 4 - 1 = 3$ .

(i) Critical value : For 3 degrees of freedom at 5% level of significance, the table value of  $\chi^2$  is 7.81.

(ii) Decision : Since the calculated value of  $\chi^2 = 4.72$  is less than the table value of  $\chi^2 = 7.81$ , the null hypothesis is accepted.

$\therefore$  The proportion 9 : 3 : 3 : 1 is correct.

Example 6 : In an experiment on pea breeding the following frequencies were obtained.

Round yellow	Wrinkled yellow	Round green	Wrinkled green	Total
315	101	108	32	556

Theory predicts that the frequencies should be in proportion of 9 : 3 : 3 : 1.

Examine the correspondence between theory and experiment using Chi-square Test.

(M.U. 2016)

Sol. : (i) Null Hypothesis  $H_0$  : The proportion of the peas in the four groups say A, B, C, D is in the given proportion 9 : 3 : 3 : 1.

Alternative Hypothesis  $H_A$  : The proportion is not as given above.

(ii) Calculation of test statistic : On the basis of the above hypothesis since the sum is  $9 + 3 + 3 + 1 = 16$ , the number of peas in the four groups will be

$$A = \frac{9}{16} \times 556 = 312.75 = 313, \quad B = \frac{3}{16} \times 556 = 104.25 = 104,$$

$$C = \frac{3}{16} \times 556 = 104.25 = 104, \quad D = \frac{1}{16} \times 556 = 34.75 = 35.$$

$$\therefore \chi^2 = \sum \frac{(O - E)^2}{E} = \frac{(315 - 313)^2}{313} + \frac{(101 - 104)^2}{104} + \frac{(108 - 104)^2}{104} + \frac{(32 - 35)^2}{35}$$

$$= 0.013 + 0.086 + 0.154 + 0.257 = 0.51$$

(iii) Level of significance :  $\alpha = 0.05$ .

Degree of freedom =  $n - 1 = 4 - 1 = 3$ .

(iv) Critical value : For 3 degrees of freedom at 5% level of significance table value of  $\chi^2$  is 7.81.

(v) Decision : Since the calculated value of  $\chi^2 = 0.51$  is less than the table value of  $\chi^2 = 7.81$ , the null hypothesis is accepted.

$\therefore$  The proportion 9 : 3 : 3 : 1 is correct.

Example 7 : The figures given below are (a) the observed frequencies of a distribution, (b) the frequencies of the normal distribution, having the same mean, standard deviation and the total frequency as in (a).

(a) 1, 12, 66, 220, 495, 792, 924, 792, 495, 220, 66, 12, 1.

(b) 2, 15, 66, 210, 484, 799, 943, 799, 484, 210, 66, 15, 2.

Apply  $\chi^2$  test of goodness of fit.

(M.U. 2004)

Sol. : Since the frequencies at the beginning and end are less than 10, we group them and then apply the  $\chi^2$  test.

Calculation of  $\chi^2$ 

$O$	: 1, 12, 66, 220, 495, 792, 924, 792, 495, 220, 66, 12, 1
$E$	: 2, 15, 66, 210, 484, 799, 943, 799, 484, 210, 66, 15, 2
$(O-E)^2/E$	: 0.94, 0.0, 0.48, 0.25, 0.06, 0.38, 0.06, 0.25, 0.48, 0, 0.94

$$\therefore \chi^2 = \sum \frac{(O-E)^2}{E} = 3.84.$$

- (i) Null Hypothesis  $H_0$  : The fit is good.  
 Alternative Hypothesis  $H_a$  : The fit is not good.
- (ii) Calculation of test statistic :  $\chi^2 = 3.84$

(iii) Level of significance :  $\alpha = 0.05$ .

Number of degrees of freedom : There are originally 13 classes. Since they are reduced to 11 by grouping twice, the degrees of freedom is reduced by 2. Further, since the mean, the standard deviation and the total frequency of original data are used, three constraints are introduced, reducing the degree of freedom by 3. (For calculating the mean and the standard deviation, three sums  $\sum f$ ,  $\sum f x_i$  and  $\sum f x_i^2$  are required. Hence, the degree of freedom is reduced by 3.) Thus, the d.f. =  $13 - (2) - (3) = 8$ .

- (iv) Critical value : For 8 d.f. at 5% level of significance, the table value of  $\chi^2 = 15.51$ .  
 (v) Decision : Since the calculated value of  $\chi^2 = 3.84$  is less than the table value  $\chi^2 = 15.51$ , the null hypothesis is accepted.

∴ The fit is good.

**Example 8 :** The number of defects in printed circuit board is hypothesised to follow Poisson distribution. A random sample of 60 printed boards showed the following data.

Number of defects : 0 1 2 3

Observed frequency : 32 15 9 4

Does the hypothesis of Poisson distribution seem appropriate.

(M.U. 2004)

Sol. : (i) Null Hypothesis  $H_0$  : The defects follow Poisson distribution.

Alternative Hypothesis  $H_a$  : The defects do not follow Poisson distribution.

(ii) Calculation of test statistic : The expected frequencies of Poisson's distribution are given by

$$\text{Expected frequency} = Np = N \times \frac{e^{-m} m^x}{x!}$$

where,  $m$  = mean of the distribution,

$x$  = random variable,

$N$  = number of observations.

$$\text{Here, } m = \frac{\sum f x}{\sum f} = \frac{32 \times 0 + 15 \times 1 + 9 \times 2 + 4 \times 3}{32 + 15 + 9 + 4} = \frac{45}{60} = 0.75$$

$$\text{Exp. Freq.} = 60 \times \frac{e^{-0.75} (0.75)^x}{x!}, \quad x = 0, 1, 2, 3$$

Of zero defects = 28.32, Of one defect = 21.25, Of two defects = 7.97,  
 Of three defects = 60 - (Sum of the above frequencies)  
 $= 60 - 57.54 = 2.46$

Calculation of  $(O-E)^2/E$ 

No. of defects	O	E	$(O-E)^2/E$
0	32	28.32	0.4782
1	15	21.25	1.8382
2	9	7.97	2.46
3	4	2.46	0.6332
		Total	2.9494

$$\therefore \chi^2 = \sum \frac{(O-E)^2}{E} = 2.95$$

- (iii) Level of significance :  $\alpha = 0.05$ .  
 Degrees of freedom =  $4 - (1 + 2) = 1$

(The number of degrees of freedom for each class is one. There are originally 4 classes. Hence, the degrees of freedom originally is 4. But we reduced the classes by one, thus, reducing the degree by one. Further, while calculating the parameter  $m$ , we used two sums  $\sum f$  and  $\sum f x_i$  thus, reducing the degree of freedom by two.)

(iv) Critical value : For 1 degree of freedom at 5% level of significance the table value of  $\chi^2$  is 3.84.

(v) Decision : Since the calculated value of  $\chi^2 = 2.95$  is less than the table value of  $\chi^2 = 3.84$ , the null hypothesis is accepted.

∴ The defects follow Poisson's distribution.

**Example 9 :** The following mistakes per page were observed in a book.

No. of mistakes per page : 0 1 2 3 4

No. of pages : 211 90 19 5 0

Fit a Poisson distribution and test the goodness of fit.

Sol. : (i) Null Hypothesis  $H_0$  : The mistakes follow Poisson's distribution. The fit is good.

Alternative Hypothesis  $H_a$  : The mistakes do not follow Poisson's distribution.

(ii) Calculation of test statistic : The expected frequencies by Poisson's distribution are given by

$$\text{Expected frequency} = Np = N \times \frac{e^{-m} m^x}{x!}$$

where,  $m$  = mean of the distribution,  $x$  = random variable,

$N$  = number of observations.

$$\text{Here, } m = \frac{\sum f x}{\sum f} = \frac{211(0) + 90(1) + 19(2) + 5(3) + 0(4)}{211 + 90 + 19 + 5 + 0} = \frac{143}{325} = 0.44$$

$x = 0, 1, 2, 3, 4 ; \quad N = 325$ .

$$\text{Exp. Freq.} = \frac{325 \times e^{-0.44} (0.44)^x}{x!}$$

Since  $N \times e^{-m}$  appears in every calculation we calculate it first.

$$N \times e^{-m} = 325 \times e^{-0.44} = 209.31$$

Now, the expected frequencies are

$$\begin{aligned}\text{Of zero mistakes} &= 325 \times \frac{e^{-0.44} (0.44)^0}{0!} = 209.31(1) = 209.31 \\ \text{Of one mistakes} &= 325 \times \frac{e^{-0.44} (0.44)^1}{1!} = 209.31(0.44) = 92.1 \\ \text{Of two mistakes} &= 325 \times \frac{e^{-0.44} (0.44)^2}{2!} = 209.31(0.0968) = 20.26 \\ \text{Of three mistakes} &= 325 \times \frac{e^{-0.44} (0.44)^3}{3!} = 209.31(0.0142) = 2.97 \\ \text{Of four mistakes} &= 325 - (\text{sum of the above frequencies}) \\ &= 325 - 324.64 = 0.36.\end{aligned}$$

#### Calculation of $(O - E)^2 / E$

No. of mistakes	O	E	$(O - E)^2$	$(O - E)^2 / E$
0	211	209.31	2.87	0.014
1	90	92.10	4.41	0.048
2	19	20.26		
3	5	2.97	0.17	0.007
4	0	0.36		
Total				0.069

$$\therefore \chi^2 = \sum \frac{(O - E)^2}{E} = 0.069.$$

(iii) Level of significance :  $\alpha = 0.05$ .

Degrees of freedom =  $5 - 4 = 1$ .

(The number of degrees of freedom is 1 for each class. There are 5 classes originally. Hence, the degrees of freedom originally is 5. But we reduced the classes by two, thus reduced the degrees of freedom by 2. Further, while calculating the parameter  $m$ , we used two sums  $\sum f_i$  and  $\sum f_i x_i^2$ , thus, reducing the degree of freedom again by 2.)

Hence, the number of degrees of freedom =  $5 - (2 + 2) = 1$ .

(iv) Critical value : For 1 degree of freedom at 5% level of significance the table value of  $\chi^2$  is 3.84.

(v) Decision : Since the calculated value of  $\chi^2 = 0.069$  is less than the table value of  $\chi^2 = 3.84$  we accept the hypothesis.

∴ The mistakes follow Poisson's distribution.

Example 10 : Weights in kgs. of 10 students are given below.

38, 40, 45, 53, 47, 43, 55, 48, 52, 49.

Can we say that the variance of the normal distribution from which the above sample is drawn is 20 kg. ? (M.U. 2004)

Sol. :  $x_i$  : 38, 40, 45, 53, 47, 43, 55, 48, 52, 49,  
 $(x_i - \bar{x})^2$  : 81, 49, 4, 36, 0, 16, 64, 1, 25, 04.

$$\bar{x} = \frac{\sum x_i}{n} = \frac{470}{10} = 47; \quad \sum (x_i - \bar{x})^2 = 280.$$

(i) Null Hypothesis  $H_0$  :  $\sigma^2 = 20$   
 Alternative Hypothesis  $H_a$  :  $\sigma^2 \neq 20$

(ii) Calculation of test statistic :  $\chi^2 = \frac{\sum (x_i - \bar{x})^2}{\sigma^2} = \frac{280}{20} = 14$ .

(iii) Level of significance :  $\alpha = 0.05$ .

(iv) Critical value : For 9 degrees of freedom at 5% level of significance, the table value of  $\chi^2$  is 16.99.

(v) Decision : Since the calculated value of  $\chi^2 = 14$  is less than the critical value  $\chi^2 = 16.99$ , the hypothesis is accepted.

∴ The sample was drawn from the normal population with variance 20.

Example 11 : Five dice were thrown 192 times and the number of times 4, 5 or 6 were obtained as follows.

No. of dice showing 4, 5, 6 : 5, 4, 3, 2, 1, 0.

Frequency : 6, 46, 70, 48, 20, 2.

Calculate  $\chi^2$ . (M.U. 2002)

Sol. : Assuming that all 5 dice are fair, probability of getting 4, 5 or 6 in throw of single die is 1/2.  
 ∴ By Binomial Theorem, probability distribution is given by

$${}^5 C_x \left(\frac{1}{2}\right)^x \left(\frac{1}{2}\right)^{5-x}, \quad x = 0, 1, 2, 3, 4, 5.$$

The number of times getting  $x = 0, 1, 2, 3, 4, 5$  is given by

$$192 \cdot {}^5 C_x \left(\frac{1}{2}\right)^x \left(\frac{1}{2}\right)^{5-x}$$

Thus, the expected frequencies are given as

No. of successes : 5, 4, 3, 2, 1, 0.

Exp. frequency : 6, 30, 60, 60, 30, 6.

Obs. frequency : 6, 46, 70, 48, 20, 2.

$\frac{(O - E)^2}{E}$  : 0, 256, 100, 144, 100, 16.

$\frac{(O - E)^2}{E}$  : 0, 8.53, 1.67, 2.40, 1.67, 2.67. ∴  $\chi^2 = \sum \frac{(O - E)^2}{E} = 16.94$

**13. Hypothesis Concerning Several Proportions**

If we want to test the equality of parameter  $p$  of several Binomial distributions we have to use  $\chi^2$ -test as explained below.

For example, if we want to test the consumer responses to several products of the same kind, to test the proportion of defective parts produced on different machines. We assume that the proportion of items having a particular characteristic is same in all samples. On the basis of this assumption, we calculate the expected  $E$  frequency of each cell. Then as usual we calculate

$$\chi^2 = \sum \frac{(O - E)^2}{E}.$$

We compare this calculated value with the table value. If the calculated value is less than the table value, we accept the hypothesis that the proportion is same otherwise we reject it.

**Example 1:** Samples of three shipments A, B, C of defective items gave the following results.

	Shipment A	Shipment B	Shipment C	Total
Defective	5	8	9	21
Non-defective	35	42	51	129
Total	40	50	60	150

Test whether the proportion of defective items is same in the three shipments at 0.05 level of significance.

Sol.: (i) Null Hypothesis  $H_0 : p_1 = p_2 = p_3$ .

Alternative Hypothesis  $H_A : p_1 \neq p_2 \neq p_3$ .

(ii) Calculation of test statistic : If the proportion of defective item is same in the three shipments

then there will be  $\frac{40 \times 21}{150} = 5.6$  defective items in shipment A and the remaining  $40 - 5.6 = 34.4$  non-defective. In the same way defectives in B =  $\frac{50 \times 21}{150} = 7$  and remaining  $50 - 7 = 43$

non-defective. Defective in C =  $\frac{60 \times 21}{150} = 8.4$  and remaining  $60 - 8.4 = 51.6$  non-defective.

**Calculation of  $\chi^2$**

O	E	$(O - E)^2$	$(O - E)^2 / E$
5	5.6	0.36	0.064
35	34.4	0.36	0.029
8	7.0	1.00	0.143
42	43.0	1.00	0.023
9	8.4	0.36	0.043
51	51.6	0.36	0.007
$\chi^2 = 0.309$			

(iii) Level of significance :  $\alpha = 0.05$ .

Degrees of freedom =  $(r - 1)(c - 1) = (2 - 1)(3 - 1) = 2$ .

(iv) Critical value : For 2 degrees of freedom and 5% level of significance, the table value of  $\chi^2 = 5.991$ .

(v) Decision : Since the calculated value of  $\chi^2 = 0.309$  is less than the table value of  $\chi^2 = 5.991$ , the hypothesis is accepted.

∴ Proportion of defective is same in all shipments.

**Example 2 :** An item is produced on four machines and inspection of samples of these items show the following results.

	M - 1	M - 2	M - 3	M - 4	Total
Grade I	30	42	32	45	149
Grade II	20	18	18	15	71
Total	50	60	50	60	220

Test at 0.05 level of significance whether the proportion of Grade I items is same in the production of all machines.

Sol.: (i) Null Hypothesis  $H_0 : p_1 = p_2 = p_3 = p_4$ .

Alternative Hypothesis  $H_A : p_1 \neq p_2 \neq p_3 \neq p_4$ .

(ii) Calculation of test statistic : If the proportion of Grade I item is same in the production of all machines then there will be  $\frac{50 \times 149}{220} = 33.86$  items of grade I in the production of machine

M - 1 and the remaining  $50 - 33.86 = 16.14$ . In the same way,

Grade I items in B =  $\frac{60 \times 149}{220} = 40.64$  and remaining  $60 - 40.64 = 19.36$ .

Grade I items in C =  $\frac{50 \times 149}{220} = 33.86$ , remaining  $50 - 33.86 = 16.14$ .

Grade I items in D =  $\frac{60 \times 149}{220} = 40.64$  and remaining  $60 - 40.64 = 19.36$ .

**Calculation of  $\chi^2$**

O	E	$(O - E)^2$	$(O - E)^2 / E$
30	33.86	14.90	0.30
20	16.14	14.90	0.92
42	40.64	1.85	0.05
18	19.36	1.85	0.09
32	33.86	3.46	0.10
18	16.14	3.46	0.21
45	40.64	19.01	0.47
15	19.36	19.01	0.98
$\chi^2 = 3.12$			

(iii) Level of significance :  $\alpha = 0.05$ .

Degrees of freedom =  $(r - 1)(c - 1) = (2 - 1)(4 - 1) = 3$ .

- (iv) Critical value : For 3 degrees of freedom and 5% level of significance, the table value of  $\chi^2 = 7.815$ .
- (v) Decision : Since the calculated value of  $\chi^2 = 3.12$  is less than the table value of  $\chi^2 = 7.815$ , the hypothesis is accepted.  
 $\therefore$  Proportion of Grade I items is same for all machines.

**EXERCISE - IV****Type I : Independence of Attributes**

1. In an experiment on immunisation of cattle from Tuberculosis the following results were obtained.

	Affected	Not affected	Total
Inoculated	267	27	294
Not inoculated	757	155	912
Total	1024	182	1206

Use  $\chi^2$ -test to determine the efficacy of vaccine in preventing tuberculosis. (M.U. 2018)  
[ Ans. :  $\chi^2 = 10.19$ , d.f. =  $(2-1)(2-1) = 1$ , Table value of  $\chi^2 = 3.84$ , Effective ]

2. Based on the following data determine if there is a relation between literacy and smoking.

Smokers	Non-smokers	
Literates	63	57
Illiterates	45	68

(M.U. 2008) [ Ans. :  $\chi^2 = 9.19$ , Yes ]

3. A total of 3759 individuals were interviewed in a public opinion survey on a political proposal. Of them 1872 were men and the rest were women. A total of 2257 individuals were in favour of the proposal and 917 were opposed to it. A total of 243 men were undecided and 442 women were opposed to it. Do you justify or contradict the hypothesis that there is no association between sex and attitude at 5% level of significance. (M.U. 2007, 09, 14)

[ Ans. :  $\chi^2 = 18.76$ , Sex and attitude are associated. ]

4. A sample of 300 students of under-graduate and 300 students of post-graduate classes of a university were asked to give their opinion on autonomy of colleges. 190 of the under graduate and 210 of the post-graduate students favoured autonomous states.

Present the above facts in the form of a frequency table and test at 5% level the opinions of under-graduate and post-graduate students on autonomous status of colleges are independent. (Table value of  $\chi^2$  at 5% level for 1 d.f. is 3.84)

[ Ans. :  $\chi^2 = 3$ , Independent ]

5. Out of 800 persons 25% were literate and 300 had travelled beyond the limits of the district. 40% of the literates were among those who had not travelled. Prepare a  $2 \times 2$  table and test at 5% level of significance whether there is any relation between travelling and literacy.

[ Ans. :  $\chi^2 = 57.6$ , There is a relation ]

6. In the contingency table given in adjoining table, use  $\chi^2$ -test for independence of hair colour and eye-colour of persons.

[ Ans. :  $\chi^2 = 57.6$ , There is a relation ]

Eye colour	Hair colour		
	Light	Dark	Total
Blue	26	9	35
Brown	7	18	25
Total	33	27	60

[ Ans. :  $\chi^2 = 13.59$ , d.f. = 1, Table value of  $\chi^2 = 3.84$ , Attributes are associated. ]

7. Calculate the expected frequencies for the following data presuming the two attributes viz. condition of home and condition of child independent.

Condition of child	Condition of Home	
	Clean	Dirty
Clean	70	50
Fairly clean	80	20
Dirty	35	45

Use  $\chi^2$ -test at 5% level to find whether the two attributes are independent. (Table value of  $\chi^2$  at 5% for 2, 3, 4 d.f.s. are 5.991, 7.815 and 9.488 respectively.)

[ Ans. :  $\chi^2 = 26.25$ , d.f. = 2, Not independent ]

8. A certain drug is claimed to be effective in curing fever in an experiment on 164 persons with fever. Half of them were given the drug and half were given sugar pills. The results obtained are shown in the following table. Test the hypothesis that the drug is effective in curing fever.

	Helped	Harmed	No effect	Total
Drug	52	10	20	82
Sugar pills	44	12	26	82
Total	96	22	46	164

[ Ans. :  $\chi^2 = 1.86$ , d.f. =  $(r-1)(c-1) = (3-1)(2-1) = 2$ . ]

Table value of  $\chi^2 = 5.99$ , Not effective. ]

9. The following table gives the information regarding the colour of hair and the colour of eye.

Eye colour	Hair colour			Total
	Black	Fair	Brown	
Brown	10	22	32	64
Blue	15	28	29	72
Grey	25	20	19	64
Total	50	70	80	200

Use  $\chi^2$ -test to check whether there is any association between the hair colour and eye colour.

[ Ans. :  $\chi^2 = 10.64$ , d.f. = 4, Table value of  $\chi^2 = 9.48$ , No ]

10. In an industry 200 workers employed for a specific job were classified according to their performance and training received to test independence of training received and performance. The data are summarised as follows.

## Applied Mathematics - IV

(9-43)

Performance	Trained	Untrained	Total
Good	100	20	120
Not good	50	30	80
Total	150	50	200

Use  $\chi^2$ -test for independence at 5% level of significance and write your conclusion.  
(Given  $\chi^2 = 3.84$  for 1 d.f.)

[Ans. :  $\chi^2 = 11.11$ , Training and performance are not independent]

11. Table below shows the performances of students in Mathematics and Physics. Test the hypothesis that the performance in Mathematics is independent of performance in Physics.

Grades in Physics	Grades in Maths		
	High	Medium	Low
High	56	71	12
Medium	47	163	38
Low	14	42	81

(M.U. 2014)

[Ans. :  $\chi^2 = 132.31$ , Table value of  $\chi^2$  at 5% level of significance for  $v = 4$  is 9.49. Reject the hypothesis.]

12. The result of a certain survey shows that out of 50 ordinary shops of small size 35 are managed by men of which 17 are in cities. 12 shops in villages are run by women. Can it be inferred that shops run by women are relatively more in villages than in cities?

Use  $\chi^2$ -test. (Table value of  $\chi^2$  for 1 d.f. is 3.84.)

[Ans. :  $\chi^2 = 3.57$ , No]

## Type II : Goodness of Fit

1. The following figures show the distribution of digits in numbers chosen at random from a telephone directory.

Digit : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.  
Freq. : 1026, 1107, 997, 986, 1075, 933, 1107, 972, 964, 853.

Test at 5% level whether digits may be taken to occur equally frequently in the directory. (Table value of  $\chi^2$  at 9 d.f. is 16.92.)

[Ans. :  $\chi^2 = 59.36$ , Yes]

2. The following table gives the number of accidents in a district during a week. Apply  $\chi^2$ -test to find whether the accidents are uniformly distributed over the week.

Day : Sun., Mon., Tues., Wed., Thur., Fri., Sat.  
No. of accidents : 13, 12, 11, 9, 15, 10, 14.

[Ans. :  $\chi^2 = 2.33$ , d.f. = 7 - 1 = 6. Table value of  $\chi^2 = 12.59$ , Yes]

3. The following data represent the monthly sales in ₹ of a certain retail store in a leap year. Examine if daily sales are uniform throughout the year.

6100, 6600, 6350, 6050, 6250, 6200,  
6300, 6250, 5800, 6000, 6150, 6150.

[Ans. :  $\chi^2 = 11.96$ , d.f. = 6 - 1 = 5. Table value of  $\chi^2 = 11.07$ , No]

## Small Sample Tests

## Applied Mathematics - IV

(9-44)

## Small Sample Tests

[Ans. :  $\bar{X} = 73200 / 366 = ₹ 200$  per day.

$E_1 = 200 \times 31 = 6200$  for Jan.,  $E_2 = 200 \times 29 = 5800$  for Feb. etc.

$\chi^2 = 40.6$ . Reject the hypothesis.]

4. According to a theory the proportion of a commodity in the four classes A, B, C, D should be 9:4:2:1. In a survey of 1800 items of this commodity the numbers in the four classes were 862, 422, 168 and 118. Does the survey support the theory?

(Hint : Expected frequencies in the four classes are

$$A = \frac{9}{16} \times 1800 = 900, B = 400, C = 200, D = 100.)$$

[Ans. :  $\chi^2 = 16.06$ , d.f. = 4 - 1 = 3, Table value of  $\chi^2 = 7.81$ , No]

5. Of the 64 offsprings of a certain cross between guinea pigs, 34 were red, 10 were black and 20 were white. According to genetic model these numbers should be in the ratio 9 : 3 : 4. Use  $\chi^2$ -test to check whether the data are consistent with the model.

[Ans. :  $\chi^2 = 1.31$ , d.f. = 2, Table value of  $\chi^2 = 5.99$ , Consistent.]

6. The following table shows the number of heads obtained when 5 coins were tossed 3200 times.

Heads : 0 1 2 3 4 5  
Frequency : 80 570 1100 900 500 50

Fit a Binomial distribution and test whether the coins are unbiased.

(Hint : Expected Frequencies are

$$= 3200 \cdot {}^5C_x \left(\frac{1}{2}\right)^x \left(\frac{1}{2}\right)^{5-x}, x = 0, 1, 2, 3, 4, 5.  
= 100, 500, 1000, 1000, 500, 100.)$$

[Ans. :  $\chi^2 = 58.8$ , d.f. = 5 - 1 = 4, Table value of  $\chi^2 = 11.07$ , No]

7. Twelve dice were thrown 4096 times and the number of appearance of 6 each time was noted. The results were recorded as follows :

No. of successes : 0, 1, 2, 3, 4, 5, 6 and above.

Frequency : 447, 1145, 1181, 796, 380, 115, 32.

Fit a Binomial distribution and test whether the dice are unbiased.

$$(Hint : Expected frequency = 4096 \times {}^{12}C_x \left(\frac{1}{6}\right)^x \left(\frac{5}{6}\right)^{12-x})$$

$$= 459, 1103, 1209, 803, 363, 117, 42.$$

where,  $x = 0, 1, 2, 3, 4, 5$ . The last frequency is obtained by subtracting the sum from 4096.)

[Ans. :  $\chi^2 = 6.18$ , d.f. = 7 - 1 = 6, Table value of  $\chi^2 = 12.59$ , Yes]

8. A survey of 320 families with 5 children revealed the distribution of boys as given below. Is the result consistent with the hypothesis that male and female births are equally probable?

No. of boys : 0 1 2 3 4 5  
No. of families : 8 40 88 110 56 18

$$(Hint : Expected frequencies = 320 \cdot {}^5C_x \left(\frac{1}{2}\right)^x \left(\frac{1}{2}\right)^{5-x} = 10, 50, 100, 100, 50, 10.)$$

[Ans. :  $\chi^2 = 11.96$ , d.f. = 6 - 1 = 5, Table value of  $\chi^2 = 11.07$ , No]

9. The following mistakes per page were observed in a book.

No. of mistakes per page	0	1	2	3	4	Total
No. of pages	17167	1861	124	2	1	19155

Fit a Poisson distribution and test the goodness of fit.

(Hint :  $\bar{X} = 0.11$ ,

$$\text{Expected frequencies} = 19155 \cdot e^{-0.11} \frac{(0.11)^x}{x!} = 17160, 1887, 104, 4, 0,$$

[Ans. :  $\chi^2 = 3.7$ , d.f. = 5 - 2 - 2 = 1, Table value of  $\chi^2 = 3.84$ . Fit is not good]

10. A list of wars of modern civilisation provided the following data for the period 1550-1981.

Fit a Poisson distribution to the data and test the goodness of fit.

No. of outbreaks in year	0	1	2	3	4	5	Total
No. of years	223	142	48	15	4	0	432

(Hint :  $\bar{X} = \frac{\sum f_x}{\sum f} = 0.69$ ,

$$\text{Expected frequencies} = 320 \cdot e^{-0.69} \frac{(0.69)^x}{x!} = 217, 149, 52, 12, 2, 0,$$

[Ans. :  $\chi^2 = 2.6$ , d.f. = 6 - 4 = 2, Table value of  $\chi^2 = 5.99$ , Fit is good.  
Combine the last three groups]

### EXERCISE - VI

#### Theory

- Write a short note on degrees of freedom in connection with the applications of  $\chi^2$ -test.
- Write two uses of  $\chi^2$ -test.
- What are the purposes for which  $\chi^2$ -tests of significance are used? Explain and illustrate.
- What is meant by parametric and non parametric tests?
- Explain  $r \times c$  table.
- Discuss the importance of  $\chi^2$ -test. How is it used to test independence of attributes? (M.U. 2000)
- Define student's  $t$ -distribution and state its properties. (M.U. 2001)
- Define  $\chi^2$  distribution and state its uses.
- State the uses of  $\chi^2$  test and the conditions for these uses. (M.U. 2005)
- What is test of "independence"?
- Why the test-statistics are different for large samples and small samples?
- What is the necessity of level of significance?
- What are type I and type II errors and how are they minimised?



## Correlation

### 1. Introduction

In Statistics so far we have studied problems involving a single variable. Many a time, we come across problems which involve two or more than two variables. Data relating to two variates are called **Bivariate Data**. If we study bivariate data carefully, we may find some relation between the two variables. For example, if a car-owner maintains the record of petrol consumption and mileage, he will find that there is some relation between the two variables. On the other hand, if we compare the figures of rainfall with the production of cars, we may find that there is no relation between the two variables. If there is any relation between two variables i.e. if as one variable changes the other also changes in the same or opposite direction, we say that they are correlated. Thus, correlation means "the study of existence and the magnitude and direction of variation between two or more variables".

### 2. Types of Correlation

Correlation may be classified as :

- Positive and negative,
- Linear and non-linear.

#### (1) Positive and Negative Correlation

The distinction between the positive and negative correlation depends upon the direction of change of two variables. If both the variables change in the same direction i.e. if, as one variable increases, the other also increases and as one variable decreases, the other also decreases, the correlation is called positive (e.g. advertising and sales). If, on the other hand, the variables change in opposite direction i.e. if, as one variable increases, the other decreases and vice-versa, then the correlation is called negative (e.g. T.V. registrations and cinema attendance).

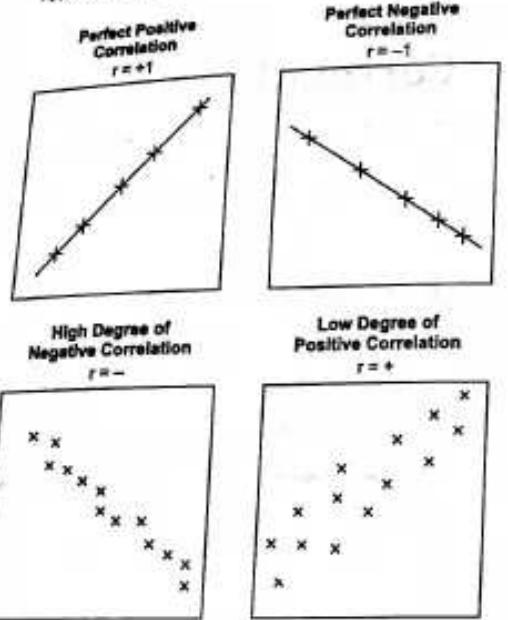
#### (2) Linear or Non-linear Correlation

This distinction is based upon the nature of the graph of the relation between the variables. If the graph is a straight line the correlation is called linear and if the graph is not a straight line but a curve it is called non-linear or curvi-linear correlation.

We shall consider the following commonly used methods of studying correlation. (1) Scatter Diagram, (2) Karl Pearson's Coefficient of Correlation, (3) Spearman's Rank-Correlation Coefficient.

### 3. Scatter Diagram

One of the most simple methods of studying correlation between two variables is to construct a scatter diagram.



To obtain a scatter diagram, one variable is plotted along the  $x$ -axis and the other along the  $y$ -axis, on a graph paper. By plotting data in this way, we get points which are generally scattered but which show a pattern. The way in which the points are scattered indicates the degree and direction of correlation. If the points are close to each other we infer that the variables are correlated. If they are spread away from each other, we infer that the variables are not correlated. Moreover, if the points lie in a narrow strip rising from left-hand bottom to the right-hand top, we say that there is positive correlation of high order. If the points lie in a narrow strip, falling from the left-hand top to the right-hand bottom, we say that there is negative correlation of high order. If the points are all spread over, we say that there is zero correlation.

#### 4. Karl Pearson's Coefficient of Correlation

The method of scatter diagram is descriptive in nature and gives only a general idea of correlation. The most commonly used method which gives a mathematical expression for correlation is the one suggested by Karl Pearson (1857-1936) a British Biometrist.

#### Karl Pearson (1857 - 1936)

Born in London, he went to King's College, Cambridge in 1876 to study mathematics graduating in 1879 as Third Wrangler in the Mathematical Tripos. He then went to Germany to study Physics at the University of Heidelberg. Other subjects he studied in Germany include metaphysics, physiology, Roman Law, German Literature and Socialism. He studied so many subjects because he believed that there was no subject in the universe unworthy of study. Then he returned to London to study Law, although he never practised. In 1881 he returned to mathematics and was appointed as professor of mathematics at University College, London. In 1881 he met Walter Weldon, a zoologist and worked with him in biometry and evolutionary theory. He was introduced to Galton, Darwins cousin and became Galton's statistical heir. He was the first holder of the Galton's Chair of Eugenics. In 1911 he founded the world's first university statistics department at University College, London. He remained with the department until his retirement in 1933 and continued to work until his death in 1936. He thus established the new discipline of mathematical statistics.

His famous book "The Grammar of Science" covers several themes that were later to become part of the theories of Einstein and other scientists. He speculated that an observer who travelled at the speed of light would see an eternal now and an observer who travelled faster than light would see time reversal. He also discussed antimatter, fourth dimension and wrinkles in time.

Karl Pearson was awarded many medals including The Darwin Medal, a DSc from university of London. His commitment to socialism and his ideals led him to refuse the honours of being an OBE (Officer of the Order of the British Empire) and knighthood in 1935.

Karl Pearson is known for Karl Pearson's coefficient of correlation, methods of moments, Pearson's system of continuous curves, Chi-distance, Statistical hypothesis testing theory, Statistical decision theory, Pearson's chi-square test, etc.



Just as  $\sigma_x^2 = \frac{1}{N} \sum (x - \bar{x})^2$  gives us a measure of variation in  $x$  and  $\sigma_y^2 = \frac{1}{N} \sum (y - \bar{y})^2$  gives a measure of variation in  $y$  we may expect  $\frac{1}{N} \sum (x - \bar{x})(y - \bar{y})$  to give the measure of simultaneous variation in  $x$  and  $y$ . But this will depend upon the units of  $x$  and  $y$ . To find a ratio which is independent of these units, we divide it by the quantities of the same order that is by  $\sigma_x \cdot \sigma_y$ . With this view in mind Karl Pearson suggested in 1890 the following coefficient of correlation to measure correlation between  $x$  and  $y$ . It is denoted by  $r$ .

Thus,

$$r = \frac{\sum (x - \bar{x})(y - \bar{y})}{N \sigma_x \sigma_y} \quad (1)$$

But  $\frac{1}{N} \sum (x - \bar{x})(y - \bar{y})$  is called the covariance between  $x$  and  $y$ . Hence, from (1), we have

$$r = \frac{\text{cov.}(x, y)}{\sigma_x \cdot \sigma_y} \quad (2)$$

If we put  $\sigma_x = \sqrt{\frac{\sum(x-\bar{x})^2}{N}}$ ,  $\sigma_y = \sqrt{\frac{\sum(y-\bar{y})^2}{N}}$ , then

$$r = \frac{\sum(x-\bar{x})(y-\bar{y})}{\sqrt{\sum(x-\bar{x})^2} \sqrt{\sum(y-\bar{y})^2}}$$

If we write  $x - \bar{x} = x'$ ,  $y - \bar{y} = y'$ , then

$$r = \frac{\sum x' y'}{\sqrt{\sum x'^2} \sqrt{\sum y'^2}}$$

The Karl Pearson's coefficient of correlation is also called the product moment coefficient of correlation.

Further, we can expand (3) and write

$$\begin{aligned} r &= \frac{\sum(xy - \bar{x}\bar{y} + \bar{x}\bar{y})}{\sqrt{\sum(x^2 - 2x\bar{x} + \bar{x}^2)} \cdot \sqrt{\sum(y^2 - 2y\bar{y} + \bar{y}^2)}} \\ &= \frac{\sum xy - \bar{y} \sum x - \bar{x} \sum y + \bar{x}\bar{y} \sum 1}{\sqrt{(\sum x^2 - 2\bar{x}\sum x + \bar{x}^2 \sum 1)} \cdot \sqrt{(\sum y^2 - 2\bar{y}\sum y + \bar{y}^2 \sum 1)}} \end{aligned}$$

But  $\sum x = N\bar{x}$ ,  $\sum y = N\bar{y}$  and  $\sum 1 = N$

$$r = \frac{\sum xy - N\bar{x}\bar{y}}{\sqrt{(\sum x^2 - N\bar{x}^2)} \cdot \sqrt{(\sum y^2 - N\bar{y}^2)}}$$

If  $\bar{x}, \bar{y}$  are integers we take deviations of  $x$  and  $y$  from them and use the formula (3). If we have to find  $r$  from direct values we use the formula (5). This is the most commonly used formula.

#### (i) Limits for $r$ : $-1 \leq r \leq 1$

Proof : If we write  $E(X) = \mu_X$ ,  $E(Y) = \mu_Y$ , then

(M.U. 2004)

$$\begin{aligned} E\left[\left(\frac{X-\mu_X}{\sigma_X}\right) \pm \left(\frac{Y-\mu_Y}{\sigma_Y}\right)\right]^2 &\geq 0 \\ \therefore E\left(\frac{X-\mu_X}{\sigma_X}\right)^2 + E\left(\frac{Y-\mu_Y}{\sigma_Y}\right)^2 \pm 2 \frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma_X \sigma_Y} &\geq 0 \\ \therefore 1 + 1 \pm 2r \geq 0 &\quad \therefore 1 \pm r \geq 0 \\ \therefore 1 + r \geq 0 &\quad \text{or} \quad 1 - r \geq 0 \\ \therefore 1 \geq r &\quad \text{or} \quad 1 \geq r \\ \therefore -1 \leq r &\quad \therefore -1 \leq r \leq 1 \quad [\because E(X-\mu_X)^2 = \sigma_X^2] \end{aligned}$$

#### (ii) Theorems on correlation

**Theorem 1 :** If  $x, y$  are independent variables they are not correlated.

We accept this theorem without proof.

**Theorem 2 :** Correlation coefficient is independent of change of origin and change of scale. (M.U. 2002, 07)

This means if we write  $u_i = \frac{x-a}{h}$ ,  $v_i = \frac{y-b}{k}$ , then

$$r_{xy} = r_{uv}$$

i.e., the correlation between  $x$  and  $y$  is equal to the correlation between  $u$  and  $v$ .  
We accept this theorem without proof.

**Remark :** The above theorem can also be stated as :-

"If  $x = au + b$ ,  $y = cv + d$  where  $a, b, c, d$  are constants then  $r_{xy} = r_{uv}$ ".

**Example :** Discuss the statement : "If the coefficient of correlation between  $x$  and  $y$  is negative then the coefficient of correlation between  $(-x)$  and  $(-y)$  is positive." (M.U. 1998)

Sol. : If we write  $a = 0$  and  $b = 0$ ,  $h = -1$  and  $k = -1$  in (A), then by the above theorem since  $r_{xy} = r_{uv}$  the coefficient of correlation between  $-x$  and  $-y$  will be also the same in magnitude and sign as the coefficient of correlation between  $x$  and  $y$ .

Or since the coefficient of correlation does not change under change of scale and since  $-x$  and  $-y$  mean the change of scale, the coefficient of correlation between  $-x$  and  $-y$  will be also negative.

**Theorem 3 :** If  $d_x$  and  $d_y$  denote the deviations of  $x$  and  $y$  from the assumed means  $A$  and  $B$  then

$$r = \frac{\sum d_x d_y - \frac{(\sum d_x)(\sum d_y)}{N}}{\sqrt{\sum d_x^2 - \frac{(\sum d_x)^2}{N}} \sqrt{\sum d_y^2 - \frac{(\sum d_y)^2}{N}}}$$

We accept this result without proof.

#### 5. Interpretation of the Coefficient of Correlation

1.  $r > 0.95$  : If  $r$  is greater than 0.95, it indicates high degree of correlation and the value of one variable can be estimated from a known value of the other fairly accurately.

2.  $r > 0.75$  but  $< 0.95$  : If  $r$  is greater than 0.75 but less than 0.95, there is probably a definite relationship between the variables and the value of one variable can be roughly estimated from a known value of the other.

3.  $r > 0.40$  but  $< 0.60$  : If  $r$  is greater than 0.40 but less than 0.60 there may be some relationship between the two variables. But the value of one variable calculated from a known value of the other cannot be reliable.

4.  $r < 0.35$  : If  $r$  is less than 0.35 the correlation is poor and one variable cannot be estimated from the other.

5.  $r$  nearly zero : If  $r$  is nearly equal to zero, it indicates that there is probably no relation between the two variables i.e. they are independent of each other.

#### 6. Computation of Coefficient of Correlation : (Ungrouped Data)

There are three methods of calculating  $r$ .

- (1) Actual mean method,
- (2) Step deviation method,
- (3) Assumed mean method.

Applied Mathematics - IV

(1) Actual Mean Method

The formula to be used is,

(10-6)

$$r = \frac{\sum xy}{\sqrt{\sum x^2 \cdot \sum y^2}}$$

Steps:

- Calculate mean  $\bar{X}$  and then take deviation  $x$  of  $X$  from  $\bar{X}$  i.e., calculate  $x = X - \bar{X}$ .
- Calculate mean  $\bar{Y}$  and then take deviation  $y$  of  $Y$  from  $\bar{Y}$  i.e., calculate  $y = Y - \bar{Y}$ .
- Multiply  $x$  by  $y$  and prepare the column of  $xy$ .
- Take the squares of  $x$  and prepare the column of  $x^2$ .
- Take the squares of  $y$  and prepare the column of  $y^2$ .
- Apply the above formula.

**Example 1:** Find from the following values of the demand and the corresponding price of a commodity, the degree of correlation between the demand and price by computing Karl Pearson's coefficient of correlation.

Demand in quintals : 65, 66, 67, 67, 68, 69, 70, 72.

Price in Paisa per k.g. : 67, 68, 65, 68, 72, 72, 69, 71.

Sol.: Let  $X$  denote the demand in Quintals and  $Y$  denote the price in paisa per kg.

Calculation of  $r$  between demand and price

Sr. No.	Demand in Qnt. $X - \bar{X}, \bar{X} = 68$			Price per Kg. $Y - \bar{Y}, \bar{Y} = 69$			Product
	$X$	$x$	$x^2$	$Y$	$y$	$y^2$	
1	65	-3	9	67	-2	4	6
2	66	-2	4	68	-1	1	2
3	67	-1	1	65	-4	16	4
4	67	-1	1	68	-1	1	1
5	68	0	0	72	+3	9	0
6	69	+1	1	72	+3	9	3
7	70	+2	4	69	0	0	0
8	72	+4	16	71	+2	4	8
N = 8	$\sum X = 544$	$\sum x^2 = 36$		$\sum Y = 552$	$\sum y^2 = 44$		$\sum xy = +24$

Now,  $\bar{X} = \frac{544}{8} = 68$  and  $\bar{Y} = \frac{552}{8} = 69$ .

$$\therefore r = \frac{\sum xy}{\sqrt{\sum x^2 \cdot \sum y^2}}$$

But  $\sum xy = 24$ ,  $\sum x^2 = 36$ ,  $\sum y^2 = 44$ .

$$\therefore r = \frac{24}{\sqrt{36 \times 44}} = \frac{24}{\sqrt{39.60}} = 0.6030.$$

**Example 2:** Calculate Karl Pearson's coefficient of correlation for the following bivariate series.

$X$  : 28, 45, 40, 38, 35, 33, 40, 32, 36, 33

$Y$  : 23, 34, 33, 34, 30, 26, 28, 31, 36, 35

(M.U. 2015)

Applied Mathematics - IV  
Correlation

(10-7)

Calculation of  $r$  between  $X$  and  $Y$

Sol.:

Sr. No.	$X - \bar{X}, \bar{X} = 36$			$Y - \bar{Y}, \bar{Y} = 31$			Product
	$X$	$x$	$x^2$	$Y$	$y$	$y^2$	
1	28	-8	64	23	-8	64	+64
2	45	+9	81	34	+3	9	+27
3	40	+4	16	33	+2	4	+8
4	38	+2	4	34	+3	9	+6
5	35	-1	1	30	-1	1	+1
6	33	-3	9	26	-5	25	-15
7	40	+4	16	28	-3	9	-12
8	32	-4	16	31	0	0	0
9	36	0	0	36	+5	25	0
10	33	-3	9	35	+4	16	-12
N = 10	$\sum X = 360$	$\sum x^2 = 216$		$\sum Y = 310$	$\sum y^2 = 162$		$\sum xy = +97$

Now,  $\bar{X} = \frac{360}{10} = 36$  and  $\bar{Y} = \frac{310}{10} = 31$ .

$$\therefore r = \frac{\sum xy}{\sqrt{\sum x^2 \cdot \sum y^2}}$$

But  $\sum xy = 97$ ,  $\sum x^2 = 216$ ,  $\sum y^2 = 162$ .

$$\therefore r = \frac{97}{\sqrt{216 \times 162}} = \frac{97}{\sqrt{36 \times 180}} = 0.5186.$$

(2) Step-deviation Method

As in the case of mean and standard deviation, to simplify calculations we can use step-deviation method whenever possible for calculating  $r$ . But it should be noted that the result is not to be multiplied by the constant in the final stage. The reason is the coefficient of correlation is independent of change of origin and change of scale. (See Theorem 2 of  $r$ , page 11-4)

**Example 1:** Calculate the co-efficient of correlation from the following data.

$X$ : 100, 200, 300, 400, 500.

$Y$ : 30, 40, 50, 60, 70.

(M.U. 2015)

Sol.:

Calculations of  $r$  between  $X$  and  $Y$

Sr. No.	$X - \bar{X}$				$Y - \bar{Y}$				Product
	$X = 300, X - \bar{X} = 100$	$X - 300$	$x$	$x^2$	$Y = 50, Y - \bar{Y} = 10$	$Y - 50$	$y$	$y^2$	
1	100	-200	-2	4	30	-20	-2	4	4
2	200	-100	-1	1	40	-10	-1	1	1
3	300	0	0	0	50	0	0	0	0
4	400	100	1	1	60	10	1	1	1
5	500	200	2	4	70	20	2	4	4
N = 5	$\sum X = 1500$	$\sum x^2 = 10$			$\sum Y = 250$	$\sum y^2 = 10$			$\sum xy = 10$

(10-8)

$$\text{Now } \bar{x} = \frac{1500}{5} = 300 \text{ and } \bar{y} = \frac{250}{5} = 50$$

$$r = \frac{\sum xy}{\sqrt{\sum x^2 + \sum y^2}}$$

$$\text{But } \sum xy = 10, \sum x^2 = 10, \sum y^2 = 10$$

$$r = \frac{10}{\sqrt{10 \times 10}} = \frac{10}{10} = +1.$$

## (ii) Assumed Mean Method

Since in the calculation of  $r$ , deviations are to be squared the calculations will be tedious if means are not integers but data are in integers. In such cases, we take deviations from an assumed mean conveniently chosen. The corresponding formula is

$$r = \frac{\sum d_x d_y - \frac{(\sum d_x)(\sum d_y)}{N}}{\sqrt{\sum d_x^2 - \frac{(\sum d_x)^2}{N}} \sqrt{\sum d_y^2 - \frac{(\sum d_y)^2}{N}}}$$

where,  $d_x$  = deviations of  $X$  from an assumed mean, ( $X - A$ ),  
 $d_y$  = deviations of  $Y$  from an assumed mean, ( $Y - B$ ),  
 $N$  = Number of pairs of observations.

## Steps :

- Assume any mean  $A$  for  $X$  and calculate deviations  $d_x$  of  $X$  from  $A$  i.e.,  $d_x = X - A$ .
- Assume any mean  $B$  for  $Y$  and calculate deviations  $d_y$  of  $Y$  from  $B$  i.e.,  $d_y = Y - B$ .
- Take the squares of  $d_x$ .
- Take the squares of  $d_y$ .
- Take the products of  $d_x$  and  $d_y$ .
- Apply the formula.

**Example 4 :** Find the co-efficient of correlation for the prices (in Rs.) and sales units.

Price in Rs. : 100, 98, 85, 92, 90, 84, 86, 90, 93, 95.

Sales Units : 500, 610, 700, 630, 670, 800, 800, 750, 700, 690.

Sol.: Let us assume 92 and 670 to be the means of  $X$  and  $Y$  respectively.

Calculations of  $r$  between price and sale

Sr. No.	Price in Rs. ( $X - 92$ )			Sales Units ( $Y - 670$ )			Product $d_x d_y$
	$X$	$d_x$	$d_x^2$	$Y$	$d_y$	$d_y^2$	
1	100	+8	64	500	-170	28900	-1360
2	98	+6	36	610	-60	3600	-360
3	85	-7	49	700	+30	900	-210
4	92	0	0	630	-40	1600	0
5	90	-2	4	670	0	0	0
6	84	-8	64	800	+130	16900	-1040
7	68	-4	16	800	+130	16900	-520
8	90	-2	4	750	+80	6400	-160
9	93	+1	1	700	+30	900	+30
10	85	+3	9	690	+20	400	+40
$N = 10$		$\sum d_x = -5$	$\sum d_x^2 = 247$	$\sum d_y = 150$	$\sum d_y^2 = 76500$		$\sum d_x d_y = -3560$

(10-9)

(10-9)

$$\text{Now, } r = \frac{\sum d_x d_y - \frac{(\sum d_x)(\sum d_y)}{N}}{\sqrt{\sum d_x^2 - \frac{(\sum d_x)^2}{N}} \sqrt{\sum d_y^2 - \frac{(\sum d_y)^2}{N}}}$$

$$\text{But, } \sum d_x d_y = -3560, \sum d_x = -5, \sum d_y = 150$$

$$N = 10, \sum d_x^2 = 247, \sum d_y^2 = 76500$$

$$= \frac{-3560 - (-5) \times (150)}{10}$$

$$= \frac{25}{247} \sqrt{76500 - 22500}$$

$$= \frac{25}{247} \times 2 \cdot 5 \sqrt{76500 - 22500}$$

$$= \frac{3485}{2445} \sqrt{74250}$$

$$= \frac{3485}{4261} = -0.8179$$

**Example 5 :** Calculate the correlation coefficient from the following data.

$X : 23, 27, 28, 29, 30, 31, 33, 36, 38, 39$ .

$Y : 18, 22, 23, 24, 25, 26, 28, 29, 30, 32$ .

(M.U. 2004, 14)

Sol.: Let us assume 30 and 25 to be the means of  $x$  and  $y$  respectively.

Calculation of  $r$  between  $X$  and  $Y$ 

Sr. No.	$(X - 30)$			$(Y - 25)$			Product $d_x d_y$
	$X$	$d_x$	$d_x^2$	$Y$	$d_y$	$d_y^2$	
1	23	-7	49	18	-7	49	49
2	27	-3	9	22	-3	9	9
3	28	-2	4	23	-2	4	4
4	29	-1	1	24	-1	1	1
5	30	0	0	25	0	0	0
6	31	+1	1	26	+1	1	1
7	33	+3	9	28	+3	9	9
8	35	+5	25	29	+4	16	20
9	36	+6	36	30	+5	25	30
10	38	+8	64	32	+7	49	56
$N = 10$		$\sum d_x = -7$	$\sum d_x^2 = 215$		$\sum d_y = 7$	$\sum d_y^2 = 163$	$\sum d_x d_y = -106$

$$\text{Now, } r = \frac{\sum d_x d_y - \frac{(\sum d_x)(\sum d_y)}{N}}{\sqrt{\sum d_x^2 - \frac{(\sum d_x)^2}{N}} \sqrt{\sum d_y^2 - \frac{(\sum d_y)^2}{N}}}$$

But,  $\sum d_x d_y = 186$ ,  $\sum d_x = 11$ ,  $\sum d_y = 7$   
 $N = 10$ ,  $\sum d_x^2 = 215$ ,  $\sum d_y^2 = 163$ .

$$\therefore r = \frac{186 - \frac{11 \times 7}{10}}{\sqrt{215 - \frac{(11)^2}{10}} \sqrt{163 - \frac{(7)^2}{10}}} = \frac{186 - 77}{\sqrt{215 - 12.1} \sqrt{163 - 4.9}} = \frac{178.3}{\sqrt{202.9} \sqrt{158.1}} = 0.9948$$

### 7. Direct Method of Calculating Coefficient of Correlation

We can find the coefficient of correlation directly without taking the deviations of  $x$  and  $y$  from their respective means. In such cases the following formula is used.

$$r = \frac{\sum xy - \frac{\sum x \sum y}{n}}{\sqrt{\left( \sum x^2 - \frac{(\sum x)^2}{n} \right) \left( \sum y^2 - \frac{(\sum y)^2}{n} \right)}} \quad (8)$$

where,  $x$  and  $y$  are the observed values of the variables and  $\bar{x}, \bar{y}$  are their respective means.

The formula can also be written as,

$$r = \frac{\sum xy - n \bar{x} \bar{y}}{\sqrt{n} \sqrt{\left( \frac{\sum x^2}{n} - \bar{x}^2 \right) \left( \frac{\sum y^2}{n} - \bar{y}^2 \right)}} \quad (9)$$

$$r = \frac{\sum xy - n \bar{x} \bar{y}}{n \sigma_x \sigma_y}$$

**Example 1:** Calculate the coefficient of correlation between  $X$  and  $Y$  from the following data.

$$\begin{array}{ccccc} X & : & 3 & , & 5 & , & 4 & , & 6 & , & 2 \\ Y & : & 3 & , & 4 & , & 5 & , & 2 & , & 6 \end{array}$$

Sol.:

Calculations of  $r$

$x$	$x^2$	$y$	$y^2$	$xy$
3	9	3	9	9
5	25	4	16	20
4	16	5	25	20
6	36	2	4	12
2	4	6	36	12
$\Sigma x = 20$	$\Sigma x^2 = 90$	$\Sigma y = 20$	$\Sigma y^2 = 90$	$\Sigma xy = 73$

Since,  $\bar{x} = 4$ ,  $\bar{y} = 4$  putting these values in equation (8).

$$\therefore r = \frac{73 - \frac{20^2}{5}}{\sqrt{90 - \frac{20^2}{5}} \sqrt{90 - \frac{20^2}{5}}} = \frac{73 - 80}{10} = -0.7.$$

### EXERCISE - I

1. Calculate the coefficient of correlation from the following data. Is there any marked correlation between the production and price of tea?

Production in crores (kgs)	:	34, 27, 31, 38, 38, 36, 39, 40.
Price in Rs. per kg	:	3.75, 4.62, 4.25, 4.12, 4.28, 4.32, 4.21, 4.05.

[Ans. :  $r = -0.48$ ]

2. Compute the coefficient of correlation between  $X$  and  $Y$  from their values given below.

$X$ : 30, 33, 25, 10, 33, 75, 40, 85, 90, 95.
$Y$ : 68, 65, 80, 85, 70, 30, 55, 18, 15, 10. (M.U. 2015) [Ans. : $r = -0.7069$ ]

3. The following data give the hardness ( $X$ ) and tensile strength ( $Y$ ) for some specimens of a material in certain units in a factory. Find the correlation coefficient and interpret your result.

$X$ : 23.3, 17.5, 17.8, 20.7, 18.1, 20.9, 22.9, 20.8.
$Y$ : 4.2, 3.8, 4.6, 3.2, 5.2, 4.7, 4.4, 5.6.

[Ans. :  $r = -0.072$ . No correlation.]

4. Calculate the product moment coefficient of correlation between the indices of business activity ( $X$ ) and employment ( $Y$ ) from the following data.

$X$ : 100, 102, 108, 111, 115, 116, 118.
$Y$ : 110, 100, 104, 108, 112, 116, 120. [Ans. : $r = 0.75$ ]

5. Find Karl Pearson's coefficient of correlation between  $X$  and  $Y$ .

$X$ : 10, 12, 14, 15, 16, 17, 18, 10, 14, 15
$Y$ : 17, 16, 15, 12, 10, 9, 8, 15, 13, 12 [Ans. : $r = -0.93$ ]

6. Compute a coefficient of correlation between  $X$  and  $Y$ .

$X$ : 3, 6, 4, 5, 7
$Y$ : 2, 4, 5, 3, 6 [Ans. : $r = 0.7$ ]

7. Calculate the coefficient of correlation between price and demand by direct method.

Price : 2, 3, 4, 7, 4
Demand : 8, 7, 3, 1, 1 [Ans. : $-0.81$ ]

8. Calculate the coefficient of correlation between  $X$  and  $Y$  by direct method.

$X$ : 8, 8, 7, 5, 6, 2
$Y$ : 3, 4, 10, 13, 22, 8 [Ans. : $0.2646$ ]

9. Soil temperature ( $x$ ) and Germination interval ( $y$ ) for winter wheat in 12 places are as follows.

$x$ (in $^{\circ}\text{F}$ ) : 57, 42, 38, 42, 45, 42, 44, 40, 46, 44, 43, 40.
--

$y$ (days) : 10, 26, 41, 29, 27, 27, 19, 18, 19, 31, 29, 33.
--

Calculate the coefficient of correlation between  $x$  and  $y$ . (M.U. 2015) [Ans. :  $r = -0.74$ ]

10. Find the Karl Pearson's coefficient of correlation between  $X$  and  $Y$  from the following.
- $X$ : 51, 54, 56, 59, 65, 60, 70  
 $Y$ : 38, 44, 33, 36, 33, 23, 13
- [Ans.:  $r = -0.7977$ ]

### 8. Spearman's Rank Correlation

The method developed by Spearman is simpler than Karl Pearson's method since, it depends upon ranks of the items and actual values of the items are not required. Hence, this can be used to study correlation even when actual values are not known. For instance we can study correlation between intelligence and honesty by this method.

Let  $x_i, y_i$  be the ranks in the two characteristics of the  $i$ -th member where  $i = 1, 2, \dots, n$ . We assume that no two members have the same rank either for  $x$  or for  $y$ . Thus,  $x$  and  $y$  take all integral values between 1 and  $n$ .

$$\therefore \bar{x} = \frac{1}{2}(1+2+3+\dots+n) = \frac{n+1}{2}$$

$$\text{Similarly, } \bar{y} = \frac{1}{2}(1+2+3+\dots+n) = \frac{n+1}{2} \quad \therefore \bar{x} = \bar{y}$$

$$\begin{aligned} \therefore \sum(x_i - \bar{x})^2 &= \sum(x_i^2 - 2x_i\bar{x} + \bar{x}^2) = \sum x_i^2 - 2\bar{x}\sum x_i + \bar{x}^2 \Sigma 1 \\ &= \sum x_i^2 - 2n\bar{x}^2 + n\bar{x}^2 = \sum x_i^2 - n\bar{x}^2 \\ &= (1^2 + 2^2 + \dots + n^2) - n\left(\frac{n+1}{2}\right)^2 \end{aligned}$$

$$\therefore \sum(x_i - \bar{x})^2 = \frac{n}{6}(n+1)(2n+1) - \frac{n(n+1)^2}{4} = \frac{1}{12}(n^3 - n)$$

$$\text{Similarly, } \sum(y_i - \bar{y})^2 = \frac{1}{12}(n^3 - n).$$

If  $d_i$  denotes the difference between the ranks of  $i$ -th member in the two variables, we have

$$d_i = (x_i - \bar{x}) - (y_i - \bar{y}) = x_i' - y_i' \text{ (since, } \bar{x}, \bar{y} \text{ are equal)}$$

where,  $x_i', y_i'$  denote the deviations of  $x_i, y_i$  from their means  $\bar{x}, \bar{y}$  respectively.

$$\therefore \sum d_i^2 = \sum x_i'^2 + \sum y_i'^2 - 2\sum x_i' y_i'$$

$$\therefore \sum d_i^2 = \frac{1}{12}(n^3 - n) + \frac{1}{12}(n^3 - n) - 2\sum x_i' y_i'$$

$$\therefore \sum x_i' y_i' = \frac{1}{2} \left[ \frac{n^3 - n}{6} - \sum d_i^2 \right]$$

But the coefficient of correlation

$$\begin{aligned} &= \frac{\sum x_i' y_i'}{\sqrt{\sum x_i'^2 + \sum y_i'^2}} = \frac{\frac{1}{2} \left[ \frac{n^3 - n}{6} - \sum d_i^2 \right]}{\frac{1}{12}(n^3 - n)} = 1 - \frac{6 \sum d_i^2}{n^3 - n} \end{aligned}$$

This coefficient is denoted by  $R$

$$\therefore R = 1 - \frac{6 \sum d_i^2}{n^3 - n}. \quad (10)$$

The value of  $R$ , as of  $r$ , lies between +1 and -1. If  $R = +1$ , there is perfect positive correlation i.e. there is complete agreement in the same direction. If  $R = -1$ , there is perfect negative correlation i.e. there is complete agreement but in opposite direction. Generally, the value of  $R$  is neither +1 nor -1 but lies somewhere in between. If  $R = 0$ , there is no correlation between  $X$  and  $Y$ .

Charles Edward Spearman (1863 - 1945)



He was greatly influenced by the work of Galton. He did pioneering work in psychology and developed correlation coefficient known by his name.

#### (a) Interpretation of $R = +1$ and $R = -1$

Two values of  $R$  need special attention. They are +1 and -1.  $R = +1$ , when the scatter diagram is a straight line rising to the right. In this case the ranks of the value of  $X$  are the same as the ranks of the values of  $Y$ .  $R = -1$ , when the scatter diagram is a straight line falling to right. In this case, when the ranks of the values of  $X$  go on increasing in order, the ranks of the corresponding values of  $Y$  go on decreasing in the same order.

For example, consider the following data.

$R = +1$			
$X$	$Y$	$R_1$	$R_2$
8	115	1	1
11	120	2	2
14	125	3	3
17	130	4	4
20	135	5	5

$R = -1$			
$X$	$Y$	$R_1$	$R_2$
8	135	1	5
11	130	2	4
14	125	3	3
17	120	4	2
20	115	5	1

Note ...

When the scatter diagram is a straight line  $r = +1$  or  $-1$  and also  $R = +1$  or  $-1$ .

#### (b) Relation between Spearman's Rank Correlation Coefficient $R$ and Karl Pearson's Correlation Coefficient $r$ .

Generally, for a given distribution the values of Spearman's rank correlation coefficient and Karl Pearson's correlation coefficient are different. Although both of them lie between +1 and -1, but actual values of the two coefficients for a given distribution are different. However, if the data are such that if the values of the two variables  $x$  and  $y$  are arranged in either ascending or descending

order and if they are found to increase or decrease by the equal amount i.e., if the difference between two values of  $x$  and the difference between the corresponding two values of  $y$  is constant, then the two values of  $R$  and  $r$  are equal. This is illustrated by the following example.

**Example 1 :** Calculate  $R$  and  $r$  from the following data.

$$\begin{array}{cccccc} X : & 12 & 17 & 22 & 27 & 32 \\ Y : & 113 & 119 & 117 & 115 & 121 \end{array}$$

Interpret your result.

Sol.:

#### Calculation of $R$ and $r$

Sr. No.	$X - \bar{X}$			$Y - \bar{Y}$			$XY$	$R_1$	$R_2$	$(R_1 - R_2)^2$
	$X$	$x$	$x^2$	$Y$	$y$	$y^2$				
1	12	-10	100	117	-4	16	40	5	5	0
2	17	-5	25	119	2	4	-10	4	2	4
3	22	0	0	117	0	0	0	3	3	0
4	27	5	25	115	-2	4	-10	2	4	4
5	32	10	100	121	4	16	40	1	1	0
$N=5$	110	250	585	586	40	60				8

$$R = 1 - \frac{6 \sum D^2}{N^3 - N} = 1 - \frac{6 \times 8}{125 - 5} = 0.6; \quad \bar{X} = \frac{110}{5} = 22, \quad \bar{Y} = \frac{586}{5} = 117$$

$$r = \frac{\sum xy}{\sqrt{\sum x^2 \cdot \sum y^2}} = \frac{60}{\sqrt{250 \cdot 40}} = 0.6.$$

Thus, the values of  $R$  and  $r$  are equal. It should be noted that the values of  $X$  increase by 5 and the values of  $Y$ , when arranged in ascending order also increase by the same amount 2 every time.

In general, if the values of  $x$ , when arranged in ascending order increase (or decrease) by a fixed amount and if the values of  $y$ , when arranged in ascending order increase (or decrease) by another (or the same) fixed amount, then the values of  $r$  and  $R$  come out to be equal.

#### (c) Computation of Correlation

There are two types of problems.

- (i) When ranks of items are given.
- (ii) When the actual values of the items are given.

##### (i) When ranks are given :

**Steps :** (i) Calculate the difference  $D = R_1 - R_2$ .

(ii) Calculate :  $D^2$ .

(iii) Apply the formula,  $R = 1 - \frac{6 \sum D^2}{N^3 - N}$ .

(ii) When the actual values are given : We first ascertain the ranks of all items and follow the above procedure.

**Example 1 :** Compute Spearman's rank correlation coefficient from the following data.

$$X : 18 \ 20 \ 34 \ 52 \ 12$$

$$Y : 39 \ 23 \ 35 \ 18 \ 46$$

(M.U. 2016)

Sol. : First we give ranks to the data in descending order and then calculate  $D^2 = (R_1 - R_2)^2$ .

#### Calculation of $R$ between $X$ and $Y$

Serial No.	$X$	$R_1$	$Y$	$R_2$	$D^2$ $(R_1 - R_2)^2$
1	18	4	39	2	4
2	20	3	23	4	1
3	34	2	35	3	1
4	52	1	18	5	16
5	12	5	46	1	16
$N=5$					$\Sigma D^2 = 38$

$$\therefore R = 1 - \frac{6 \sum D^2}{N^3 - N} \quad \text{Here, } \Sigma D^2 = 38, \quad N = 5.$$

$$\therefore R = 1 - \frac{6 \times 38}{125 - 5} = 1 - \frac{228}{120} = 1 - 1.9 = -0.9$$

**Example 2 :** Calculate the rank correlation coefficient from the following data, relating to the ranks of 10 students in English and Mathematics.

Student No. : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

Rank in English : 1, 3, 7, 5, 4, 6, 2, 10, 9, 8.

Rank in Mathematics : 3, 1, 4, 5, 6, 9, 7, 8, 10, 2.

#### Calculation of $R$ between English and Mathematics

Student No.	Rank in English $R_1$	Rank in Mathematics $R_2$	$D^2$ $(R_1 - R_2)^2$
1	1	3	4
2	3	1	4
3	7	4	9
4	5	5	0
5	4	6	4
6	6	9	9
7	2	7	25
8	10	8	4
9	9	10	1
10	8	2	36
$N=10$			$\Sigma D^2 = 96$

$$\text{Now, } R = 1 - \frac{6 \sum D^2}{N^3 - N} \quad \therefore \Sigma D^2 = 96, \quad N = 10$$

$$\therefore R = 1 - \frac{6 \times 96}{990} = 1 - \frac{96}{165} = 1 - 0.5819 = 0.4181$$

**Example 3 :** Calculate Spearman's coefficient of rank correlation from the data on height and weight of eight students.

Height (in inches) : 60 62 64 66 68 70 72 74  
Weight (in lbs.) : 92 83 101 110 128 119 137 146

(M.U. 2016)

Sol.:

Serial No.	Height	Rank $R_1$	Weight	Rank $R_2$	$D^2$ $(R_1 - R_2)^2$
1	60	1	92	2	1
2	62	2	83	1	1
3	64	3	101	3	0
4	66	4	110	4	0
5	68	5	128	6	1
6	70	6	119	5	1
7	72	7	137	7	0
8	74	8	146	8	0
$N = 8$					
$\sum D^2 = 4$					

$$\text{Now, } R = 1 - \frac{6 \sum D^2}{N^2 - N} \quad \therefore \sum D^2 = 4, N = 8$$

$$\therefore R = 1 - \frac{6 \times 4}{512 - 8} = 1 - \frac{24}{504} = 1 - 0.048 = 0.952$$

#### (d) Equal Ranks

In some cases it may happen that there is a tie between two or more members i.e., they have equal values and hence equal ranks. In such cases we divide the rank among equal members. For instance, if two items have 4th rank we divide the 4th and the next rank 5th between them equally and give  $\frac{4+5}{2} = 4.5$ th rank to each of them. If three items have the same 4th rank, we give each of them  $\frac{4+5+6}{3} = 5$ th rank.

After assigning ranks in this way an adjustment is necessary. If  $m$  is the number of items having equal ranks then the factor  $\frac{1}{12}(m^3 - m)$  is added to  $\sum d_i^2$ . If there are more than one cases of this type this factor is added corresponding to each case. Then,

$$R = 1 - \frac{6 \left[ \sum d_i^2 + \frac{1}{12} (m_1^3 - m_1) + \frac{1}{12} (m_2^3 - m_2) + \dots \right]}{n^3 - n}$$

**Example 1 :** Obtain the rank correlation coefficient from the following data.

X : 10, 12, 18, 18, 15, 40.

Y : 12, 18, 25, 25, 50, 25.

(M.U. 2004, 05, 10, 14)

#### Calculation of R

X	Rank $R_1$	Y	Rank $R_2$	$D^2$ $(R_1 - R_2)^2$
10	1	12	1	0.00
12	2	18	2	0.00
18	4.5	25	4	0.25
18	4.5	25	4	0.25
15	3	50	6	9.00
40	6	25	4	4.00
$N = 6$				$\sum D^2 = 13.50$

There are two items in X series having equal values at the rank 4. Each is given the rank  $\frac{4+5}{2} = 4.5$ . Similarly, there are three items in Y series at the rank 3. Each of them is given the rank  $\frac{3+4+5}{3} = 4$ .

$$R = 1 - \frac{6 \left[ \sum d_i^2 + \frac{1}{12} (m_1^3 - m_1) + \frac{1}{12} (m_2^3 - m_2) \right]}{n^3 - n}$$

Since,  $\sum D^2 = 13.50$ ,  $m_1 = 2$ ,  $m_2 = 3$ ,  $N = 6$ ,

$$R = 1 - \frac{6 \left[ 13.50 + \frac{1}{12} (8 - 2) + \frac{1}{12} (27 - 3) \right]}{216 - 6} = 1 - 0.4571 = 0.5429.$$

**Example 2 :** Calculate the value of rank correlation coefficient from the following data regarding marks of 6 students in statistics and accountancy in a test :

Marks in Statistics : 40, 42, 45, 35, 36, 39.

Marks in Accountancy : 46, 43, 44, 39, 40, 43.

(M.U. 2014, 17)

Sol.:

X	$R_1$	Y	$R_2$	$D^2$ $(R_1 - R_2)^2$
40	3	46	1	4.00
42	2	43	3.5	2.25
45	1	44	2	1.00
35	6	39	6	0.00
36	5	40	5	0.00
39	4	43	3.5	0.25
$N = 6$				$\sum D^2 = 7.50$

$$R = 1 - \frac{6 \left[ \sum D^2 + \frac{1}{12} (2^3 - 2) \right]}{N^3 - N} = 1 - \frac{6 (7.5 + 0.5)}{216 - 6}$$

$$= 1 - \frac{48}{210} = 1 - 0.229 = 0.771$$

**Example 3 :** From the following data calculate the coefficient of rank correlation between  $X$  and  $Y$ .

$X : 32, 55, 49, 60, 43, 37, 43, 49, 10, 20.$   
 $Y : 40, 30, 70, 20, 30, 50, 72, 60, 45, 25.$

Sol.:

Calculation of  $R$  between  $X$  and  $Y$ 

(M.U. 2018, 17)

$X$	$R_1$	$Y$	$R_2$	$D^2$ $(R_1 - R_2)^2$
32	3	40	5	4.00
55	9	30	3.5	30.25
49	7.5	70	9	2.25
60	10	20	1	81.00
43	5.5	30	3.5	4.00
37	4	50	7	9.00
43	5.5	72	10	20.25
49	7.5	60	8	0.25
10	1	45	6	25.00
20	2	25	2	0
$N = 10$				$\sum D^2 = 176$

Since there are two items in the  $X$  series having equal values at the rank 5 and 7 they are given rank 5.5 and 7.5 each respectively. Similarly, in the  $Y$  series two items at the rank 3 are given the rank 3.5 each. There are three cases where there is a tie each having 2 times.

$$\therefore R = 1 - \frac{6 \left\{ \sum D^2 + \frac{1}{12} (m_1^3 - m_1) + \frac{1}{12} (m_2^3 - m_2) + \frac{1}{12} (m_3^3 - m_3) \right\}}{N^3 - N}$$

But,  $\sum D^2 = 176$ ,  $m_1 = m_2 = m_3 = 2$ ,  $N = 10$ 

$$\therefore R = 1 - \frac{6 \left[ 176 + \frac{1}{12} (8 - 2) + \frac{1}{12} (8 - 2) + \frac{1}{12} (8 - 2) \right]}{1000 - 10}$$

$$= 1 - \frac{6(177.5)}{990} = 1 - 1.076 = -0.076.$$

**EXERCISE - II**

1. Sixteen industries of the State have been ranked as follows according to profits earned in 1980 - 81 and the working capital for the year. Calculate the rank correlation coefficient.

Industry : A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P.  
Rank (Profit) : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16.  
Rank (Capital) : 13, 16, 14, 15, 10, 12, 4, 11, 5, 9, 8, 3, 1, 6, 7, 2

[Ans. :  $R = -0.916$ ]

2. Distribution of marks in Economics and Mathematics for ten students in a certain test are given below :

Student No. : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.  
Marks in Eco. : 25, 28, 32, 36, 38, 40, 39, 42, 41, 45.  
Marks in Maths. : 70, 80, 65, 75, 59, 65, 48, 50, 54, 66.

Calculate the value of Spearman's Rank correlation coefficient.

[Ans. :  $-0.636$ ]

3. Calculate Spearman's coefficient of rank correlation for the following data.

$X : 53, 98, 95, 81, 75, 61, 59, 58.$   
 $Y : 47, 25, 32, 37, 30, 40, 39, 45.$

[Ans. :  $R = 0.9048$ ]

4. Calculate Spearman's coefficient of rank correlation from the following data.

$X : 35, 38, 43, 30, 54, 68, 70, 92, 44, 56.$   
 $Y : 51, 37, 48, 62, 93, 73, 56, 72, 70, 92.$

[Ans. :  $R = 0.59$ ]

5. Calculate Spearman's coefficient of rank correlation for the following data of scores in psychological tests ( $X$ ) and arithmetical ability ( $Y$ ) of 10 children.

Child : A, B, C, D, E, F, G, H, I, J.  
 $X : 105, 104, 102, 101, 100, 99, 98, 96, 93, 92.$   
 $Y : 101, 103, 100, 98, 95, 96, 104, 92, 97, 94.$

[Ans. :  $R = 0.782$ ]

6. Find the rank correlation coefficient between poverty and over crowding of cities from the following data.

Town : A, B, C, D, E, F, G, H, I, J.  
No. of poor families : 17, 13, 15, 16, 8, 11, 14, 9, 7, 12.  
Population (over crowding) : 30, 46, 35, 24, 12, 18, 27, 22, 46, 8.

[Ans. :  $R = 0.73$ ]

7. Calculate the rank coefficient of correlation from the following data.

$X : 105, 110, 112, 108, 111, 118, 120, 104, 115, 125.$   
 $Y : 39, 41, 45, 38, 48, 58, 60, 35, 54, 69.$

[Ans. :  $R = 0.9636$ ]

8. Two judges X, Y ranked 8 candidates as follows. Find the correlation coefficient.

Candidates : A, B, C, D, E, F, G, H.  
First judge X : 5, 2, 8, 1, 4, 6, 3, 7.  
Second judge Y : 4, 5, 7, 3, 2, 8, 1, 6.

[Ans. :  $R = 0.67$ ]

9. Calculate the rank correlation coefficient from the following data.

Marks in Paper I : 52, 63, 45, 36, 72, 65, 45, 25.  
Marks in Paper II : 62, 53, 51, 25, 79, 43, 60, 33.

[Ans. :  $R = 0.648$ ]**Miscellaneous Examples**

- Example 1 :** State true or false with proper justification.

If coefficient of correlation between  $x$  and  $y$  is negative then the coefficient of correlation between  $-x$  and  $-y$  is positive.

(M.U. 1998)

- Sol. : Coefficient of correlation between  $x$  and  $y$  is given by

$$r = \frac{\sum xy - \sum x \cdot \sum y / N}{\sqrt{\sum x^2 - (\sum x)^2 / N} \sqrt{\sum y^2 - (\sum y)^2 / N}}$$

If we change the signs of  $x$  and  $y$  both, since the product and square terms occur, the sign of  $r$  will remain the same.

∴ The statement is false.

**Example 2:** The coefficient of rank correlation of the marks obtained by 10 students in Physics and Chemistry was found to be 0.5. It was later discovered that the difference in ranks in the two subjects obtained by one of the students was wrongly taken as 3 instead of 7. Find the correct coefficient of rank correlation.

Sol.: Since  $R = 1 - \frac{6 \sum d_i^2}{N(N-1)}$  and  $R = 0.5$ ,  $n = 10$ .

$$0.5 = 1 - \frac{6 \sum d_i^2}{1000 - 10} \quad \therefore \sum d_i^2 = \frac{495}{6}$$

$$\begin{aligned} \therefore \text{Correct } \sum d_i^2 &= \text{Incorrect } \sum d_i^2 - (\text{incorrect rank diff.})^2 + (\text{Correct rank diff.})^2 \\ &= \frac{495}{6} - 3^2 + 7^2 = \frac{735}{6} \\ \therefore \text{Correct } R &= 1 - \frac{6 \times [735/6]}{990} = 1 - \frac{735}{990} = 0.26. \end{aligned}$$

**Example 3 :** (a) Let  $r_{xy} = 0.4$ , Cov.  $(x, y) = 1.6$ ,  $\sigma_y^2 = 25$ . Find  $\sigma_x$ .

(b) If  $R_{xy} = 0.143$  and the sum of the squares of the differences between the ranks is 48, find  $N$ .

Sol.: (a) We have  $r = \frac{\text{cov}(x, y)}{\sigma_x \cdot \sigma_y}$ . But  $r = 0.4$ , cov.  $(x, y) = 1.6$ ,  $\sigma_y = 5$ .

$$\therefore 0.4 = \frac{1.6}{5 \sigma_x} \quad \therefore \sigma_x = \frac{1.6}{5 \times 0.4} = 0.8$$

(b) We have,  $R = 1 - \frac{6 \sum D^2}{N(N-1)}$ . By data,  $R = 0.143$ ,  $\sum D^2 = 48$ .

$$\therefore 0.143 = 1 - \frac{6 \times 48}{N(N-1)} = 1 - \frac{288}{N(N-1)} \quad \therefore \frac{288}{N(N-1)} = 1 - 0.143 = 0.857$$

$$\therefore N(N-1) = \frac{288}{0.857} = 336 \quad \therefore N(N-1) = 336 = 0$$

$$\therefore N^2 - 7N^2 + 7N^2 - 48N + 48N - 336 = 0$$

$$\therefore (N-7)(N^2 + 7N + 48) = 0 \quad \therefore N = 7, \text{ other roots of } N \text{ are imaginary.}$$

**Example 4 :** Calculate the correlation coefficient between  $x$  and  $y$  from the following data.

$$N = 10, \sum x = 140, \sum y = 150, \sum (x-10)^2 = 180,$$

$$\sum (y-15)^2 = 215, \sum (x-10)(y-15) = 60.$$

Sol.: With usual notation  $\sum d_x^2 = 180$ ,  $\sum d_y^2 = 215$ ,  $\sum d_x d_y = 60$ .

$$\text{Now, } \bar{x} = A + \frac{\sum dx}{N} \quad \therefore 14 = 10 + \frac{\sum d_x}{10} \quad \therefore \sum d_x = 40$$

$$\text{Similarly, } \bar{y} = B + \frac{\sum dy}{N} \quad \therefore 15 = 15 + \frac{\sum d_y}{10} \quad \therefore \sum d_y = 10$$

$$\text{Now, } r = \frac{\sum d_x d_y - \frac{\sum d_x \cdot \sum d_y}{N}}{\sqrt{\sum d_x^2 - \frac{(\sum d_x)^2}{N}} \sqrt{\sum d_y^2 - \frac{(\sum d_y)^2}{N}}}$$

$$\therefore r = \frac{60 - \frac{40 \times 0}{10}}{\sqrt{180 - \frac{(40)^2}{10}} \sqrt{215 - \frac{(0)^2}{10}}} = \frac{60}{\sqrt{20} \sqrt{215}} = 0.915.$$

**EXERCISE - III****Type I**

1. Compute Spearman's rank correlation coefficient from the following data.

X : 85, 74, 86, 50, 65, 78, 74, 60, 74, 90  
Y : 78, 91, 78, 58, 60, 72, 80, 55, 68, 70. (M.U. 2007) [Ans. : R = 0.45]

2. Compute Spearman's rank correlation coefficient from the following data.

X : 18, 20, 34, 52, 12.  
Y : 39, 23, 35, 18, 46. (M.U. 2004) [Ans. : -0.824]

3. From the following data calculate Spearman's rank correlation between x and y.

x : 36, 56, 20, 42, 33, 44, 50, 15, 60.  
y : 50, 35, 70, 58, 75, 60, 45, 80, 38. (M.U. 2010) [Ans. : R = 0.92]

4. Find the coefficient of correlation ( $r$ ) between  $x$  and  $y$  for the following data.

x : 62 64 66 69 70 71 72 74  
y : 126 125 139 145 165 152 180 208 (M.U. 2003, 04) [Ans. : 0.9032]

5. Find Karl Pearson's coefficient of correlation and also, the Spearman's rank coefficient of correlation for the following data.

x : 12 17 22 27 32  
y : 113 119 117 115 121

Also interpret your result. [Ans. :  $r = R = 0.6$ ]

6. The following data give the growth of employment in lakhs in organised sector in India between 1988 and 1995.

Year : 1988, 89, 90, 91, 92, 93, 94, 95.  
Public Sector : 98, 101, 104, 107, 113, 120, 125, 128.  
Private Sector : 65, 65, 67, 68, 68, 69, 68, 68.

Find the correlation coefficient ( $r$ ) between the employment in public and private sectors and give your comments. (M.U. 1998) [Ans. :  $r = 0.98$ ]

7. Calculate the coefficient of correlation from the following figures. Is there any marked correlation between the production and price of tea?

Production in crores of lbs. : 44, 37, 31, 38, 36, 35, 40.

Price in Rs. per lbs. : 2.75, 3.62, 4.25, 4.12, 4.26, 4.32, 4.05.

8. Draw a scatter diagram to represent the following data.

X : 2, 4, 5, 6, 8, 11.  
Y : 18, 12, 10, 8, 7, 5.

Calculate the coefficient of correlation between X and Y for the above data.

(M.U. 1998) [Ans. :  $r = -0.92$ ]

9. Find the coefficient of correlation between height of father and height of son from the following data.
- Height of father : 65, 66, 67, 67, 68, 69, 71, 73.  
 Height of son : 67, 68, 64, 68, 72, 70, 69, 70. [Ans. :  $r = +0.95$ ]
10. Calculate Spearman's coefficient of rank correlation and Pearson's coefficient of correlation from the data on height and weight of eight students. Why the two values are same?
- Height (in inches) : 60, 62, 64, 68, 70, 72, 74.  
 Weight (in lbs.) : 92, 83, 101, 110, 128, 119, 137, 146.  
 [Ans. :  $r = R = 0.93$ ; For both the series, the difference between consecutive terms remains constant if arranged in order.]
11. The following table shows the marks obtained by 10 students in Accountancy and Statistics. Find the Spearman's coefficient of rank correlation.
- |             |   |
|-------------|---|
| Student No. | : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.          |
| Accountancy | : 45, 70, 65, 30, 90, 40, 50, 57, 85, 60. |
| Statistics  | : 35, 90, 70, 40, 95, 40, 60, 80, 80, 50. |

Will the result change if the marks in the two subjects of all the students are increased by 5 and 10 respectively? Will the result change if marks in the two subjects of all the students are halved?

[Ans. :  $r = 0.8608$ ; No. : No.]

#### Type II

1. The coefficient of rank correlation between marks in Physics and Chemistry obtained by a group of students is 0.8. If the sum of the squares of differences in ranks is 33, find the number of pairs. [Ans. :  $N = 10$ ]

2. Find the number of pairs of observations from the following data.

$$r = 0.4, \Sigma xy = 108, \sigma_y = 3, \Sigma x^2 = 900.$$

where  $x, y$  are the deviations of  $x, y$  from their respective means. [Ans. :  $N = 10$ ]

3. Coefficient of correlation between two variables is 0.4. Their covariance is 12. The variance of  $x$  is 25. Find the standard deviation of  $y$ . [Ans. :  $\sigma_y = 6$ ]

4. A computer while calculating the correlation coefficient between two variables  $x$  and  $y$ , from 25 observations obtained the following results.

$$N = 25, \Sigma x = 125, \Sigma y = 100, \Sigma x^2 = 850, \Sigma y^2 = 960, \Sigma xy = 508$$

where  $x, y$  denote the actual values of the variables. Find the value of  $r$ . [Ans. :  $r = 0.067$ ]

5. A sample of 25 pairs of values of  $x$  and  $y$  lead to the following results.

$$\Sigma x = 127, \Sigma y = 100, \Sigma x^2 = 760, \Sigma y^2 = 449, \Sigma xy = 500.$$

Later on it was found that two pairs of values were taken as (8, 14) and (8, 6) instead of correct values (8, 12) and (6, 8).

Find corrected correlation coefficient between  $x$  and  $y$ . (M.U. 2004) [Ans. :  $r = -0.31$ ]

6. Given : Number of pairs of observations = 10

$X$  series standard deviation = 22.70,  $Y$  series standard deviation = 9.592

Summation of the products of corresponding deviations of  $X$  and  $Y$  from their respective actual means = -1439. Find  $r$ .

[Ans. :  $r = -0.66$ ]

#### EXERCISE - IV

- Theory**
- What is meant by correlation? Describe scatter diagram and interpret.
  - Define - (i) Karl Pearson's coefficient of correlation, (ii) Spearman's rank correlation coefficient. (M.U. 2005)
  - Two variables  $x$  and  $y$  are connected by the relation  $ax + by + c = 0$ . Show that the coefficient of correlation is either +1 or -1.
  - Define product moment correlation coefficient and show that it is always numerically less than or equal to unity.
  - Define - (i) Covariance between two variables  $x$  and  $y$ , (ii) Karl Pearson's Product moment correlation coefficient.
  - Prove that Spearman's rank correlation coefficient  $R$  is given by

$$R = 1 - \frac{6 \sum D^2}{N^2 - N}$$

(M.U. 1996, 99, 2002, 03, 04, 05, 06, 08)

7. What is scatter diagram? How does it help in studying the correlation between two variables. Draw scatter diagrams for  $r = +1, r = -1$  and  $r = 0$ .

8. Define the Karl Pearson's coefficient of correlation  $r$  between two variables  $x$  and  $y$ . What is "Spurious Correlation"? Interpret the cases  $r = +1, r = -1, r = 0$ . Also draw the scatter diagrams corresponding to these cases.



# Regression

## 1. Introduction

We have seen in the previous chapter how to examine and measure in magnitude and direction correlation between two variables. After establishing correlation, it is natural to search for a method which will help us to estimate the value of one variable when that of the other is known. This is achieved by the analysis of regression. Regression can be defined as 'a method of estimating the value of one variable when that of the other is known and when the variables are correlated'.

The term, regression was first used by Galton. He found that although tall fathers have tall sons, and short fathers have short sons, the average height of sons of tall fathers is less than the average height of their fathers and the average height of sons of short fathers is more than the average height of their fathers. In other words the average height of sons of tall fathers or short fathers will regress or go back to the general average height. This phenomenon was described by him as 'regression.'

## 2. Lines of Regression

We have seen in the previous chapter that if the variables which are highly correlated are plotted on a graph then the points lie in a narrow strip. If the strip is nearly straight, we may draw a line such that all the points are close to it from both the sides. Such a line can be taken as the representative of the ideal variation. It is called the line of best fit. It is a line such that the sum of the distances of the points from the line is minimum. It is also called 'the line of regression'. But we do not measure the distance by dropping a perpendicular from a point to the line. We measure, the deviations (i) vertically and (ii) horizontally, and get one line when distances are minimised vertically and second line when distances are minimised horizontally. Thus, we get two lines of regression.

### (i) Line of regression of $Y$ on $X$

If we minimise the deviations of the points from the line measured along  $y$ -axis we get a line which is called the line of regression of  $Y$  on  $X$ . Its equation is written in the form  $Y = a + bX$ . This line is used for estimating the value of  $Y$  for a given value of  $X$ . [ See Fig. 11.1 ]

The equation of the line of regression of  $Y$  on  $X$  must be written with  $Y$  on the left hand side and  $X$  and the constant term on the right hand side.

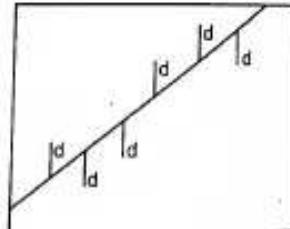


Fig. 11.1  
For the Line of Regression of  $Y$  on  $X$   
the distances  $d$  are minimised.

### (ii) Line of regression of $X$ on $Y$

If we minimise the deviations of the points from the line measured along  $x$ -axis we get a line which is called the line of regression of  $X$  on  $Y$ . Its equation is written in the form  $X = a + bY$ . This line is used for estimating the value of  $X$  for a given value of  $Y$ . [ See Fig. 11.2 ]

The equation of the line of regression of  $x$  on  $y$  must be written with  $x$  on the left hand side and  $y$  and constant term on the right hand side.

There are two methods of obtaining the lines of regression. The first is graphical, the other is mathematical. They are :

1. The method of Scatter Diagram,
2. The Method of Least Squares.

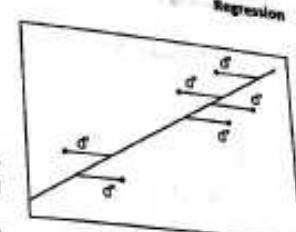


Fig. 11.2  
For the line of regression of  $X$  on  $Y$   
the distances  $d$  are minimised.

## 3. The Method of Scatter Diagram

It is the simplest method of obtaining the lines of regression. The data are plotted on a graph paper by taking the independent variable on  $x$ -axis and the dependent variable on  $y$ -axis. We thus get points which are generally scattered. If the correlation is perfect i.e. if  $r$  is equal to one, positive or negative, the points will lie on a line, which is the line of regression. And there is only one line of regression and not two in such cases. However, in practice we rarely come across problems wherein we have perfect correlation. Usually, the points are scattered in a narrow straight strip and we have to find a line which will best represent all the points of the scatter diagram. We draw a line which will be close to all the points as far as possible.

Example : Given the following pairs of values of  $X$  and  $Y$ .

$$\begin{aligned} X &: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 \\ Y &: 5, 6, 5, 6, 6, 8, 7, 9, 8, 9, 10, 11 \end{aligned}$$

Plot the points on a graph and draw a line of regression.

Sol. :

### Scatter Diagram and Line of Regression

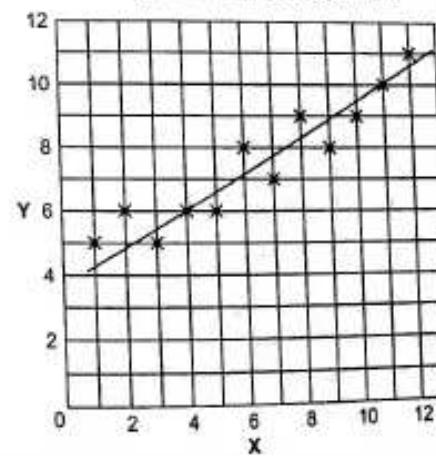


Fig. 11.3

#### 4. The Method of Least Square

This is a mathematical method which gives an objective treatment to find a line of regression.

Let  $y = a + bx$  be the equation of the line required. To find the line of regression of  $y$  on  $x$  we minimise the sum of the absolute distances of the points like  $P(x_i, y_i)$  from the line measured along the  $y$ -axis. If  $Q$  is the point on the line corresponding to  $P(x_i, y_i)$  we have to minimise the absolute distance  $PQ$ . Since  $Q$  lies on  $y = a + bx$  its  $y$ -coordinate is  $a + bx_i$ .

$\therefore |PQ| = |y_i - a - bx_i|$

For minimising  $|PQ|$  we minimise its squares. Hence, if  $S$  denotes the sum of the squares of these distances,

$$S = \sum f_i (y_i - a - bx_i)^2 \quad \text{where } f_i \text{ is the frequency of } (x_i, y_i).$$

We have to find  $a$  and  $b$  such that  $S$  is minimum, the conditions for which are

$$\frac{\partial S}{\partial a} = 2 \sum f_i (y_i - a - bx_i) = 0 \quad \text{and} \quad \frac{\partial S}{\partial b} = 2 \sum f_i (y_i - a - bx_i) x_i = 0$$

$$\sum f_i (y_i - a - bx_i) = 0$$

$$\sum x_i f_i (y_i - a - bx_i) = 0$$

From (A) we get,  $\sum f_i y_i - a \sum f_i - b \sum f_i x_i = 0$

$$\therefore N\bar{y} - aN - bN\bar{x} = 0 \quad \therefore \bar{y} = a + b\bar{x}$$

which shows that the line of regression passes through  $(\bar{x}, \bar{y})$ .

From (B) we get,  $\sum f_i x_i y_i - a \sum f_i x_i - b \sum f_i x_i^2 = 0$

We now find the values of these expressions in terms of  $r$ ,  $\sigma_x$ ,  $\sigma_y$ .

$$\text{But since, } r = \frac{1}{N} \frac{\sum f_i (x_i - \bar{x})(y_i - \bar{y})}{\sigma_x \sigma_y}$$

$$r = \frac{\sum f_i x_i y_i - N\bar{x}\bar{y}}{N\sigma_x \sigma_y} \quad \therefore \sum f_i x_i y_i = Nr\sigma_x \sigma_y + N\bar{x}\bar{y}$$

$$\text{and } \sigma_x^2 = \frac{1}{N} \sum f_i (x_i - \bar{x})^2 = \frac{1}{N} \sum f_i x_i^2 - \bar{x}^2 \quad \therefore \sum f_i x_i^2 = N\sigma_x^2 + N\bar{x}^2$$

Putting the values of  $\sum f_i x_i y_i$  and  $\sum f_i x_i^2$  in D, we get

$$Nr\sigma_x \sigma_y + N\bar{x}\bar{y} = aN\bar{x} + bN\sigma_x^2 + bN\bar{x}^2$$

$$\text{i.e. } r\sigma_x \sigma_y + \bar{x}\bar{y} = a\bar{x} + b\sigma_x^2 + b\bar{x}^2$$

Multiply (C) by  $\bar{x}$  and subtract it from (E)

$$r\sigma_x \sigma_y = b\sigma_x^2 \quad \therefore b = r \frac{\sigma_y}{\sigma_x}$$

Since, the line passes through  $(\bar{x}, \bar{y})$  and its slope  $b = r \frac{\sigma_y}{\sigma_x}$  its equation is

$$y - \bar{y} = r \frac{\sigma_y}{\sigma_x} (x - \bar{x})$$

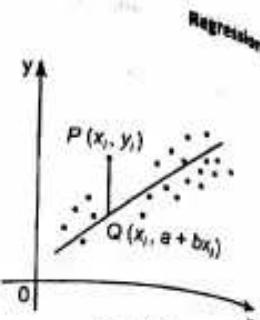


Fig. 11.4

Similarly, the equation of the line of regression of  $x$  on  $y$  can be shown to be

$$x - \bar{x} = r \frac{\sigma_x}{\sigma_y} (y - \bar{y}) \quad (G)$$

**Alternative Method:** Instead of calculating  $\bar{x}$ ,  $\bar{y}$ ,  $\sigma_x$ ,  $\sigma_y$  and  $r$  we may use the following method.

(i) The line of regression of  $y$  on  $x$   
Let the equation of the line of regression of  $y$  on  $x$  be  $y = a + bx$ . Then as before we have to minimise

$S = \sum f_i (y_i - a - bx_i)^2$  the conditions of which are

$$\frac{\partial S}{\partial a} = -2 \sum f_i (y_i - a - bx_i) = 0 \quad \text{and} \quad \frac{\partial S}{\partial b} = -2 \sum f_i (y_i - a - bx_i) x_i = 0$$

$$\text{i.e. } \sum f_i (y_i - a - bx_i) = 0 \quad \text{and} \quad \sum f_i x_i (y_i - a - bx_i) = 0$$

$$\text{i.e. } \sum f_i y_i - a \sum f_i - b \sum f_i x_i = 0 \quad \text{and} \quad \sum f_i x_i y_i - a \sum f_i x_i - b \sum f_i x_i^2 = 0.$$

If the required sums are known, by solving the above two equations simultaneously for  $a$  and  $b$  we get the required equation.

In particular if all values occur only once i.e. if  $f_i = 1$  for all  $i$  then the above equations take the form

$$\sum y = aN + b \sum x \quad \text{and} \quad \sum xy = a \sum x + b \sum x^2$$

from which  $a$  and  $b$  can be calculated.

The above equations are called normal equations.

(ii) The line of regression of  $x$  on  $y$

Let the equation of the line be  $x = a + by$ .

Proceeding as above we get the normal equations as

$$\sum x = aN + b \sum y \quad \text{and} \quad \sum xy = a \sum y + b \sum y^2$$

from which we can find the values of  $a$  and  $b$ .

**Example:** Find the equations of the lines of regression from the following data.

$$x: 5 \ 6 \ 7 \ 8 \ 9$$

$$y: 2 \ 4 \ 5 \ 6 \ 8 \quad \text{Also find } r.$$

Sol. :

Calculations of regression

Sr. No.	$x$	$x^2$	$y$	$y^2$	$xy$
1	5	25	2	4	10
2	6	36	4	16	24
3	7	49	5	25	35
4	8	64	6	36	48
5	9	81	8	64	72
$N = 5$	35	255	25	145	189

The equation of the line of regression of  $y$  on  $x$  is  $y = a + bx$  where  $a, b$  are given by

$$\Sigma y = aN + b \sum x \quad \text{and} \quad \Sigma xy = a \sum x + b \sum x^2$$

Putting the values of  $\sum x, \sum x^2, \sum xy$ , we get

$$25 = 5a + 35b \quad \dots \dots \dots (i) \quad \text{and} \quad 189 = 35a + 255b \quad \dots \dots \dots (ii)$$

Multiply the first by 7 and subtract it from the second.

$$189 = 35a + 255b$$

$$175 = 35a + 245b$$

$$14 = 10b \quad \therefore b = 1.4$$

Putting this value of  $b$  in (i), we get

$$25 = 5a + 35(1.4) \quad \therefore 5a = 25 - 49 = -24 \quad \therefore a = -4.8$$

∴ The equation of the line of regression of  $y$  on  $x$  is

$$y = -4.8 + 1.4x$$

The equation of the line of regression of  $x$  on  $y$  is  $x = a + by$  where  $a, b$  are given by

$$\Sigma x = aN + b \sum y \quad \text{and} \quad \Sigma xy = a \sum y + b \sum y^2$$

Putting the values of  $\sum x, \sum y, \sum xy, \sum y^2$ , we get

$$35 = 5a + 25b \quad \dots \dots \dots (iii) \quad \text{and} \quad 189 = 25a + 145b \quad \dots \dots \dots (iv)$$

Multiply (iii) by 5 and subtract it from (iv).

$$189 = 25a + 145b$$

$$175 = 25a + 120b$$

$$14 = 25b \quad \therefore b = 0.56$$

Putting this value of  $b$  in (iii), we get

$$35 = 5a + 25(0.56) \quad \therefore 5a = 35 - 14 = 11 \quad \therefore a = 2.2$$

∴ The equation of the line of regression of  $x$  on  $y$  is

$$x = 2.2 + 0.56y$$

Now,  $r = \sqrt{b_1 \times b_2} = \sqrt{1.4 \times 0.56} = 0.88$ .

## 5. Calculations of the Equations of the Lines of Regression

There are various methods of calculating the equations of the lines of regression. The choice is yours. We state them below.

- (a) By calculating the coefficient of correlation  $r$  and standard deviation  $\sigma_x$  and  $\sigma_y$

The equation of the line of regression of  $Y$  on  $X$ .

The equation of the line of regression of  $Y$  on  $X$  is given by,

$$Y - \bar{Y} = b_{yx}(X - \bar{X})$$

where,  $\bar{X}$  = the mean of  $X$ ,  $\bar{Y}$  = the mean of  $Y$  and  $b_{yx} = r \frac{\sigma_y}{\sigma_x}$ .

[See § 6]

The equation, therefore can be written as

$$Y - \bar{Y} = r \frac{\sigma_y}{\sigma_x} (X - \bar{X}) \quad \dots \dots \dots (1)$$

This equation is to be used for calculating the most probable value of  $Y$  for a given value of  $X$ .

The equation of the line of regression of  $X$  on  $Y$ .

The equation of the line of regression of  $X$  on  $Y$  is given by,

$$X - \bar{X} = b_{xy}(Y - \bar{Y})$$

where,  $\bar{X}$  = the mean of  $X$ ,  $\bar{Y}$  = the mean of  $Y$  and  $b_{xy} = r \frac{\sigma_x}{\sigma_y}$ .

The equation, therefore can be written as

$$X - \bar{X} = r \frac{\sigma_x}{\sigma_y} (Y - \bar{Y}) \quad \dots \dots \dots (2)$$

This equation is to be used for calculating the most probable value of  $X$  for a given value of  $Y$ . When the values of  $X$  and  $Y$  are known, we can as usual calculate  $r, \sigma_x$  and  $\sigma_y$  and then obtain equations of the lines of regression of  $X$  and  $Y$ .

- (b) By calculating  $a$  and  $b$  directly

Instead of calculating  $\bar{X}, \bar{Y}, \sigma_x, \sigma_y$  and  $r$  we may calculate  $a$  and  $b$  directly as explained below.

The line of regression of  $Y$  on  $X$  : The constants  $a$  and  $b$  of the equation of the line of regression of  $Y$  on  $X$  i.e. of,

$$Y = a + bX$$

can be obtained by solving the following simultaneous equations.

$$\Sigma Y = aN + b \sum X \quad \text{and} \quad \Sigma XY = a \sum X + b \sum X^2 \quad \dots \dots \dots (3)$$

The line of regression of  $X$  on  $Y$  : The constants  $a$  and  $b$  of the equation of the line of regression of  $X$  on  $Y$  i.e. of,

$$X = a + bY$$

can be obtained by solving the following simultaneous equations,

$$\Sigma X = aN + b \sum Y \quad \text{and} \quad \Sigma XY = a \sum Y + b \sum Y^2 \quad \dots \dots \dots (4)$$

The equations, are called 'Normal equations'.

The formulae (3) and (4) are convenient when  $\Sigma X, \Sigma Y, \Sigma XY, \Sigma X^2, \Sigma Y^2$  are known.

- (c) By taking deviations from the means  $X$  and  $Y$

If  $x$  and  $y$  denote the deviations of  $X$  and  $Y$  from their means, we know that,

$$b_{yx} = r \frac{\sigma_y}{\sigma_x} = \frac{\sum xy}{N \sigma_x \sigma_y}, \quad \frac{\sigma_y}{\sigma_x} = \frac{\sum xy}{N \sigma_x^2} = \frac{\sum xy}{N \cdot \sum x^2 / N} = \frac{\sum xy}{\sum x^2}$$

$$\therefore b_{yx} = \frac{\sum xy}{\sum x^2} \quad \dots \dots \dots (5)$$

(11-7)

Similarly, we can show that,

$$b_{xy} = r \frac{\sigma_x}{\sigma_y} = \frac{\sum xy}{\sum y^2}$$

where,  $x = X - \bar{X}$ ,  $y = Y - \bar{Y}$ .

Hence, the equations of the lines of regression become,

$$Y - \bar{Y} = \frac{\sum xy}{\sum x^2} (X - \bar{X})$$

$$X - \bar{X} = \frac{\sum xy}{\sum y^2} (Y - \bar{Y})$$

and

(d) By taking deviations from assumed means

If the deviations of  $X$  and  $Y$  are taken from assumed means i.e. if  $d_x = X - A$  and  $d_y = Y - B$  then the coefficients  $b_{yx}$  and  $b_{xy}$  are given by,

$$b_{yx} = \frac{\sum d_x d_y - \frac{\sum d_x \sum d_y}{N}}{\sum d_x^2 - \frac{(\sum d_x)^2}{N}}$$

$$b_{xy} = \frac{\sum d_x d_y - \frac{\sum d_x \sum d_y}{N}}{\sum d_y^2 - \frac{(\sum d_y)^2}{N}}$$

(e) By using actual values directly

If  $X$ ,  $Y$  are actual values of the two variates then it can be shown that

$$b_{yx} = \frac{\sum XY - \frac{\sum X \cdot \sum Y}{N}}{\sum X^2 - \frac{(\sum X)^2}{N}}$$

$$b_{xy} = \frac{\sum XY - \frac{\sum X \cdot \sum Y}{N}}{\sum Y^2 - \frac{(\sum Y)^2}{N}}$$

## 6. Regression Coefficients

The slope  $b$  of the line of regression of  $y$  on  $x$  i.e.  $b$  of the equation  $y = a + bx$  is called the coefficient of regression of  $y$  on  $x$ . It represents the increment in  $y$  for unit change in the value of  $x$ . It is denoted by  $b_{yx}$ .

$\therefore b_{yx}$  = Coefficient of Regression of  $y$  on  $x$ .

$$b_{yx} = r \frac{\sigma_y}{\sigma_x}$$

(11-8)

Similarly, the slope  $b$  of the line of regression  $x$  on  $y$  i.e.  $b$  of the equation  $x = a + by$  is called the coefficient of regression of  $x$  on  $y$ . It represents the increment in  $x$  for unit change in  $y$ . It is denoted by  $b_{xy}$ .

$\therefore b_{xy}$  = Coefficient of Regression of  $x$  on  $y$ .

$$b_{xy} = r \frac{\sigma_x}{\sigma_y}$$

Putting  $b_{yx}$  and  $b_{xy}$  which are the slopes of the lines of regression in (F) and (G), we can write the equations of lines of regression as

$$y - \bar{Y} = b_{yx}(x - \bar{X})$$

$$x - \bar{X} = b_{xy}(y - \bar{Y})$$

By putting the values of  $r$  and  $\sigma_y$ ,  $\sigma_x$  in terms of actual values of  $x$  and  $y$  or by taking deviations from actual means or assumed means, we get the following formulae for  $b_{yx}$  and  $b_{xy}$  (We repeat the first two.)

$$b_{yx} = r \frac{\sigma_y}{\sigma_x}$$

$$b_{yx} = \frac{\sum xy}{\sum x^2}$$

where  $x = X - \bar{X}$ ,  $y = Y - \bar{Y}$  i.e.  $x$ ,  $y$  are deviations of  $X$ ,  $Y$  from actual means.

$$b_{yx} = \frac{\sum d_x d_y - \frac{\sum d_x \cdot \sum d_y}{N}}{\sum d_x^2 - \frac{(\sum d_x)^2}{N}}$$

where  $d_x = X - A$ ,  $d_y = Y - B$  i.e.  $d_x$ ,  $d_y$  are deviations of  $X$ ,  $Y$  from assumed means  $A$  and  $B$ .

$$b_{yx} = \frac{\sum XY - \frac{\sum X \cdot \sum Y}{N}}{\sum X^2 - \frac{(\sum X)^2}{N}}$$

where  $X$ ,  $Y$  are the actual values of the variables.

$$b_{xy} = r \frac{\sigma_x}{\sigma_y}$$

$$b_{xy} = \frac{\sum xy}{\sum y^2}$$

where  $x = X - \bar{X}$ ,  $y = Y - \bar{Y}$  i.e.  $x$ ,  $y$  are the deviations of  $X$ ,  $Y$  from actual means

$$b_{xy} = \frac{\sum d_x d_y - \frac{\sum d_x \cdot \sum d_y}{N}}{\sum d_y^2 - \frac{(\sum d_y)^2}{N}}$$

where  $d_x = X - A$ ,  $d_y = Y - B$  i.e.  $d_x$ ,  $d_y$  are the deviations of  $X$ ,  $Y$  from assumed means  $A$  and  $B$ .

$$b_{xy} = \frac{\sum XY - \frac{\sum X \cdot \sum Y}{N}}{\sum Y^2 - \frac{(\sum Y)^2}{N}}$$

where  $X$ ,  $Y$  are the actual values of the variables.

### 7. Properties of Coefficients of Regression

1. Coefficient of correlation is the geometric mean between the coefficients of regression.

Proof : From the above results we have

$$b_{yx} \cdot b_{xy} = r \frac{\sigma_y}{\sigma_x} \cdot r \frac{\sigma_x}{\sigma_y}$$

$$\therefore b_{yx} \cdot b_{xy} = r^2$$

Hence, the result.

Remark ...

Since the product of  $b_{yx}$  and  $b_{xy}$  is positive, if one of them is negative, the other also must be negative. In other words both the coefficients of regression are positive or both the coefficients of regression are negative together.

2. If one coefficient of regression is greater than one, the other must be less than one.

Proof : Since  $-1 \leq r \leq 1$ ,  $r^2 \leq 1$ .

Hence, from the above result,

$$b_{yx} \cdot b_{xy} \leq 1 \quad \therefore b_{yx} \leq \frac{1}{b_{xy}} \quad \therefore \text{If } b_{yx} < 1, \text{ then } b_{xy} > 1.$$

[ See the values of  $b_{yx}$  and  $b_{xy}$  in Ex. 4, page 11-16. See that  $b_{yx}$  is less than one and  $b_{xy}$  is greater than one. ]

3. Arithmetic mean of the coefficients of regression is greater than or equal to the coefficient of correlation.

Proof : We have to show that  $\frac{b_{yx} + b_{xy}}{2} \geq r$

$$\text{i.e. } \frac{1}{2} \left( r \frac{\sigma_y}{\sigma_x} + r \frac{\sigma_x}{\sigma_y} \right) \geq r \quad \text{i.e. } \frac{\sigma_y}{\sigma_x} + \frac{\sigma_x}{\sigma_y} \geq 2$$

$$\text{i.e. } \sigma_x^2 + \sigma_y^2 \geq 2\sigma_x\sigma_y \quad \text{i.e. } \sigma_x^2 - 2\sigma_x\sigma_y + \sigma_y^2 \geq 0$$

$$\text{i.e. } (\sigma_x - \sigma_y)^2 \geq 0 \text{ which is obviously true.}$$

Remark ...

In other words this means the sum of the two coefficients of regression is greater than or equal to  $2r$ . We shall verify this in Ex. 2, page 11-19 and Ex. 7, page 11-22 below. We further note that equality will hold when  $\sigma_x = \sigma_y$ .

4. Coefficients of regression are independent of change of origin but not of change of scale.

If  $u = ax + h$  and  $v = by + k$ , then

$$b_{uv} = \frac{a}{b} \cdot b_{xy} = \frac{\text{Coefficient of } x}{\text{Coefficient of } y} \cdot b_{xy}$$

We accept this result without proof.

5. If the correlation is perfect then the two coefficients of regression are reciprocals of each other.

Proof : We have  $r = \pm 1$  and  $r = \sqrt{b_{yx} \cdot b_{xy}} \quad \therefore \pm 1 = \sqrt{b_{yx} \cdot b_{xy}}$ .

$$\text{Squaring } 1 = b_{yx} \cdot b_{xy} \quad \therefore b_{yx} = \frac{1}{b_{xy}}$$

e.g., if one coefficient of regression is 0.5 and if the correlation is perfect, then the other coefficient of regression is 2.

Example 1 : State whether the following statement is true or false with reasoning : "The regression coefficients between  $2x$  and  $2y$  are the same as those between  $x$  and  $y$ ". (M.U. 1997)

Sol. : As seen above if  $u = ax + h$  and  $v = by + k$ ,  $b_{uv} = \frac{a}{b} \cdot b_{xy}$ .

$$\text{But by data } u = 2x \text{ i.e. } a = 2 \text{ and } v = 2y \text{ i.e. } b = 2.$$

$$\therefore b_{uv} = \frac{2}{2} \cdot b_{xy} = b_{xy}. \quad \text{Hence, the statement is true.}$$

Example 2 : State whether the following statement is true or false : "The lines of regression between  $x$  and  $y$  are parallel to the lines of regression between  $2x$  and  $2y$ ".

Sol. : True. Explanation is left to you.

Example 3 : State whether the following statement is true or false : "The coefficients of regression between  $x$  and  $y$  are the same as the coefficients of regression between  $2x + 5$  and  $2y - 7$ ".

Sol. : True. Explanation is left to you.

Example 4 : If the arithmetic mean of regression coefficients is  $p$  and their difference is  $2q$ , find the correlation coefficient. (M.U. 1998, 2017)

Sol. : Let the coefficients of regression be  $b_1$  and  $b_2$ . (See § 6, page 11-7)

$$\text{Now by data } \frac{b_1 + b_2}{2} = p \text{ and } b_1 - b_2 = 2q$$

$$\therefore b_1 + b_2 = 2p \text{ and } b_1 - b_2 = 2q$$

$$\therefore b_1 = p + q \text{ and } b_2 = p - q$$

$$\therefore \text{Coefficient of correlation} = r = \sqrt{b_1 b_2} = \sqrt{p^2 - q^2}$$

Example 5 : State true or false with reasoning : "2x + y = 3 and x = 2y + 3 cannot be the lines of regression." (M.U. 2004)

Sol. : If the first line is the line of regression of  $y$  on  $x$  it must be written as  $y = -2x + 3$  and if the second line is the line of regression of  $x$  on  $y$ , then it must be written as  $x = 2y + 3$ .

Hence, the coefficients of regression are  $b_{yx} = -2$  and  $b_{xy} = 2$  which is not possible as one of them is negative and the other is positive and both are greater than 1 numerically.

Now, we consider the lines in other way round. Let the first line be the line of regression of  $y$  on  $x$  and let the second line be the line of regression of  $x$  on  $y$ .

$$\therefore x = -\frac{1}{2}y + \frac{3}{2} \quad \text{and} \quad y = \frac{1}{2}x - \frac{3}{2}$$

Hence, the coefficients of regression are

$$b_{yx} = -\frac{1}{2} \quad \text{and} \quad b_{xy} = \frac{1}{2}$$

which is again not possible because one is positive and the other is negative.

Hence, the statement is true.

**Example 6 :** State true or false with justification. If two lines of regression are  $x + 3y - 5 = 0$  and  $4x + 3y - 8 = 0$  then the correlation coefficient is +0.5. (M.U. 2003, 14)

**Sol. :** Let the line  $x + 3y - 5 = 0$  be the line of regression of  $x$  on  $y$ . Writing it as  $x = -3y + 5$ , we get  $b_{yx} = -3$ .

Let the line  $4x + 3y - 8 = 0$  be the line of regression of  $y$  on  $x$ . Writing it as  $3y = -4x + 8$ , i.e., as  $y = -\frac{4}{3}x + 2$ , we get  $b_{xy} = -\frac{4}{3}$ .

$$\therefore r = \sqrt{b_{yx} \cdot b_{xy}} = \sqrt{(-3)(-4/3)} = \sqrt{4} = 2$$

But  $r$  cannot be greater than 1.

Hence, our suppositions are wrong.

Now, let the line  $x + 3y - 5 = 0$  be the line of regression of  $y$  on  $x$ . Writing it as

$$3y = -x + 5 \quad \text{i.e.,} \quad y = -\frac{1}{3}x + \frac{5}{3}, \text{ we get } b_{yx} = -\frac{1}{3}.$$

Let the line  $4x + 3y - 8 = 0$  be the line of regression of  $x$  on  $y$ . Writing it as

$$4x = -3y + 8 \quad \text{i.e.,} \quad x = -\frac{3}{4}y + 2, \text{ we get } b_{xy} = -\frac{3}{4}.$$

$$\text{Now, } r = \sqrt{b_{yx} \cdot b_{xy}} = \sqrt{\left(-\frac{1}{3}\right)\left(-\frac{3}{4}\right)} = \sqrt{\frac{1}{4}} = \frac{1}{2} = 0.5$$

Hence, the statement is true.

#### 6. Angle between the lines of regression

The equation of the lines of regression of  $y$  on  $x$  is

$$y - \bar{y} = r \frac{\sigma_y}{\sigma_x} (x - \bar{x}). \quad \text{Hence, its slope } m_1 = r \frac{\sigma_y}{\sigma_x}$$

The equation of the line of regression of  $x$  on  $y$  is

$$x - \bar{x} = r \frac{\sigma_x}{\sigma_y} (y - \bar{y})$$

$$\text{I.e., } y - \bar{y} = \frac{\sigma_y}{r \cdot \sigma_x} (x - \bar{x}) \quad \text{Hence, its slope } m_2 = \frac{\sigma_y}{r \cdot \sigma_x}$$

If  $\theta$  is the angle between the lines of regression

$$\begin{aligned} \tan \theta &= \frac{m_1 - m_2}{1 + m_1 m_2} = \frac{r \frac{\sigma_y}{\sigma_x} - r \frac{\sigma_x}{\sigma_y}}{1 + r \frac{\sigma_y}{\sigma_x} \cdot r \frac{\sigma_x}{\sigma_y}} = \frac{r \frac{\sigma_y}{\sigma_x} - r \frac{\sigma_x}{\sigma_y}}{\frac{\sigma_x^2 + \sigma_y^2}{\sigma_x^2}} \\ &= \frac{(r^2 - 1)}{r} \left( \frac{\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2} \right) = \frac{1 - r^2}{r} \left( \frac{\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2} \right) \end{aligned}$$

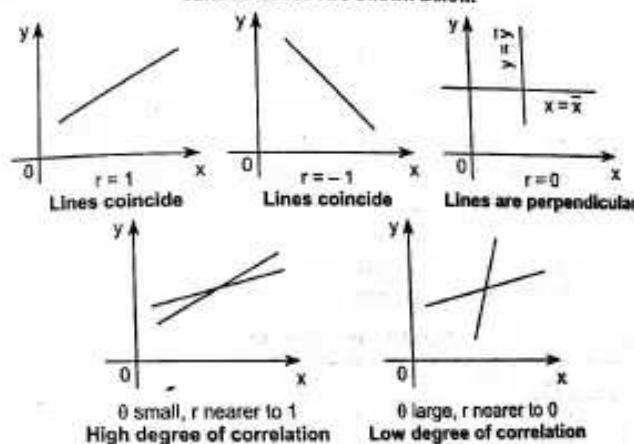
**Corollary 1 :** If  $r = 0$ ,  $\tan \theta = \infty \Rightarrow \theta = \pi/2$ .

The lines of regression are perpendicular to each other.

**Corollary 2 :** If  $r = \pm 1$ ,  $\tan \theta = 0 \Rightarrow \theta = 0$ .

The lines of regression are coincident.

#### Various Cases Are Shown Below.



#### Illustrative Examples

**Example 1 :** A panel of two judges A and B graded dramatic performances by independently awarding marks as follows :

Performance No. : 1, 2, 3, 4, 5, 6, 7.

Marks by A : 36, 32, 34, 31, 32, 32, 34.

Marks by B : 35, 33, 31, 30, 34, 32, 36.

The eighth performance, however, which judge B could not attend, got 38 marks by judge A. If judge B had also been present, how many marks would he be expected to have awarded to the eighth performance ?

Sr. No.	$X - \bar{X}$			$Y - \bar{Y}$			Product $xy$
	$X$	$x$	$x^2$	$Y$	$y$	$y^2$	
1	36	3	9	35	2	4	6
2	32	-1	1	33	0	0	0
3	34	1	1	31	-2	4	-2
4	31	-2	4	30	-3	9	6
5	32	-1	1	34	1	1	-1
6	32	-1	1	32	-1	1	1
7	35	1	1	36	3	9	3
$N = 7$	$\Sigma X = 231$	$\Sigma x^2 = 18$		$\Sigma Y = 231$	$\Sigma y^2 = 28$		$\Sigma xy = 13$

We have to find the marks that would have been awarded by the judge B. Therefore, the marks given by the judge B be denoted by  $Y$  and those given by A by  $X$ .

$$\therefore \bar{X} = \frac{\sum X}{N} = \frac{231}{7} = 33, \bar{Y} = \frac{\sum Y}{N} = \frac{231}{7} = 33$$

$$\therefore b_{yx} = \frac{\sum xy}{\sum x^2} = \frac{13}{18} = 0.72$$

The equation of the line of regression of  $Y$  on  $X$  is,

$$Y - \bar{Y} = b_{yx}(X - \bar{X}) \text{ i.e. } Y - 33 = 0.72(X - 33)$$

To find the value of  $Y$  when  $X = 38$ , put  $X = 38$  in the above equation.

$$\therefore Y - 33 = 0.72(38 - 33) = 0.72 \times 5 = 3.6$$

$$\therefore Y = 33 + 3.6 = 36.6 = 37 \text{ approximately.}$$

$\therefore$  The judge B would have given 37 marks to the eighth performance.

Alternatively:

#### Calculations of regression

Sr. No.	$x$	$x^2$	$y$	$xy$
1	36	1296	35	1260
2	32	1024	33	1056
3	34	1156	31	1054
4	31	961	30	930
5	32	1024	34	1088
6	32	1024	32	1024
7	34	1156	36	1224
$N = 7$	$\Sigma x = 231$	$\Sigma x^2 = 7641$	$\Sigma y = 231$	$\Sigma xy = 7636$

Let the marks given by A be  $x$  and those given by B be  $y$ .

Then the line of regression of  $y$  on  $x$  is  $y = a + bx$ .

And the normal equations are

$$\Sigma y = Na + b \sum x$$

$$\Sigma xy = a \sum x + b \sum x^2 \quad \therefore 231 = 7a + 231b \quad \dots \dots \dots (1)$$

$$\Sigma xy = a \sum x + b \sum x^2 \quad \therefore 7636 = 231a + 7641b \quad \dots \dots \dots (2)$$

Multiply the first by 33 and subtract it from the second.

$$7636 = 231a + 7641b$$

$$7623 = 231a + 7626b$$

$$13 = 18b \quad \therefore b = 13/18 = 0.72$$

Putting this value in (1), we get,

$$231 = 7a + 231(0.72)$$

$$\therefore 7a = 231 - 231(0.72) = 64.68$$

$$\therefore a = 9.24$$

The equation of the line of regression of  $y$  on  $x$  is

$$y = 9.24 + 0.72x$$

To estimate  $y$  when  $x = 38$ , we put  $x = 38$  in the above equation

$$\therefore y = 9.24 + 0.72(38) = 36.6 = 37 \text{ approximately.}$$

Example 2 : Find the equations of the lines of regression for the following data.

$$x : 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11$$

$$y : 11 \ 14 \ 14 \ 15 \ 12 \ 17 \ 18$$

(M.U. 2003, 05, 16)

#### Calculations of regression

Sol. :

Sr. No.	$x$	$x^2$	$y$	$y^2$	$xy$
1	5	25	11	121	55
2	6	36	14	196	84
3	7	49	14	196	98
4	8	64	15	225	120
5	9	81	12	144	108
6	10	100	17	289	170
7	11	121	16	256	176
$N = 7$	$\Sigma x = 56$	$\Sigma x^2 = 476$	$\Sigma y = 99$	$\Sigma y^2 = 1427$	$\Sigma xy = 811$

Now, the line of regression of  $y$  on  $x$  is  $y = a + bx$ .

The normal equations are

$$\Sigma y = Na + b \sum x \quad \therefore 99 = 7a + 56b \quad \dots \dots \dots (1)$$

$$\Sigma xy = a \sum x + b \sum x^2 \quad \therefore 811 = 56a + 476b \quad \dots \dots \dots (2)$$

Multiply the first equation by 56 and the second by 7 and subtract

$$5544 = 392a + 3136b$$

$$5677 = 392a + 3332b$$

$$-133 = -196b \quad \therefore b = \frac{-133}{-196} = 0.6789$$

Putting this value of  $b$  in (1), we get

$$99 = 7a + 56 \times \frac{133}{196} \quad \therefore 7a = 99 - 38 \quad \therefore 7a = 61 \quad \therefore a = 8.7143$$

The equation of the line of regression of  $y$  on  $x$  is

$$y = 8.7143 + 0.6789x$$

Now, the equation of the line of regression of  $x$  on  $y$  is  $x = a + by$ .

Applied Mathematics - IV

(11-15)

The normal equations are

$$\begin{aligned} \sum x = Na + b \sum y & \therefore 56 = 7a + 99b \\ \sum xy = a \sum x + b \sum y^2 & \therefore 811 = 99a + 1427b \end{aligned}$$

Multiply the third equation by 99 and the fourth by 7 and subtract

$$\begin{aligned} 5544 = 693a + 9801b \\ 5677 = 693a + 9889b \end{aligned}$$

$$133 = 188b \quad \therefore b = \frac{133}{188} = 0.7074$$

Putting this value of  $b$  in (1), we get

$$56 = 7a + 99 \times \frac{133}{188} \quad \therefore 7a = 56 - 70.0372 = -14.0372 \quad \therefore a = -2.0053$$

The equation of the line of regression of  $x$  on  $y$  is

$$x = -2.0053 + 0.7074y$$

(Further the coefficient of correlation is given by

$$r = \sqrt{b_1 b_2} = \sqrt{0.6786 \times 0.7074} = 0.6928.$$

**Example 3 :** From the following table showing age of cars of a certain make and annual maintenance costs, obtain the regression equation for costs related to age.

Age of Cars (years) : 2, 4, 6, 7, 8, 10, 12.

Annual maintenance

Cost (Rs.) : 1,600, 1,500, 1,800, 1,900, 1,700, 2,100, 2,000.

Find the approximate cost of maintaining a 3 years old car of the same make.

Sol.: Calculations of regression

Sr. No.	$X - \bar{X}$			$Y - \bar{Y}$			Product $xy$
	$X$	$x$	$x^2$	$Y$	$y$	$y^2$	
1	2	-5	25	1,600	-200	40,000	1000
2	4	-3	9	1,500	-300	90,000	900
3	6	-1	1	1,800	0	0	0
4	7	0	0	1,900	100	10,000	0
5	8	1	1	1,700	-100	10,000	-100
6	10	3	9	2,100	300	90,000	900
7	12	5	25	2,000	200	40,000	1000
$N = 7$		$\Sigma X = 49$	$\Sigma x^2 = 70$	$\Sigma Y = 12,600$	$\Sigma y^2 = 2,80,000$	$\Sigma xy = 3,700$	

Let  $X$  denote age in years,  $Y$  denote cost in Rs.

$$\text{Now } \bar{X} = \frac{\Sigma X}{N} = \frac{49}{7} = 7, \quad \bar{Y} = \frac{12600}{7} = 1800$$

$$\text{and } b_{yx} = \frac{\Sigma xy}{\Sigma x^2} = \frac{3700}{40} = 52.86$$

The equation of the line of regression of  $Y$  on  $X$  is,

$$Y - \bar{Y} = b_{yx}(X - \bar{X}) \quad \therefore Y - 1800 = 52.86(X - 7)$$

Regression  
(3)  
(4)

Applied Mathematics - IV

(11-16)

Regression

To find the value of  $Y$  when  $X = 3$  put this value in the above equation,

$$Y - 1800 = 52.86(3 - 7) = -211.44$$

$$Y = 1800 - 211.44 = 1588.56$$

$\therefore$  The cost of maintenance of 3 years old car = ₹ 1588.56.

**Example 4 :** Find the coefficients of regression and hence the equations of the lines of regression for the following data.

$X$  : 78, 36, 98, 25, 75, 82, 90, 82, 65, 39.

$Y$  : 84, 51, 91, 60, 68, 62, 86, 58, 53, 47.

Draw the lines of regression from your equations on the graph. Estimate the value of  $Y$  when  $X = 50$  and the value of  $X$  when  $Y = 90$  from the graph.

What is the significance of the point of intersection of the two lines?

Calculations of coefficients of regression

Sol.:

Sr. No.	$X - \bar{X}$			$Y - \bar{Y}$			Product $xy$
	$X$	$x$	$x^2$	$Y$	$y$	$y^2$	
1	78	+13	169	84	+18	324	234
2	36	-29	841	51	-15	225	435
3	98	+33	1089	91	+25	625	825
4	25	-40	625	60	-6	36	240
5	75	+10	100	88	+2	4	20
6	82	+17	676	62	-4	16	-68
7	90	+25	825	86	+20	400	500
8	62	-3	9	58	-8	64	24
9	65	0	0	53	-13	169	0
10	39	-26	676	47	-19	361	494
$N = 10$		$\Sigma X = 650$	$\Sigma x^2 = 5398$	$\Sigma Y = 660$	$\Sigma y^2 = 2224$	$\Sigma xy = 2704$	

$$(i) \text{ Now } \bar{X} = \frac{\Sigma X}{N} = \frac{650}{10} = 65, \quad \bar{Y} = \frac{\Sigma Y}{N} = \frac{660}{10} = 66.$$

Coefficient of regression of  $Y$  on  $X$  is,

$$b_{yx} = \frac{\Sigma xy}{\Sigma x^2} = \frac{2704}{5398} = 0.5008$$

Coefficient of regression of  $X$  on  $Y$  is,

$$b_{xy} = \frac{\Sigma xy}{\Sigma y^2} = \frac{2704}{2224} = 1.215$$

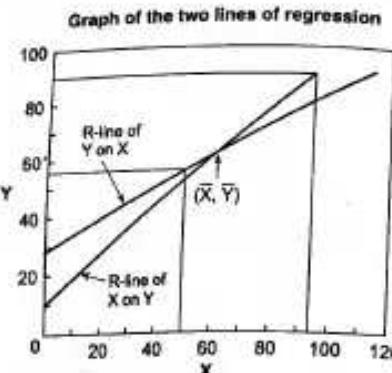
The equation of the line of regression of  $Y$  on  $X$  is,

$$Y - \bar{Y} = b_{yx}(X - \bar{X}) \quad \therefore Y - 66 = 0.5(X - 65)$$

The equation of the line of regression of  $X$  on  $Y$  is,

$$X - \bar{X} = b_{xy}(Y - \bar{Y}) \quad \therefore X - 65 = 1.2(Y - 66)$$

(ii)



To draw the lines of regression we take two points on each and connect them by a straight line.

$$\text{From } Y - 66 = 0.5(X - 65)$$

$$\text{we find that when } X = 65, Y = 66$$

$$\text{and when } X = 0, Y = 27.5$$

$$\text{From } X - 65 = 1.2(Y - 66)$$

$$\text{we find that when } Y = 66, X = 65$$

$$\text{and when } Y = 0, X = 12.5$$

To estimate  $Y$  when  $X = 50$  we draw a line at  $X = 50$ , parallel to  $y$ -axis to meet the line of regression of  $Y$  on  $X$  and read the corresponding value of  $Y$ . It is 58. To estimate  $X$  when  $Y = 90$ , we draw a line at  $Y = 90$ , parallel to  $x$ -axis, to meet the line of regression of  $X$  on  $Y$  and read the corresponding value of  $X$ . It is 94.

The two lines intersect at the point for which  $X = \bar{X} = 65$  and  $Y = \bar{Y} = 66$ .

**Example 5 :** A chemical engineer is investigating the effect of process operating temperature  $X$  on product yield  $Y$ . The study results in the following data.

$$X : 100, 110, 120, 130, 140, 150, 160, 170, 180, 190,$$

$$Y : 45, 51, 54, 61, 66, 70, 74, 78, 85, 89.$$

Find the equation of the least square line which will enable to predict yield on the basis of temperature. Find also the degree of relationship between the temperature and the yield.

Also verify that the sum of the coefficients of regression is greater than  $2r$ . (M.U. 2004, 18)

Sol.:

**Calculations of  $b_{xy}$ ,  $b_{yx}$  etc.**

Sr. No.	dx			dy			$d_x d_y$
	X	$X - 150$	$d_x^2$	Y	$Y - 70$	$d_y^2$	
1	100	-50	2500	45	-25	625	1250
2	110	-40	1600	51	-19	381	780
3	120	-30	900	54	-16	256	480
4	130	-20	400	61	-9	81	180
5	140	-10	100	66	-4	16	40
6	150	00	000	70	0	0	0
7	160	10	100	74	4	16	40
8	170	20	400	78	8	64	160
9	180	30	900	85	15	225	450
10	190	40	1600	89	19	361	760
N = 10		-50	8500		-27	2005	4120

$$\bar{X} = A + \frac{\sum dx}{N} = 150 - \frac{50}{10} = 145; \quad \bar{Y} = B + \frac{\sum dy}{N} = 70 - \frac{27}{10} = 67.3$$

$$b_{yx} = \frac{\sum d_x d_y - \frac{\sum d_x \sum d_y}{N}}{\sum d_x^2 - \frac{(\sum d_x)^2}{N}} = \frac{4120 - \frac{(-50)(-27)}{10}}{8500 - \frac{(-50)^2}{10}} = \frac{4120 - 135}{8500 - 250} = \frac{3985}{8250} = 0.483$$

$$b_{xy} = \frac{\sum d_x d_y - \frac{\sum d_x \sum d_y}{N}}{\sum d_y^2 - \frac{(\sum d_y)^2}{N}} = \frac{4120 - \frac{(-50)(-27)}{10}}{2005 - \frac{(-27)^2}{10}} = \frac{4120 - 135}{2005 - 72.9} = \frac{3985}{1932.1} = 2.06$$

The line of regression of  $Y$  on  $X$  is

$$Y - \bar{Y} = b_{yx}(X - \bar{X})$$

$$\therefore Y - 67.3 = 0.483(X - 145) \quad \therefore Y = 0.483X + 2.735$$

The coefficient of correlation

$$r = \sqrt{b_{yx} \times b_{xy}} = \sqrt{0.483 \times 2.06} = 0.9975$$

Now,  $b_{xy} + b_{yx} = 2.06 + 0.483 = 2.543$  and  $2r = 2 \times 0.9975 = 1.995$

Hence, we see that  $b_{yx} + b_{xy} > 2r$ .

**Miscellaneous Examples**

**Example 1 :** Find the angle between the lines of regression using the following data.

$$n = 10, \sum x = 270, \sum y = 630, \sigma_x = 4, \sigma_y = 5, r_{xy} = 0.6. \quad (\text{M.U. 1998})$$

Sol. : The angle between the lines of regression is given by

$$\tan \theta = \left( \frac{1 - r^2}{r} \right) \left( \frac{\sigma_x \cdot \sigma_y}{\sigma_x^2 + \sigma_y^2} \right)$$

Putting the given values

$$\tan \theta = \left( \frac{1 - r^2}{r} \right) \left( \frac{4 \times 5}{16 + 25} \right) = 0.52.$$

**Example 2 :** Discuss the statement "The sum of the two coefficients of regression is always greater than  $2r$  where  $r$  is the coefficient of correlation".

Sol. : We have proved above (§ 7, 3, page 11-9) that

$$b_{yx} + b_{xy} \geq 2r.$$

Because this statement leads us to

$$(\sigma_x - \sigma_y)^2 \geq 0 \text{ which is always true.}$$

This means the above given statement is partially true. The sum of the two coefficients of regression is greater than  $2r$  but not always. The sum can be also equal to  $2r$ .

The condition (A) shows that if  $\sigma_x = \sigma_y$ , then the sign of equality will hold and then  $b_{yx} + b_{xy}$  will be equal to  $2r$ .

This is also clear otherwise. From (1) and (1') (page 11-8), we have

$$b_{yx} + b_{xy} = r \frac{\sigma_x}{\sigma_y} + r \frac{\sigma_y}{\sigma_x}$$

If  $\sigma_x = \sigma_y$ , we will get  $b_{yx} + b_{xy} = 2r$ .

**Example 3 :** Given the following results of weights  $X$  and heights  $Y$  of 1000 men

$$\bar{X} = 150 \text{ lbs.}, \quad \sigma_x = 20 \text{ lbs.}$$

$$\bar{Y} = 68 \text{ inches.}, \quad \sigma_y = 2.5 \text{ inches.}, \quad r = 0.6.$$

where  $\bar{X}$  and  $\bar{Y}$  are means of  $X$  and  $Y$ ,  $\sigma_x$  and  $\sigma_y$  are standard deviations of  $X$  and  $Y$  and  $r$  is the correlation coefficient between  $X$  and  $Y$ .

John weighs 200 lbs., Smith is five feet tall. Estimate the height of John and weight of Smith.

From the value of height of John estimate his weight. Why is it different from 200?

Sol. : With the given notation the line of regression of  $Y$  on  $X$  is

$$Y - \bar{Y} = r \frac{\sigma_y}{\sigma_x} (X - \bar{X})$$

Substituting the given values,

$$Y - 68 = 0.6 \times \frac{2.5}{20} (X - 150) = \frac{15}{200} (X - 150).$$

Put  $X = 200$ ,

$$\therefore Y - 68 = \frac{15}{200} (200 - 150) = \frac{15}{4} = 3.75$$

$$\therefore Y = 68 + 3.75 = 71.75 \text{ inches.}$$

Now the line of regression of  $X$  of  $Y$  is

$$X - \bar{X} = r \frac{\sigma_x}{\sigma_y} (Y - \bar{Y})$$

Substituting the given values,

$$X - 150 = 0.6 \times \frac{20}{2.5} (Y - 68) = \frac{24}{5} (Y - 68)$$

Putting  $Y = 5$  feet = 60 inches.

$$\therefore X - 150 = \frac{24}{5} (60 - 68) = - \frac{192}{5}$$

$$\therefore X = 150 - \frac{192}{5} = 111.6 \text{ lbs.}$$

Hence, height of John = 71.75 inches and weight of Smith = 111.6 lbs.

To estimate the weight of John from his height 71.75 we have to use the equation of line of regression of  $X$  on  $Y$  (and not  $Y$  on  $X$ ).

$$\text{i.e., } X - 150 = \frac{24}{5} (Y - 68)$$

Putting  $Y = 71.75$ , we get

$$X - 150 = \frac{24}{5} (3.75) = 18 \quad \therefore X = 168.$$

The difference is due to the fact that for estimating  $Y$  we use one equation and for estimating  $X$  we use another equation.

**Example 4 :** Given  $6Y = 5X + 90$ ,  $15X = 8Y + 130$ ,  $\sigma_x^2 = 16$ .

Find (i)  $\bar{X}$  and  $\bar{Y}$ , (ii)  $r$  and (iii)  $\sigma_y^2$ .

(M.U. 2009, 10)

Sol.: (i) To find  $\bar{X}$  and  $\bar{Y}$  : We solve the given equations simultaneously. Multiply the first equation by 3.

$$\therefore -15X + 18Y = 270 \text{ and add } 15X - 8Y = 130$$

$$\therefore 10Y = 40 \quad \therefore \bar{Y} = 40$$

Putting this value in any of the given equations.

$$6 \times 40 = 5X + 90 \quad \therefore X = 30 \quad \therefore \bar{X} = 30.$$

(ii) To find  $r$  : Suppose the first equation represents the line of regression of  $X$  on  $Y$ .

$$\text{Writing it as } X = \frac{6}{5}Y - 18, \text{ we find } b_{xy} = \frac{6}{5}.$$

Suppose the second equation represents the line of regression of  $Y$  on  $X$

$$\text{Writing it as } Y = \frac{15}{8}X - \frac{130}{8}, \text{ we find } b_{yx} = \frac{15}{8}.$$

$$\therefore r = \sqrt{b_{xy} \times b_{yx}} = \sqrt{\frac{6}{5} \times \frac{15}{8}} = \sqrt{\frac{9}{4}} = \sqrt{2.25} = 1.5.$$

But the value of  $r$  can never be greater than 1 numerically. Hence, our supposition is wrong.

Now treating the first equation as representing the line of regression of  $Y$  on  $X$ , we write it as,

$$Y = \frac{5}{6}X + 15 \quad \therefore b_{yx} = \frac{5}{6}.$$

Treating the second equation as representing the line of regression of  $X$  on  $Y$ , we write it as,

$$X = \frac{8}{15}Y + \frac{130}{15} \quad \therefore b_{xy} = \frac{8}{15}$$

$$\therefore r = \sqrt{b_{xy} \times b_{yx}} = \sqrt{\frac{8}{15} \times \frac{5}{6}} = \sqrt{\frac{4}{9}} = \frac{2}{3} = 0.667.$$

(iii) To find  $\sigma_y$ .

$$\text{Consider, } b_{yx} = r \frac{\sigma_y}{\sigma_x} \quad \therefore \frac{5}{6} = \frac{2}{3} \times \frac{\sigma_y}{4} \quad \therefore \sigma_y = 5.$$

**Example 5:** The equations of the two regression lines are  $3x + 2y = 26$  and  $6x + y = 31$ .Find : (i) the means of  $x$  and  $y$ ,  
(ii) coefficient of correlation between  $x$  and  $y$ ,(iii)  $\sigma_y$  if  $\sigma_x = 3$ .

(M.U. 2007, 18)

**Sol. :** (i) To find  $\bar{x}$  and  $\bar{y}$ 

We solve the equations simultaneously. Multiply the second by 2 and subtract from the first.

$$\therefore 3x + 2y = 26$$

$$12x + 2y = 62$$

$$9x = 36 \quad \therefore x = 4.$$

Putting this value of  $x$  in the second equation, we get  $24 + y = 31 \quad \therefore y = 7$ .

$$\therefore \bar{x} = 4, \bar{y} = 7.$$

(ii) To find  $r$ : Suppose the first equation represents the line of regression of  $X$  on  $Y$ .

$$\text{Writing it as } 3x = -2y + 26. \quad \therefore x = -\frac{2}{3}y + \frac{26}{3}$$

$$\therefore \text{We find that } b_{yx} = -\frac{2}{3}.$$

Suppose the second equation represents the line of regression of  $Y$  on  $X$ ,

$$\text{Writing it as } y = -6x + 31 \quad \therefore b_{xy} = -6.$$

$$\therefore r = \sqrt{b_{yx} \cdot b_{xy}} = \sqrt{(-2/3)(-6)} = \sqrt{4} = 2$$

But the value of  $r$  can never be greater than 1. Hence, our supposition is wrong.Now, treating the first equation as representing the line of regression of  $Y$  on  $X$ , we write it as

$$2y = -3x + 26 \quad \therefore y = -\frac{3}{2}x + 13 \quad \therefore b_{yx} = -\frac{3}{2}.$$

Treating the second equation as representing the line of regression of  $X$  on  $Y$ , we write it as

$$6x = -y + 31 \quad \therefore x = -\frac{1}{6}y + \frac{31}{6} \quad \therefore b_{xy} = -\frac{1}{6}.$$

$$\therefore r = \sqrt{b_{yx} \cdot b_{xy}} = \sqrt{\left(-\frac{3}{2}\right)\left(-\frac{1}{6}\right)} = \sqrt{\frac{1}{4}} = \frac{1}{2} = 0.5$$

Since, both  $b_{yx}$  and  $b_{xy}$  are negative  $r$  is negative.  $\therefore r = -0.5$ .(iii) To find  $\sigma_y$ : Consider  $b_{yx} = r \frac{\sigma_y}{\sigma_x}$ .But  $b_{yx} = -\frac{3}{2}$ ,  $r = -\frac{1}{2}$ , and  $\sigma_x = 3$ .

$$\therefore \sigma_y = b_{yx} \cdot \frac{\sigma_x}{r} = \left(-\frac{3}{2}\right) \cdot \frac{3}{(-1/2)} = 9$$

**Example 6 :** The regression lines of a sample are  $x + 6y = 6$ , and  $3x + 2y = 10$ . Find (i) sample means  $\bar{x}$  and  $\bar{y}$ , (ii) coefficient of correlation between  $x$  and  $y$ . Also estimate  $y$  when  $x = 12$ .

(M.U. 2004, 14, 15)

Also verify that the sum of the coefficients of regressions is greater than  $2r$ .Sol. : (i) Mean  $\bar{x}$  and  $\bar{y}$  are obtained by solving the two given equations.

$$3x + 18y = 18 \quad \therefore y = 1/2$$

$$3x + 2y = 10 \quad \therefore x = 3$$

$$16y = 8$$

(ii) If the line  $x + 6y = 6$  is the line of regression of  $y$  on  $x$ , then

$$6y = -x + 6 \quad \text{i.e. } y = -\frac{1}{6}x + 1 \quad \therefore b_{yx} = -\frac{1}{6}$$

If the line  $3x + 2y = 10$  is the line of regression of  $x$  on  $y$ , then

$$3x = -2y + 10 \quad \text{i.e. } x = -\frac{2}{3}y + \frac{10}{3} \quad \therefore b_{xy} = -\frac{2}{3}$$

$$\therefore r = \sqrt{b_{yx} \cdot b_{xy}} = \sqrt{\left(-\frac{1}{6}\right) \times \left(-\frac{2}{3}\right)} = \sqrt{\frac{1}{9}} = \frac{1}{3}$$

Since  $b_{yx}$  and  $b_{xy}$  are both negative,  $r$  is negative  $\therefore r = -1/3$ .

$$\text{Since } b_{yx} + b_{xy} = \frac{1}{6} + \frac{2}{3} = \frac{5}{6} \text{ (Numerically)}$$

and  $2r = \frac{2}{3}$ , we see that  $b_{yx} + b_{xy} > 2r$ .(iii) To estimate  $y$  when  $x = 12$ , we use the line of regression of  $y$  on  $x$  i.e.  $y = -\frac{1}{6}x + 1$ , when  $x = 12$ ,  $y = -2 + 1 = -1$ .**Example 7 :** If the tangent of the angle made by the line of regression of  $y$  on  $x$  is 0.6 and  $\sigma_y = 2\sigma_x$ , find the correlation coefficient between  $x$  and  $y$ .

(M.U. 2004, 09, 10, 15)

Sol. : If the equation of the line of regression of  $y$  on  $x$  is  $y - \bar{y} = b_{yx}(x - \bar{x})$  then we know that  $b_{yx}$  is the slope of the line of regression. We are thus, given  $b_{yx} = 0.6$ .

$$\text{But } b_{yx} = r \frac{\sigma_y}{\sigma_x} \quad \text{and } \sigma_y = 2\sigma_x$$

$$\text{Putting these values, } 0.6 = r \cdot \frac{2\sigma_x}{\sigma_x} = 2r \quad \therefore r = \frac{0.6}{2} = 0.3$$

**Example 8 :** If  $\sigma_x = \sigma_y = \sigma$  and the angle between the lines of regression is  $\tan^{-1} 3$ , find the coefficient of correlation.

Sol. : We have

$$\tan \theta = \frac{1 - r^2}{r} \left( \frac{\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2} \right) \quad \therefore 3 = \frac{1 - r^2}{r} \cdot \left( \frac{\sigma^2}{\sigma^2 + \sigma^2} \right) = \frac{1 - r^2}{2r}$$

$$\therefore \frac{1 - r^2}{r} = 6 \quad \therefore r^2 + 6r - 1 = 0 \quad \therefore r = \frac{-6 \pm \sqrt{36 - 4}}{2} = -3 \pm 2\sqrt{2}$$

Since  $r$  cannot be numerically greater than 1,  $r = -3 + 2\sqrt{2} = -0.17$ .

**Example 9 :** The following data regarding the heights ( $y$ ) and weights ( $x$ ) of 100 college students are given  
 $\Sigma x = 15000$ ,  $\Sigma x^2 = 2272500$ ,  $\Sigma y = 6800$ ,  $\Sigma y^2 = 463025$ ,  $\Sigma xy = 1022250$ .

Find the coefficient of correlation between height and weight and also the equation of regression of height and weight.  
 Sol. : The coefficients of regression are given by (M.U. 1998)

$$b_{yx} = \frac{\sum xy - \frac{\sum x \cdot \sum y}{N}}{\sum x^2 - \frac{(\sum x)^2}{N}} = \frac{1022250 - \frac{15000 \times 6800}{100}}{2272500 - \frac{15000^2}{100}} = \frac{2250}{22500} = 0.1.$$

$$b_{xy} = \frac{\sum xy - \frac{\sum x \cdot \sum y}{N}}{\sum y^2 - \frac{(\sum y)^2}{N}} = \frac{1022250 - \frac{15000 \times 6800}{100}}{463025 - \frac{6800^2}{100}} = \frac{2250}{625} = 3.6.$$

$$\therefore r = \sqrt{b_{yx} \times b_{xy}} = \sqrt{0.1 \times 3.6} = 0.6.$$

The equation of the lines of regression of  $y$  on  $x$  is

$$y - \bar{y} = b_{yx}(x - \bar{x}) \quad \therefore y - 68 = 0.1(x - 1500)$$

$$\therefore y = 0.1x - 82.$$

**Example 10 :** It is given that the means of  $x$  and  $y$  are 5 and 10. If the line of regression of  $y$  on  $x$  is parallel to the line  $20y = 9x + 40$ , estimate the value of  $y$  for  $x = 30$ . (M.U. 1998, 2015)

Sol. : The line of regression of  $y$  on  $x$  is  $y - \bar{y} = b_{yx}(x - \bar{x})$ .

Its slope is  $b_{yx}$ . But this line is parallel to  $20y = 9x + 40$

$$\text{i.e. } y = \frac{9}{20}x + 2 \text{ whose slope is } \frac{9}{20}. \quad \therefore b_{yx} = \frac{9}{20}.$$

But by data  $\bar{x} = 5$  and  $\bar{y} = 10$ . Hence, the equation of the line of regression of  $y$  on  $x$  is

$$y - 10 = \frac{9}{20}(x - 5) \quad \text{i.e. } y = \frac{9}{20}x + \frac{155}{20}$$

$$\text{When } x = 30, \quad y = \frac{270}{20} + \frac{155}{20} = \frac{425}{20} = 21.25.$$

### EXERCISE - I

#### Type I

State true or false with proper reasoning.

1. If  $r = 0$ , the lines of regression are parallel to each other. [Ans. : False]
2. The values of  $r$  and  $R$  can never be equal. [Ans. : False]
3. In a regression analysis it was found that  $b_{yx} = 0.87$ ,  $b_{xy} = 1.55$ . These values are not consistent. [Ans. : True]
4. The two regression coefficients are both positive or both negative. [Ans. : True]
5.  $3x + y = 5$  and  $2x - 3y = 7$  cannot be lines of regression for any set of values of  $x$  and  $y$ . [Ans. : True]

**Type II**  
 1. The following table gives the age of car of a certain make and annual maintenance cost. Obtain the equation of the line of regression of cost on age.

Age of a car : 2 4 6 8  
 Maintenance : 1 2 2.5 3 (M.U. 1998, 2014) [Ans. :  $y = 0.325x + 0.5$ ]

2. Obtain the equation of the line of regression of  $y$  on  $x$  from the following data and estimate  $y$  when  $x = 73$ .

$x$  : 70, 72, 74, 76, 78, 80  
 $y$  : 163, 170, 179, 188, 196, 220.

[Ans. :  $y = 5.31x - 212.57$ ;  $y = 175.37$ ] (M.U. 1997)

3. The heights in cms of fathers ( $x$ ) and of the eldest sons ( $y$ ) are given below.

$x$  : 165 160 170 163 173 158 178 168 173 170 175 180  
 $y$  : 173 168 173 165 175 168 173 165 180 170 173 178

Estimate the height of the eldest son if the height of the father is 172 cms. and the height of the father if the height of the eldest son is 173 cm.

Also find the coefficient of correlation between the heights of fathers and sons.

(M.U. 2002, 05)

[Ans. : (i)  $y = 1.016x - 5.123$ , (ii)  $x = 0.476y + 98.98$ , (iii) 169.97, 173.45, (iv)  $r = 0.996$ ]

4. Find (i) the lines of regression, (ii) coefficient of correlation for the following data.

$x$  : 65 66 67 67 68 69 70 72

$y$  : 67 68 65 66 72 72 69 71

(M.U. 2002, 14)

[Ans. : (i)  $y = 19.79 + 0.72x$ , (ii)  $x = 33.29 + 0.5y$ ;  $r = 0.6$ ]

5. Find the line of regression for the following data and estimate  $y$  corresponding to  $x = 15.5$ .

$x$  : 10 12 13 16 17 20 25

$y$  : 19 22 24 27 29 33 37

(M.U. 2004) [Ans. :  $y = 0.8x + 13.23$ ; 25.63]

#### Type III

1. Given      **x series**      **y series**

Mean	18	100
S.D.	14	20

$$r = 0.8.$$

Find the most probable value of  $y$  when  $x = 70$  and most probable value of  $x$  when  $y = 90$ .

[Ans. :  $y = 159.3$ ,  $x = 12.4$ ]

2. Given the following information about marks of 60 students.

Mathematics      English

Mean      80      50

S.D.      15      10

Coefficient of correlation  $r = 0.4$ . Estimate the marks of the student in mathematics who scored 60 marks in English. (M.U. 2006) [Ans. : 86]

3. You are supplied with the following information. The equation of the lines of regression are  $2x + 3y + 8 = 0$  and  $x + 2y - 5 = 0$ .

Find the means of  $x$  and  $y$  and the coefficient of correlation between them. (M.U. 1997)

[Ans. :  $\bar{x} = -31$ ,  $\bar{y} = 18$ ,  $r = -0.87$ ]

4. From 8 observations the following results were obtained :  
 $\sum x = 59, \sum y = 40, \sum x^2 = 524, \sum y^2 = 256, \sum xy = 364$ .  
 Find the equation of the line of regression of  $x$  on  $y$  and the coefficient of correlation.

[ Ans. :  $x = 1.5y - 0.5, r = 0.98$  ]

5. The equations of the two lines of regression are  $x = 19.13 - 0.87y$  and  $y = 11.84 + 0.50x$ .  
 Find (i) the means of  $x$  and  $y$ , (ii) the coefficient of correlation between  $x$  and  $y$ .

[ Ans. : (i)  $\bar{x} = 15.79, \bar{y} = 3.74$ ; (ii)  $r = -0.66, b_{yx} = -0.50, b_{xy} = -0.87$  ]

6. Out of the two equations given below which can be a line of regression of  $x$  on  $y$  and why?  
 $x + 2y - 6 = 0$  and  $2x + 3y - 8 = 0$ . (M.U. 2003) [ Ans. :  $2x + 3y - 8 = 0$  ]

7. In a partially destroyed laboratory record of analysis of correlation data the following results are legible. Variance of  $x = 9$ , equations of the lines of regression

$$4x - 5y + 33 = 0, 20x - 9y - 107 = 0.$$

- Find (i) the mean values of  $x$  and  $y$ , (ii) the standard deviation of  $y$ , (iii) coefficient of correlation between  $x$  and  $y$ . (M.U. 1999, 2003) [ Ans. : (i)  $\bar{x} = 13, \bar{y} = 17$ , (ii)  $\sigma_y = 4$ , (iii)  $r = 0.6$  ]

8. Given :  $\text{var}(x) = 25$ . The equations of the two lines of regression are  $5x - y = 22$  and  $64x - 45y = 24$ .

- Find (i)  $\bar{x}$  and  $\bar{y}$ , (ii)  $r$ , (iii)  $\sigma_y$ .

(M.U. 1999)

[ Ans. : (i)  $\bar{x} = 6, \bar{y} = 8$ , (ii)  $r = 1.87$ , (iii)  $\sigma_y = 1.5$  ]

9. Find the regression coefficients and the coefficient of correlation from the following data where  $x, y$  denote the actual values.

$$N = 12, \sum x = 120, \sum y = 432, \sum xy = 4992, \sum x^2 = 1392, \sum y^2 = 18252.$$

[ Ans. :  $b_{yx} = 3.5, b_{xy} = 0.249, r = 0.99$  ]

## EXERCISE - II

### Theory

- Distinguish between correlation and regression.
- Explain "the line of regression". Why there are two lines of regression ? (M.U. 2007)
- Explain what you understand by regression. What are lines of regression ? Why are there in general two lines of regression ? When do they coincide, when are they perpendicular ? (M.U. 2004)
- Explain the method of scatter diagram to obtain a line of regression.
- Obtain the equations of lines of regression. (M.U. 2002, 03)
- Prove that the sum of the coefficients of regression is greater than or equal to  $2r$  where  $r$  is the coefficient of correlation. [ See 3, page 11-9 ] (M.U. 1999)
- Find the expression for the acute angle between the lines of regression. (M.U. 2004, 05)
- With usual notation prove that
  - $r = \sqrt{b_{yx} \cdot b_{xy}}$ ,
  - $b_{xy} + b_{yx} \geq 2r$ .

9. Examine whether the following statement is correct

$$b_{xy} = 3.2, b_{yx} = 0.7.$$

10. If  $\theta$  is the angle between the two lines of regression, prove that

$$\tan \theta = \left( \frac{1 - r^2}{r} \right) \left( \frac{\sigma_x - \sigma_y}{\sigma_x^2 + \sigma_y^2} \right)$$

(M.U. 1998, 2004, 07)



[ Ans. : No ]

# Graphs

## 1. Introduction

Graph Theory is a fast growing branch of Mathematics, having its place in several branches of Mathematics, and also of Science, Engineering, Chemistry, Defence etc. In computer engineering it is an unavoidable tool having applications in switching theory, artificial intelligence, computer graphics etc.

For us a graph is different from what you have in mind since school-days. A graph consists of two things vertices and edges. We shall denote the vertices by  $v_1, v_2, \dots$  and edges by  $e_1, e_2, \dots$  and their sets by capital letters  $V$  and  $E$ . Every edge corresponds to a pair of vertices. We denote this as  $e_1 = \{v_1, v_2\}$ ,  $e_2 = \{v_2, v_3\}$  etc.

In this chapter we shall first define and illustrate the following terms.

- (1) Graph, (2) Vertex, node, point, (3) Edge, curve, line,
- (4) Loop, (5) Parallel edges multiple edges, (6) Simple graph,
- (7) Multiple graph, (8) Adjacent vertices, (9) Incident edge,
- (10) Degree of a vertex, (11) Pendant vertex, (12) Pendant edge.

Then we shall prove some interesting theorems about graphs and shall then define specific types of graphs viz.

- (1) Complete graph, (2) Regular graph, (3) Planar graph.

## 2. Basic Terms

**Definition 1 :** A graph is an ordered pair  $(V, E)$  of two sets  $V$  and  $E$  satisfying the following conditions :

- (i)  $V$  is a finite non-empty set.
- (ii) each  $e \in E$  corresponds to a unique unordered pair  $v_1, v_2$  of elements of  $V$ .

(M.U. 1996)

**Definition 2 :** The elements of the set  $V$  are called vertices of the graph  $(V, E)$ . A vertex is also referred to as a node or a point.

**Definition 3 :** The elements of  $E$  are called edges. An edge is also referred to as a curve or a line.

**Definition 4 :** If an edge starts and ends in the same vertex then it is called a loop (or a self loop).

In the graph shown in Fig. 12.2,  $G_1$ ,  $e_1$  is a loop.

**Definition 5 :** If two edges have the same starting vertex and the same end vertex they are called parallel edges or multiple edges.

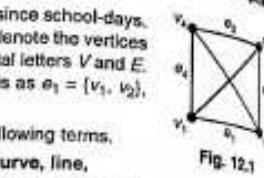


Fig. 12.1

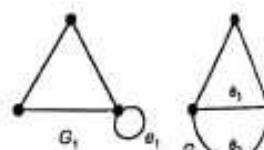


Fig. 12.2

## Applied Mathematics - IV

(12-2)  
Graphs

In the above graph  $G_2$ ,  $e_1$  and  $e_2$  are parallel edges (although they meet at the two ends). It is joining two cities by two different roads.

**Definition 6 :** A graph having no loops or parallel edges is called a simple graph or (simply) a graph.

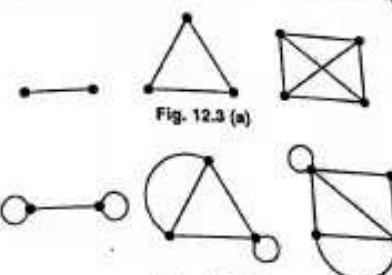


Fig. 12.3 (a)

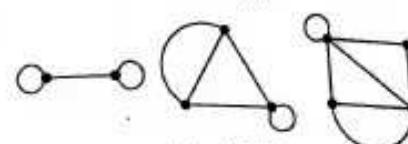


Fig. 12.3 (b)

The graphs shown in Fig. 12.3 (a) are simple graphs. The graphs shown in Fig. 12.3 (b) are not simple graphs.

**Example 1 :** Prove that in a simple graph having  $n$  vertices, there can be at most  $n(n-1)/2$  edges.

**Sol. :** If we are given  $n$  vertices, we can join any two of them to get a simple graph. But  $n$  vertices can be taken two at a time in  ${}^n C_2 = n(n-1)/2$  ways.

Hence, there will be at most  $n(n-1)/2$  edges.

In the above graph 8.3 (a), when there are two vertices the number of edges =  $2(2-1)/2 = 1$ , when there are three vertices the number of edges =  $3(3-1)/2 = 3$ , etc.

**Example 2 :** Can we have a simple graph with 6 vertices and 16 edges?

**Sol. :** In a simple graph with 6 vertices there can be at most  $6(6-1)/2 = 15$  edges.

Hence, we cannot have a simple graph with 6 vertices and 16 edges.

**Example 3 :** Show that the maximum degree of any vertex in a simple graph of  $n$  vertices is  $(n-1)$ .

**Sol. :** Consider a simple graph  $G$  (similar to any one shown above in Fig. 12.3 (a)) with  $n$  vertices.

As the graph is simple, it has no loops or parallel edges as in graphs of 8.13 (b). Now, consider any vertex of such a simple graph. Each vertex can be adjacent to at most  $(n-1)$  vertices. Hence, there will be at most  $(n-1)$  edges. Hence, the maximum degree of any vertex is  $(n-1)$ .

[In Fig. 12.13 (a), in the first graph, there are ( $n=2$ ) two vertices each of degree ( $(n-1)=1$ ), in the second graph, there are ( $n=3$ ) 3 vertices each of degree ( $(n-1)=2$ ), in the third graph, there are ( $n=4$ ) 4 vertices each of degree ( $(n-1)=3$ ).]

**Definition 7 :** A graph which is not simple is called a multigraph.

In the graphs (Fig. 12.4),  $G_1$  is (a) simple graph and (b) is a multigraph.

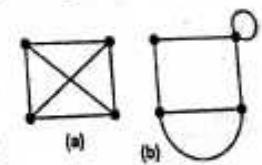


Fig. 12.4

**3. Adjacency and Incidence**

**Definition 8 :** If there is an edge between two vertices  $v_1$  and  $v_2$  then they are called adjacent vertices.

In the graph  $G$ ,  $v_1$  and  $v_2$ ,  $v_2$  and  $v_3$  are adjacent vertices but  $v_1$  and  $v_3$ ,  $v_2$  and  $v_4$  etc. are not adjacent vertices.

**Definition 9 :** If an edge starts (or ends) from a vertex then the edge is said to be incident edge on the vertex.

In the graph shown in Fig. 12.5, the edge  $e_1$  is incident on  $v_1$  or on  $v_2$ , the edge  $e_2$  is incident on  $v_2$  or on  $v_3$  etc.

**Definition 10 :** The number of edges incident (coming or leaving but counted once only) at a vertex is called the degree or the valency of the vertex. The degree of a vertex  $v$  is denoted by  $d(v)$ .

In the graph  $G$  (Fig. 12.5), the degree of the vertex  $v_1$  is 2, of  $v_2$  is 3, of  $v_3$  is 2 and of  $v_4$  is 1.

**Definition 11, 12 :** If only one edge is incident at a vertex  $v$ , then its degree is one and it is called a pendant vertex and the corresponding edge is called pendant edge.

In a loop, the same edge is incident at  $v$  twice; the degree of a loop is two.

In the graph  $G$ , there is no edge incident at  $v_5$  hence  $v_5$  is an isolated vertex; its degree is zero. There is only one edge incident at  $v_1$ , hence it is a pendant vertex; its degree is one. The degree of  $v_3$  is two. Since  $v_4$  is a loop and since two more edges are incident at  $v_4$ , the degree of  $v_4$  is four.

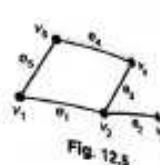


Fig. 12.5

Fig. 12.6

**Theorem 1 (Hand Shaking Lemma) :** The sum of degrees of all vertices of any graph is equal to twice number of edges.

**Proof :** Let  $G = (V, E)$  be a graph with  $m$  vertices  $v_1, v_2, \dots, v_m$  and  $n$  edges  $e_1, e_2, \dots, e_n$ . I.e.,  $V = \{v_1, v_2, \dots, v_m\}$  and  $E = \{e_1, e_2, \dots, e_n\}$ .

If  $E = \emptyset$  i.e.  $n = 0$ , (See  $G_1$ ) the degree of each vertex is zero i.e.,  $d(v_i) = 0$  for all  $i = 1, 2, \dots, n$ .  
 $\therefore \sum d(v_i) = 0$ .

The theorem is trivially true.

If  $E \neq \emptyset$  and if  $e \in E$  then  $e$  is an edge between two vertices say  $v_1$  and  $v_2$ . Clearly,  $e$  contributes 1 to  $d(v_1)$  and 1 to  $d(v_2)$  (See  $G_2$ ). Thus, each edge contributes precisely '2' to the sum of degrees of all vertices. Since there are  $n$  edges in  $G$ , the total contribution to the sum of degrees is  $2n$ .

$$\therefore \sum d(v_i) = 2n.$$

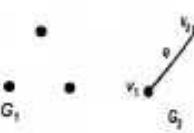


Fig. 12.7

**Remark ...**

The theorem can also be stated as "The sum of degrees of all vertices of any graph is even".

**Note ...**

The theorem 1 is also known as Hand Shaking Lemma. This is so because if in a party n hand-shakes occur, then as in each handshake two hands are involved, the total number of hands involved is  $2n$ .

**Example :** Verify Hand Shaking Lemma for the graph given in Fig. 12.8.

Sol. : In the above graph there are 5 vertices,  $d(v_1) = 1$ ,  $d(v_2) = 3$ ,  $d(v_3) = 2$ ,  $d(v_4) = 4$ ,  $d(v_5) = 0$ , and there are ( $n = 5$ ) 5 edges  $e_1, e_2, e_3, e_4, e_5$ .

$$\therefore \sum d(v_i) = 1 + 3 + 2 + 4 + 0 = 10$$

And  $2n = 2(5) = 10$  ( $n$  = number of edges). Hence,  $\sum d(v_i) = 2n$ .

**Theorem 2 :** In any graph the number of vertices of odd degree is even.

**Proof :** Let  $G = (V, E)$  be a graph. Let  $v_1, v_2, \dots, v_p$  be the vertices of odd degree and  $w_1, w_2, \dots, w_q$  be the vertices of even degree.

We have to show that  $p$  is even. Now there are two possibilities  $p = 0, p \neq 0$ .

(i) Let  $p = 0$  i.e. there is no vertex of odd degree.

But zero is an even integer and hence, the theorem is true.  
 (See Ex. 1 below)

(ii) Let  $p \neq 0$  i.e. let there be some vertices of odd degree.

Now, by the above theorem sum of the degrees of all vertices,

$$\sum_{i=1}^n d(v_i) = 2n$$

If we consider  $p$  vertices of odd degree and  $q$  vertices of even degree separately, then

$$\sum_{i=1}^p d(v_i) = \sum_{i=1}^p d(u_i) + \sum_{i=1}^q d(w_i) = 2n$$

But since  $d(w_i)$  is even for each  $i = 1, 2, \dots, q$ , then sum,  $\sum d(w_i)$  is even. Since the right hand side is even, the first term is also even

$$\therefore \sum_{i=1}^p d(u_i) \text{ is even.}$$

But by our supposition  $u_1, u_2, \dots, u_p$  are all odd vertices. If  $p$  is odd  $\sum_{i=1}^p d(u_i)$  (being the sum of odd numbers each of which is odd e.g.  $3 + 5 + 7 = 15$ ) will be odd. Hence,  $\sum_{i=1}^p d(u_i)$  is even is impossible.

Hence,  $p$  is even.

**Example 1 :** Find the number of vertices in a simple graph having  $n$  edges and having each vertex of degree 2. (M.U. 2011, 13, 14)

**Sol. :** Since each vertex is of degree 2, from any vertex, we have one edge going out and one edge coming in.

Between two vertices there is only one edge. Since there are thus  $n$  edges there will be  $n$  vertices.



Fig. 12.8

**Example 2 :** Find the number of vertices in a simple graph with exactly six edges in which each vertex is of degree 2. (M.U. 2013, 14)

**Sol. :** Let the number of vertices be  $n$ . Since each vertex is of degree 2, the sum of the degrees of all vertices =  $2n$ .

But by theorem 1 above, the sum of degrees of all vertices is equal to twice the number of edges. Since there are by data 6 edges, the sum of the degrees =  $2 \times 6 = 12$ .



Fig. 12.9

$$\text{Thus, } 2n = 12 \quad \therefore n = 6$$

Hence, there are 6 vertices. (See Fig. 12.9 on the previous page)

**Example 3 :** Determine the number of edges in a graph with 6 nodes, 2 of degree 4 and 4 of degree 2. Draw two such graphs.

**Sol.:** Let there be  $e$  edges. Then by theorem 1 above, the sum of degrees of all vertices  $= 2e$ .

Since there are 2 vertices of degree 4 and 4 vertices of degree 2, the sum of the degree of all vertices

$$= (4 \times 2) + (2 \times 4) = 16.$$

$$\text{Hence, } 16 = 2e \quad \therefore e = 8$$

There will be 8 edges in the graph.

Two such graphs are shown in Fig. 12.10.

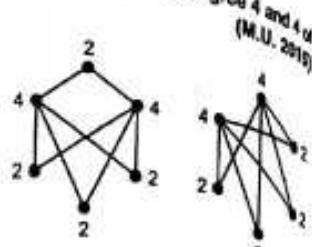


Fig. 12.10

#### 4. Types of Graphs

We shall now consider some special types of graphs.

##### (1) Complete Graph

**Definition :** A simple graph of  $n$  vertices in which the degree of each vertex is  $(n - 1)$  is called a complete graph and is denoted by  $K_n$ .

In other words in a complete graph of  $n$  vertices each vertex is connected with any other. Thus, if  $G = (V, E)$  is complete, then

(i)  $G$  has no loops.

(ii)  $G$  has no multiple edges.

(iii) If  $v_1, v_2$  are any two vertices there is precisely one edge between  $v_1$  and  $v_2$ .

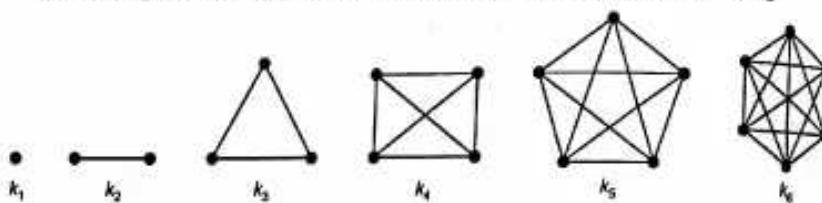


Fig. 12.11

A complete graph with  $n$  vertices is denoted by  $K_n$ .  $K$  stands for completeness and  $n$  denotes number of vertices. The above figures show complete graphs  $K_n$  for  $n = 1, 2, 3, 4, 5, 6$ .

A complete graph has the following properties.

**Property 1 :** Every pair of vertices is adjacent in  $K_n$ .

**Property 2 :** In  $K_n$ , each vertex has the same degree and that degree is  $(n - 1)$ .

**Property 3 :** The total number of edges in  $K_n$  is  $\frac{n(n - 1)}{2}$ , (where  $n$  is the number of vertices).

**Proof :** Let  $G$  be a simple graph with  $n$  vertices. Let  $e$  be the number of edges in the graph  $G$ . Then by Hand Shaking Lemma

$$d(v_1) + d(v_2) + \dots + d(v_n) = 2e$$

But by property (2), (See the previous page) each vertex has the degree  $(n - 1)$ .

$$\therefore (n - 1) + (n - 1) + \dots + (n - 1) = 2e$$

$$\therefore n(n - 1) = 2e \quad \therefore e = \frac{n(n - 1)}{2}$$

**Example 1 :** Can a complete graph with 8 vertices have 40 edges excluding self loop.

[M.U. 2016]

**Sol.:** For a complete graph with 8 vertices there are

$$\frac{8(8 - 1)}{2} = \frac{8 \cdot 7}{2} = 28 \text{ edges.}$$

Hence, there cannot be graph of 8 vertices and 40 edges.

**Example 2 :** Verify the result that in a complete graph  $K_m$  the number of edges  $= \frac{m(m - 1)}{2}$  for the graph shown in Fig. 12.10.

[M.U. 2016]

**Sol.:** The above graph is complete because (i) it has no loops, (ii) it has no multiple edges, (iii) each vertex is joined with each of the remaining vertices by a single edge.

Now, there are 10 edges. They are

(1) 4 edges  $\{v_1, v_j\}; j = 2, 3, 4, 5$

(2) 3 edges  $\{v_2, v_j\}; j = 3, 4, 5$

(3) 2 edges  $\{v_3, v_j\}; j = 4, 5$

(4) 1 edges  $\{v_4, v_5\}$

Since there are 5 vertices  $v_1, v_2, v_3, v_4, v_5, m = 5$ .

$$\therefore \text{Number of edges} = \frac{m(m - 1)}{2} = \frac{5 \times 4}{2} = 10 \text{ as shown.}$$

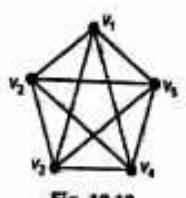
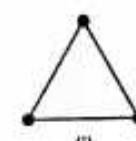


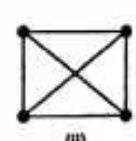
Fig. 12.12

#### EXERCISE - I

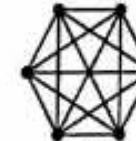
1. Verify that in  $K_m$  the number of edges in a graph is  $\frac{m(m - 1)}{2}$  for the following graphs.



(i)



(ii)



(iii)

2. Find the number of edges in a complete graph with 7 vertices.

[Ans. : 21]

3. Find the number of edges in  $K_{11}$ .

[Ans. :  $\frac{11 \times 10}{2} = 55$ ]

##### (2) Regular Graph

**Definition :** A graph in which every vertex has the same degree is called a regular graph. In other words if the number of edges incident at a vertex is the same, then the graph is called a regular graph. If the common degree of a vertex is  $r$  then it is called an  $r$ -regular graph or regular graph of degree  $r$ .

Clearly, a complete graph of  $n$  number of vertices is  $(n-1)$ -regular graph because in such a graph, we have seen that at each vertex there are  $(n-1)$  incident edges. But the converse is not true. A regular graph need not be complete.

The graphs shown below are regular but not complete. In the first and second figure there are two edges incident at each vertex. In the third and fourth figures there are three edges incident at each vertex. In the last figure there are four edges incident at each vertex. But these graphs are not complete because each vertex is not connected with the remaining vertices except (i) and the last is not a simple graph.

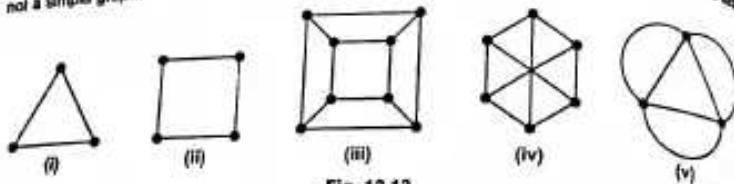


Fig. 12.13

**Example 1:** If  $r$  and  $n$  are odd natural numbers, then there cannot be an  $r$ -regular graph with  $n$  vertices.

**Sol.:** If possible let there be an  $r$ -regular graph  $G = (V, E)$  with  $n$  vertices  $v_1, v_2, \dots, v_n$  where  $r$  and  $n$  both are odd.

By data  $d(v_i) = r$  for all  $i = 1, 2, \dots, n$ .

$$\therefore \sum d(v_i) = rn$$

Since  $r$  and  $n$  both are odd,  $rn$  is an odd natural number.

But by Theorem 1, page 12-3,  $\sum d(v_i)$  is an even number. Hence, this is a contradiction.

$\therefore$  There is no  $r$ -regular graph with  $n$ -vertices where both  $r$  and  $n$  are odd.

**Example 2:** Can we have a graph in which there are 5 vertices and the degree of each vertex is 3.

**Sol.:** No because of the above result.

**Example 3:** If  $G = (V, E)$  is an  $r$ -regular graph with  $n$  vertices and  $m$  edges then  $m = \frac{nr}{2}$ .

**Sol.:** Let  $V = \{v_1, v_2, \dots, v_n\}$ . Then by Theorem 1, page 12-3,  $\sum d(v_i) = 2m$ .

Since  $G$  is regular,  $d(v_i) = r$ , for  $i = 1, 2, \dots, n$ .

$$\therefore \sum d(v_i) = rn \quad \therefore rn = 2m \quad \therefore m = \frac{rn}{2}.$$

**Example 4:** Verify the result that for a  $r$ -regular graph with  $n$  vertices and  $m$  edges  $m = \frac{nr}{2}$  for the graph shown in Fig. 12.14.

**Sol.:** We have 6 vertices  $v_1, v_2, v_3, v_4, v_5, v_6$ . There are the following 9 edges.

3 edges  $\{v_1, v_j\}$ ;  $j = 2, 4, 6$

2 edges  $\{v_2, v_j\}$ ;  $j = 3, 5$

2 edges  $\{v_3, v_j\}$ ;  $j = 4, 6$

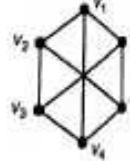


Fig. 12.14

$$\begin{aligned} & 1 \text{ edge } \{v_4, v_5\} \\ & 1 \text{ edge } \{v_5, v_6\} \\ & \text{Degree of each vertex is 3.} \\ & \therefore n = 6, m = 9, r = 3. \quad \therefore \frac{nr}{2} = \frac{6 \times 3}{2} = 9 = m \\ & \text{Hence, the } m = \frac{nr}{2} \text{ is verified.} \end{aligned}$$

**EXERCISE - II**

1. Give an example of an  $r$ -regular graph and verify for the same graph the result  $m = \frac{nr}{r}$  with usual notation.

2. If a 4 regular graph has 12 edges, find the number of vertices of the graph.

$$[\text{Ans. : } m = \frac{nr}{2} \quad \therefore n = \frac{2m}{r} = \frac{2 \times 12}{4} = 6]$$

3. Prove that there is no 5 regular graph with 7 vertices.

4. Find a regular graph of degree 3 other than  $K_4$  and  $K_{3,3}$ .

[Ans. : See adjoining figure. This is known as Peterson's graph.]

**(3) Bipartite Graph**

**Definition :** a graph  $G = (V, E)$  is called bipartite (= of two parts) if it satisfies the following conditions.

(i)  $V$  can be expressed as a union of two disjoint sets  $U$  and  $W$ .

(i.e.,  $U \cup W = V$  and  $U \cap W = \emptyset$ )

(ii) Every edge in  $E$  has one vertex in  $U$  and the other in  $W$ .

Also the sets  $U$  and  $W$  are called partitions of  $V$ .

**Example 1 :** Show that  $G = (V, E)$  where  $V = \{v_1, v_2, \dots, v_6\}$  and  $E = \{e_i\} e_i = \{v_i, v_j\}, i = 2, 3, \dots, 6$  is a bipartite graph.

**Sol.:** In this graph there are six vertices  $v_1, v_2, \dots, v_6$  and the vertex  $v_1$  is connected to every other vertex  $v_2, v_3, v_4, v_5, v_6$ . Thus, we get the Fig. 12.15 (a).

Now, let  $U = \{v_1\}$  and  $W = \{v_2, v_3, v_4, v_5, v_6\}$ .

Then  $V = U \cup W$  and  $U \cap W = \emptyset$ .

Further each vertex in  $U$  is joined with each vertex  $v_2, v_3, v_4, v_5, v_6$  in  $W$ . Hence, it is a bipartite graph.

The Fig. 12.15 (b) shows the partitions of this graph.

**Example 2 :** Show that the graph given in Fig. 12.16 (a) is bipartite.

**Sol.:** Let  $V = \{v_1, v_2, \dots, v_8\}$ .

Also let  $U = \{v_1, v_3, v_5, v_7\}$

and  $W = \{v_2, v_4, v_6, v_8\}$ .

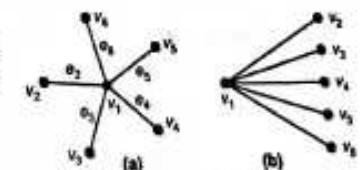


Fig. 12.15

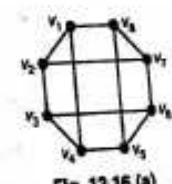


Fig. 12.16 (a)

Clearly,  $V = U \cup W$  and  $U \cap V = \emptyset$ .  
Further, every edge has one vertex in  $U$  and the other vertex in  $W$ . Hence, it is a bipartite graph. The Fig. 12.16 (b) below shows this fact clearly.

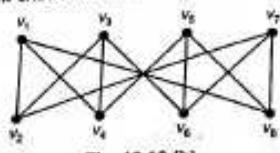


Fig. 12.16 (b)

**Example 3 :** If  $G$  is a simple, bipartite graph with  $m$  vertices and  $n$  edges show that  $m^2 \geq 4n$ .  
**Sol.:** Since  $G$  is a bipartite graph, let  $V = U \cup W$  be its partition. Let there be  $p$  vertices in  $U$  and  $q$  vertices in  $W$ , so that  $G$  has  $p+q$  vertices.

$$\therefore p+q = m$$

Since each vertex  $u$  in  $U$  can be connected to at the most  $q$  vertices in  $W$  as there are  $q$  vertices in  $W$  by our supposition. Hence, there are at the most  $pq$  edges in  $E$ .

$$\therefore n \leq pq$$

Now, from (1)

$$\begin{aligned} m^2 &= (p+q)^2 = (p-q)^2 + 4pq \\ &\geq 4pq \geq 4n \quad [\because (p-q)^2 \geq 0] \end{aligned}$$

**Example 4 :** Determine which of the following graphs are bipartite graphs. Find the partitions of the vertices if yes.

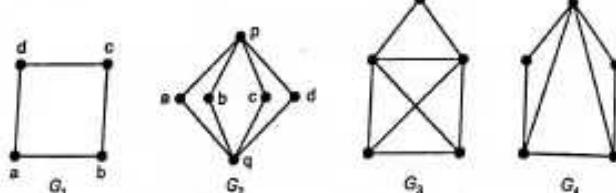


Fig. 12.17 (a)

**Sol. :** (i) In  $G_1$  there are four vertices where  $a$  and  $c$  (or  $b$  and  $d$ ) are not joined. Let  $U = \{a, c\}$ ,  $V = \{b, d\}$ . Then  $V = U \cup W$  and  $U \cap V = \emptyset$ .

$\therefore$  It is a bipartite graph.

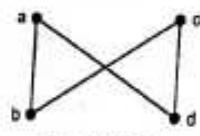


Fig. 12.17 (b)

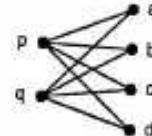


Fig. 12.17 (c)

(ii) In  $G_2$  there are 6 vertices and two are joined to the remaining four. We get the Fig. 12.17 (c).

Let  $U = \{p, q\}$ ,  $W = \{a, b, c, d\}$ . Then  $V = U \cup W$  and  $U \cap W = \emptyset$ .  
Further each vertex in  $U$  is joined with each vertex in  $W$ .  
Hence, it is a bipartite graph.

(iii)  $G_3$  is not a bipartite graph as the vertices cannot be partitioned as disjoint sets. Further in  $G_3$  there are  $m = 6$  vertices and  $n = 8$  edges and  $m^2 \geq 2n$ .

(iv)  $G_4$  is not a bipartite graph as the vertices cannot be partitioned in disjoint sets. Further, note that in  $G_4$  there are  $m = 5$  vertices and  $n = 7$  edges. Now,  $m^2 = 25$  and  $2n = 28$ ,  $m^2 \geq 4n$ .

**Example 5 :** Show that there is not bipartite graph with 6 vertices and 10 edges.  
**Sol.:** Such a graph cannot be drawn. Further for this graph  $m = 6$  and  $n = 10$  and  $m^2 \geq 4n$ .

**Example 6 :** Show that a bipartite graph has no loops.

**Sol.:** Let  $U$  and  $W$  be the two sets of vertices of the given bipartite graph such that  $V = U \cup W$  and  $U \cap W = \emptyset$  where  $V$  is the set of vertices of the given bipartite graph.

Now, suppose  $e = (v, v)$  is a loop. Hence,  $v \in U$  and  $v \in W$ .

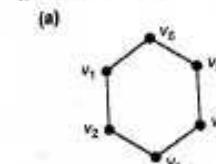
$$\therefore v \in U \cap W.$$

But by definition  $U \cap W = \emptyset$ . This is a contradiction.

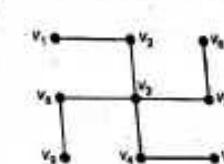
$\therefore$  A bipartite graph has no loops.

### EXERCISE - III

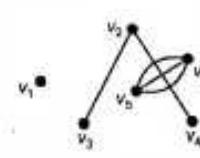
1. Show that the following are bipartite graphs. Draw the graphs again showing the partitions.



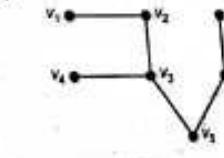
(a)



(b)

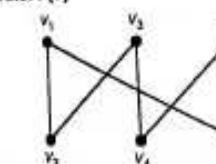


(c)



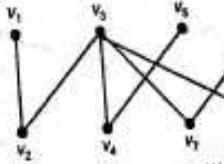
(d)

[Ans. : (a)

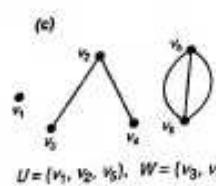


$$U = \{v_1, v_3, v_5\}, \quad W = \{v_2, v_4, v_6\}$$

(b)



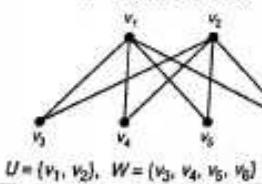
$$U = \{v_1, v_3, v_5\}, \quad W = \{v_2, v_4, v_6\}$$



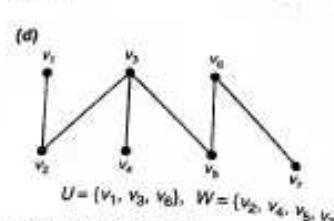
2. Show that there is no bipartite graph with six vertices and ten edges.

3. Construct some bipartite graphs on six vertices. Showing the partitions.

$$U = \{v_1\}, \\ W = \{v_2, v_3, v_4, v_5, v_6\}$$



(12.11)



#### (4) Complete Bipartite Graph

Definition :  $G = (V, E)$  is called complete bipartite graph if

- (1)  $G$  is bipartite, (2)  $G$  is simple, (3) If  $V = U \cup W$

is the partition of  $V$  then every vertex  $u_i$  in  $U$  is joined to every vertex  $w_j$  in  $W$ . In other words there is an edge between every vertex in  $U$  and every vertex in  $W$ .

If  $U$  has  $m$  vertices and  $W$  has  $n$  vertices, then the complete bipartite graph is denoted by  $K_{m,n}$ .

Since each of the  $m$  vertices in  $U$  is adjacent (joined) to each of the  $n$  vertices in  $W$ , there will be  $mn$  edges in  $K_{m,n}$ . For standardisation we assume that  $m \leq n$  in  $K_{m,n}$ .

#### Notes ....

1. Since a complete bipartite graph is simple it has no loops and no multiple edges.
  2. If  $u \in U$  and  $w \in W$  then there is only one edge between  $u$  and  $w$ ,  $e = (u, w) \in E$ .
- The following are complete bipartite graphs. The graph  $K_{1,n}$  is called star.

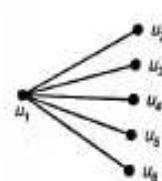
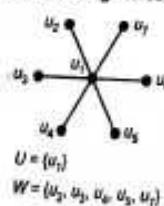


Fig. 12.18 (a)

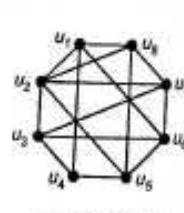


Fig. 12.18 (c)

(12.12)

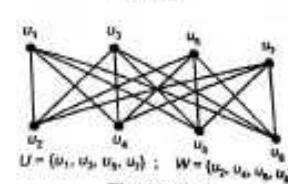


Fig. 12.18 (d)

Clearly  $K_{mn} = K_{nm}$ . The first graph in (2) is a complete bipartite graph  $K_{1,5}$ .

Observe the following complete bipartite graphs.

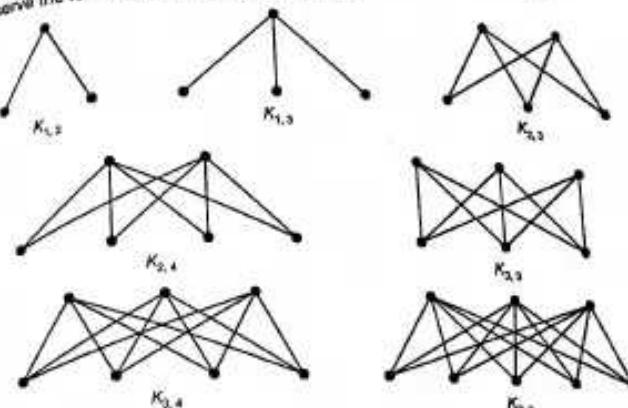


Fig. 12.19

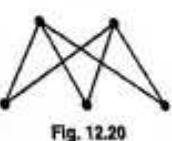


Fig. 12.20

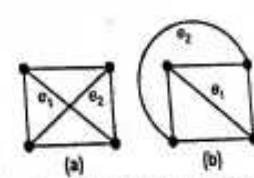
(M.U. 2007, 12, 13)

#### (5) Planar and Plane Graphs

Definition : If it is possible to draw the diagram of a given graph in such a way that no two edges intersect (except at a vertex) it is called a planar graph.

Definition : The diagram of a graph drawn in such a way that no two edges intersect is called a plane graph.

For example, the graph shown in the Fig. 12.21 (a) is a planar graph because (although the two edges  $e_1$  and  $e_2$  cross each other) it is possible to redraw the graph in such a way that the edges  $e_1$  and  $e_2$  do not cross as shown in the Fig. 12.21 (b) which is a plane graph.

Fig. 12.21 : (a) Planar Graph,  
(b) Plane Graph.

The graphs shown in Fig. 12.22 (a) and (b) below are plane graphs.

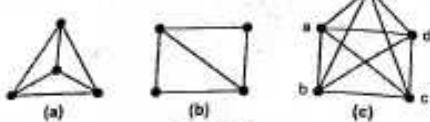


Fig. 12.22

The graph shown in Fig. 12.23 (a) is a planar graph as it can be redrawn as in Fig. 12.23 (b) which is a plane graph.

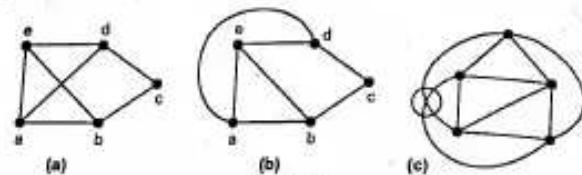


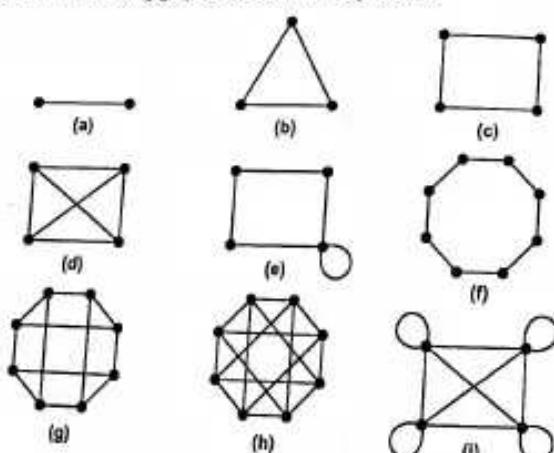
Fig. 12.23

But the graph  $G$  shown in Fig. 12.22 (c) is not a planar graph as it cannot be drawn without intersecting edges as shown in Fig. 12.23 (c).

We shall study planar graphs in details in Chapter 16.

#### EXERCISE - IV

Carefully observe the following graphs and answer the questions.



1. Which are planar graphs?

2. Which are simple graphs?

3. Which are regular graphs?

5. Which are complete graphs?

| Ans. : (1) All are planar graphs. (2) Except (a) and (i) all are simple. (3) Except (a) all are regular. (4) (a), (i), (g), (h) are bipartite. (5) (a), (b), (d), (h) are complete. (6) (a), (h) are complete bipartite. |

4. Which are bipartite graph?

6. Which are complete bipartite graphs?

Graphs

#### 5. Isomorphism

Consider diagrams  $G_1$  and  $G_2$ .

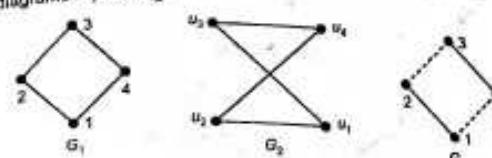


Fig. 12.24

Do they represent the same graph? If we change the names of vertices in  $G_2$  as  $u_1 \rightarrow 2$ ,  $u_2 \rightarrow 1$ ,  $u_3 \rightarrow 3$ ,  $u_4 \rightarrow 4$ , then we see that the second diagram can be redrawn to get the first diagram. Imagine that you "lift" the vertex  $u_1$  and put it on the left. Essentially the two graphs are the 'same' although they 'look' different. Such graphs are called Isomorphic, (Iso = same, morph = form).

**Definition :** Two graphs  $G = (V, E)$  and  $G' = (V', E')$  are said to be Isomorphic, if there exists a one-to-one correspondence  $f$  from  $V$  to  $V'$  such that if  $v_1, v_2 \in V$  and  $v'_1, v'_2 \in V'$  and  $f(v_1) = v'_1$ ,  $f(v_2) = v'_2$  then the number of edges between  $v_1, v_2$  is the same as the number of edges between  $v'_1$  and  $v'_2$ . The function  $f$  is called an Isomorphism between  $G$  and  $G'$ . If  $G$  and  $G'$  are isomorphic we write  $G \cong G'$ .

(M.U. 2000, 01, 09, 14)

#### Notes ...

- If  $f$  is an isomorphism between  $G$  and  $G'$  then  $f^{-1}$  is also an isomorphism.
- If  $G$  is isomorphic to  $G'$  and  $G'$  is isomorphic to  $G''$  then  $G$  is isomorphic to  $G''$ .
- If  $v_1, v_2 \in V$  are adjacent then  $v'_1, v'_2 \in V'$  are also adjacent.
- If  $e = \{v_1, v_1\}$  is a loop, then  $e' = \{v'_1, v'_1\}$  is also a loop.
- If  $e_1 = \{v_1, v_2\}$  and  $e_2 = \{v_2, v_3\}$  are two adjacent edges i.e.  $e_1, e_2$  are two edges incident at a common vertex  $v_2$  then  $e'_1 = \{v'_1, v'_2\}$  and  $e'_2 = \{v'_2, v'_3\}$  are also adjacent edges.
- If  $e_1 = \{v_1, v_2\}$ ,  $e_2 = \{v_1, v_2\}$  are parallel edges then  $e'_1 = \{v'_1, v'_2\}$ ,  $e'_2 = \{v'_1, v'_2\}$  are also parallel edges. In other words if  $G$  is a multigraph then  $G'$  is also a multigraph.
- $d(v) = d(v')$  for all  $v \in V$  i.e. degree of vertex  $v$  is equal to the degree of vertex  $v'$  under  $f$ .

It is not always easy to determine whether two graphs are isomorphic.

If two graphs are isomorphic then,

1. They must have the same number of vertices,

2. They must have the same number of edges,

3. They must have the same degrees of vertices.

If one of the above conditions is not satisfied then the graphs are not isomorphic.

Graphs may satisfy all the above three conditions and yet they may not be isomorphic, for example, see the Ex. 1 (a) below.

4. It may be noted that in addition to the above three conditions 'adjacency' also is an important condition.

**Example 1 :** Determine whether the following pairs of graph are isomorphic.

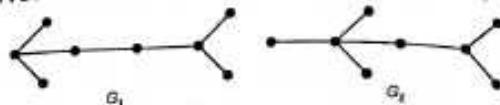


Fig. 12.25 (a)

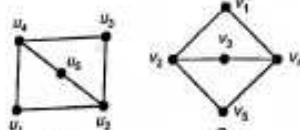


Fig. 12.25 (b)

**Sol. :** (a) The two graphs  $G_1, G_2$  have eight vertices and seven edges. However, in the first graph  $G_1$ , there are four vertices of degree one and in the second graph  $G_2$ , there are five vertices of degree one.

Hence, the two graphs are not isomorphic.

(b) The two graphs  $G_1, G_2$  have five vertices and six edges each. Further, in both the graphs there are three vertices of degree two and two vertices of degree three.

We can define one-to-one correspondence  $f$  as follows :

$$u_1 \rightarrow v_5, u_2 \rightarrow v_4, u_3 \rightarrow v_1, u_4 \rightarrow v_2, u_5 \rightarrow v_3.$$

This correspondence preserves the adjacency and incidence relationship.

∴ The graphs are isomorphic.

#### Note ...

$G_2$  can be obtained by just turning  $G_1$  through  $125^\circ$ .

**Example 2 :** Draw all non-isomorphic graphs of (i) 2 vertices, (ii) 3 vertices and state reasons.

**Sol. :** (i) All non-isomorphic graphs will have two vertices are



Fig. 12.26 (a)

(ii) All non-isomorphic graphs with three vertices are

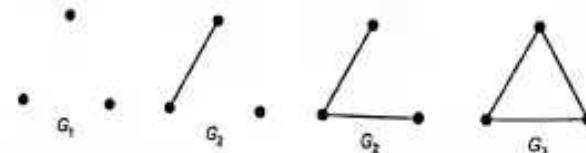


Fig. 12.26 (b)

**Example 3 :** Find all non-isomorphic connected graphs with four vertices and state reasons.

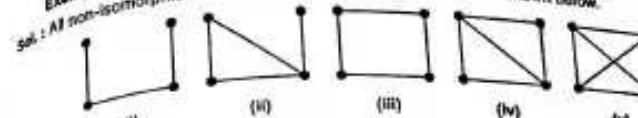


Fig. 12.27

**Example 4 :** Are the following pairs of graphs isomorphic? Give reasons?

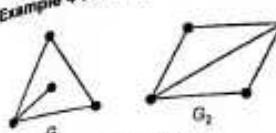


Fig. 12.28 (a)

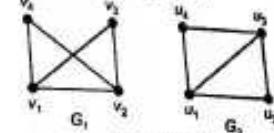


Fig. 12.28 (b)

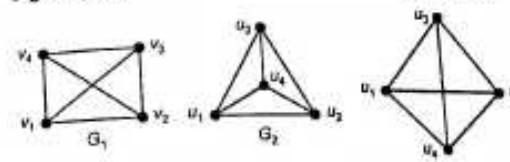


Fig. 12.28 (c)

**Sol. :** (a) No. Although  $G_1$  and  $G_2$  have 4 vertices both;  $G_1$  has 4 edges and  $G_2$  has 5 edges;  $G_1$  has a pendant vertex,  $G_2$  has not.  $G_1$  has only one vertex with 3 edges while  $G_2$  has two vertices with 3 edges.

(b) Yes.  $G_1$  and  $G_2$  both have 4 vertices; 5 edges; 2 vertices of degree 2 and 2 vertices of degree 3. The correspondence is obtained by lifting  $v_3$  and placing it below  $v_2$ . [ See Fig. 12.28 (d) ]

$$\therefore v_1 \rightarrow u_1, v_3 \rightarrow u_2, v_2 \rightarrow u_3, v_4 \rightarrow u.$$

(c) Yes.  $G_1$  and  $G_2$  both have 4 vertices 4 edges. Each vertex in  $G_1$  and  $G_2$  is of degree 3. The correspondence is obtained if  $u_4$  is pulled down and the figure is rotated through  $45^\circ$ . [ See Fig. 12.28 (e) ]

$$\therefore v_1 \rightarrow u_1, v_2 \rightarrow u_4, v_3 \rightarrow u_2, v_4 \rightarrow u_3.$$

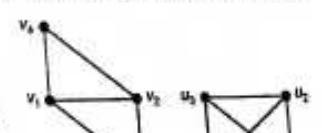


Fig. 12.28 (d)

Fig. 12.28 (e)

**Example 5 :** Are the graphs shown in the Fig. 12.29 isomorphic? Give reasons.

**Sol. :** Yes. Both  $G$  and  $G'$  have 6 vertices and 9 edges. Each vertex in  $G$  and  $G'$  is of degree 3. The correspondence is obtained if  $G$  is rotated through  $45^\circ$  (in anticlockwise direction) and  $d$  and  $a$  are interchanged by pushing  $a$  up and pulling  $d$  down.

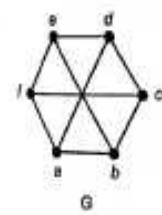


Fig. 12.29

$\Delta$ :  $a \rightarrow u, b \rightarrow v, c \rightarrow w, f \rightarrow p, d \rightarrow q, b \rightarrow r$ .

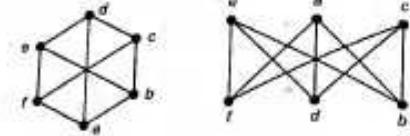


Fig. 12.29 (a)

**Example 6:** Find whether the following graphs  $G = (V, E)$  and  $G^* = (V^*, E^*)$  are isomorphic giving reasons.

- (i)  $V = \{a, b, c, d\}$ ,  $E = \{(a, b), (a, d), (b, d), (c, d), (c, b), (c, d)\}$
- (ii)  $V^* = \{1, 2, 3, 4\}$ ,  $E^* = \{(1, 2), (2, 3), (3, 1), (3, 4), (4, 1), (4, 2)\}$

**Sol.:** (i) We shall first draw the diagrams of these graphs which are given in set notation. In  $E$  the edge  $(c, d)$  occurs twice, indicating that there are two edges between  $c$  and  $d$ .

(ii) No. Both graphs  $G$  and  $G^*$  have 4 vertices and 6 edges. But the degree of vertex  $a$  in  $G$  is 2 and there is no vertex of degree 2 in  $G^*$ . Also in  $G$  the degree of vertex  $d$  is 4, but there is no vertex of degree 4 in  $G^*$ .

**Example 7:** Find whether the graphs shown in Fig. 12.31 are isomorphic. (M.U. 2000, 14, 15)

**Sol.:** We first note that both the graphs have

1. five vertices
2. eight edges

In  $G_1$  there is one vertex  $v_5$  of degree 4 and the remaining vertices are of degree 3.

In  $G_2$ , there is one vertex  $u_4$  of degree 4 and the remaining are of degree 3.

Further, the adjacency property is observed. The vertex with degree 4 is adjacent to the remaining vertices in both the graphs.

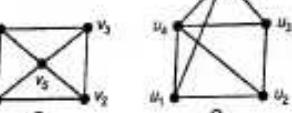


Fig. 12.31

Hence, the two graphs are isomorphic.

If you pull  $u_4$  inside and  $u_5$  to the position of  $u_4$ , you will get  $G_1$ .

The correspondence is

$$v_1 \rightarrow u_1, v_2 \rightarrow u_2, v_3 \rightarrow u_3, v_4 \rightarrow u_5 \text{ and } v_5 \rightarrow u_4.$$

**Example 8:** Determine whether the following graphs are isomorphic. (M.U. 2002, 17)

**Sol.:** There are 8 vertices in  $G_1$  and 8 vertices in  $G_2$ .

Further there are four vertices of degree 3 in  $G_1$  and four vertices of degree 3 in  $G_2$ . There are four vertices of degree 2 in  $G_1$  and there are four vertices of degree 2 in  $G_2$ .

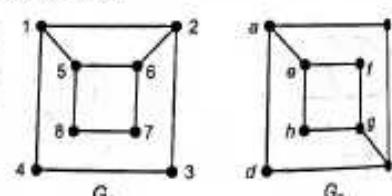


Fig. 12.32

But if  $5 \rightarrow a$  and  $6 \rightarrow g$  then although 5 and 6 are adjacent,  $a$  and  $g$  are not adjacent [See (4), page 12-15]. Thus adjacency is not preserved. Similarly, if  $1 \rightarrow a$  and  $2 \rightarrow c$  although 1 and 2 are adjacent but  $a$  and  $c$  are not adjacent. Thus, we see that the adjacency is not preserved.

The graphs are not isomorphic.

**Example 9:** Determine whether the graphs  $G_1$  and  $G_2$  are isomorphic or not. Justify your answer. (M.U. 2008)

**Sol.:** We first note the following.

1. Both the graphs have the same number of vertices viz. 8 and the same number of edges 10.
2. In  $G_1$  there are four vertices with degree 3 and in  $G_2$  also there are four vertices with degree 3.
3. But adjacency is not preserved in the two graphs. In  $G_1$  vertex with 3 edges is adjacent to only one vertex with 3 edges ( $f$  and  $b$  or  $d$  and  $h$ ). But in  $G_2$  a vertex with 3 edges is adjacent to two vertices with edges 3 ( $p$  to  $w$  and  $s$ ;  $w$  to  $p$  and  $t$  and so on). Thus, adjacency is not preserved.
4. Hence  $G_1$  and  $G_2$  as above are not isomorphic.

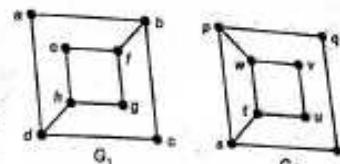


Fig. 12.33

**Example 10:** Show that the graphs shown in the Fig. 12.34 are isomorphic. (M.U. 1998, 2000, 13)

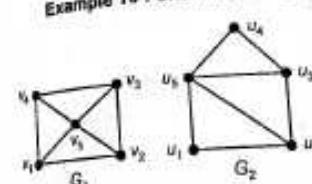


Fig. 12.34

**Sol.:** We first see that the two graphs have the same number of vertices (5) and the same number of edges (8).

In  $G_1$  there are 4 vertices of degree 3 and one vertex of degree 4. In  $G_2$  also there are 4 vertices of degree 3 and one vertex of degree 4.

Consider the correspondence

$$v_1 \rightarrow u_1, v_2 \rightarrow u_2, v_3 \rightarrow u_3, v_4 \rightarrow u_4 \text{ and } v_5 \rightarrow u_5.$$

(If we pull  $u_5$  towards  $u_2$ , so that  $u_4$  becomes the vertex of the rectangle  $G_2$  will look like  $G_1$ .)

Hence,  $G_1$  and  $G_2$  are isomorphic.

**Example 11:** Determine whether the following graphs are isomorphic or not. (M.U. 2005, 07)

**Sol.:** We first see that both the graphs have the same number of vertices (6) and the same number of edges (9).

In  $G_1$  all the vertices are of degree 3 and in  $G_2$  also all the vertices are of degree 3.

Consider the correspondence  $v_1 \rightarrow u_1, v_2 \rightarrow u_2, v_3 \rightarrow u_3, v_4 \rightarrow u_4, v_5 \rightarrow u_5, v_6 \rightarrow u_6$ .

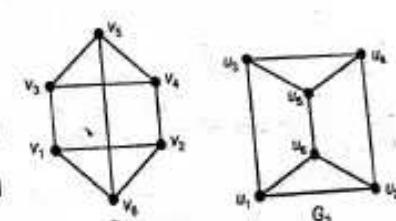


Fig. 12.35

(If we press the edge  $(v_1, v_2)$  in  $G_1$  and bring it within the rectangle after making it short, we get the graph  $G_2$ )  
Hence,  $G_1$  and  $G_2$  are isomorphic.

**Example 12 :** Show that the two graphs shown in the Fig. 12.36 are isomorphic. (M.U. 2001, 13, 14)

**Sol. :** We first see that the two graphs have the same number of vertices (5) and the same number of edges (7).

In  $G_1$  there are 4 vertices of degree 3 and one vertex of degree 2. In  $G_2$  also there are 4 vertices of degree 3 and one vertex of degree 2.

Consider the correspondence  $a \rightarrow 1, b \rightarrow 2, c \rightarrow 3, d \rightarrow 4, e \rightarrow 5$ .

(If we rotate  $G_2$  keeping the vertex 1 fixed, in clockwise direction such that the edge  $(1, 3)$  becomes horizontal, then  $G_2$  will look like  $G_1$ .)

Hence,  $G_1, G_2$  are isomorphic.

**Example 13 :** Show that the graphs shown in the Fig. 12.37 are not isomorphic. (M.U. 2005)

**Sol. :** Both the graphs have 5 vertices. Both the graphs have 6 edges.

But in graph  $G_2$  there is one vertex  $a'$  with degree 4 and one vertex  $e'$  with degree 1.

There is no vertex with degree 4 and no vertex with degree 1 in  $G_1$ .

∴ The graphs are not isomorphic.

**Example 14 :** Determine whether the pair of graphs (Fig. 12.38) is isomorphic or not. (M.U. 2012)

**Sol. :** We first note that both the graphs have

1. same number of vertices viz. 6
2. same number of edges viz. 9.

In  $G$ , there are two vertices  $a, f$  of degree 2, two vertices  $c$  and  $d$  of degree 3, two vertices  $b$  and  $e$  of degree 4.

In  $G'$ , also there are two vertices  $b'$  and  $e'$  of degree 2, two vertices  $a'$  and  $d'$  of degree 3, two vertices  $c'$  and  $f'$  of degree 4.

Yet the two graphs are not isomorphic because the property of adjacency is not observed.

In  $G$ , one vertex  $e$  (and also  $f$ ) of degree 2 is adjacent to two vertices  $d$  and  $b$  of degree 4.

In  $G'$ , one vertex  $b'$  (and also  $e'$ ) of degree 2 is adjacent to the vertex  $c'$  with degree 4 but to  $a'$  with degree 3.

Hence, the graphs are not isomorphic.

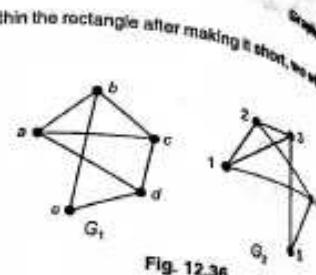


Fig. 12.36

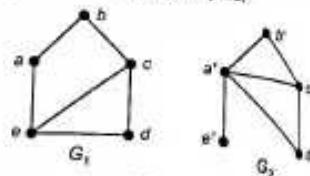


Fig. 12.37

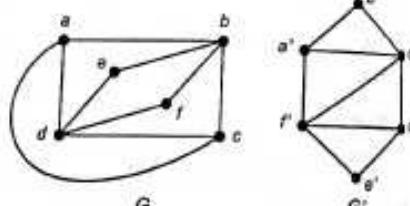


Fig. 12.38

**Example 15 :** Find whether the following graphs (Fig. 12.39) are isomorphic. (M.U. 2005)

**Sol. :** We first note that both the graphs  $G$  and  $G'$  have  
 (i) the same number of vertices viz. 6  
 (ii) the same number of edges viz. 6  
 (iii) each vertex in  $G$  and  $G'$  is of degree 2.

Hence, the two graphs are isomorphic.  
 $G$  can be obtained from  $G'$  by "pulling" the vertex  $d'$  up above the vertices  $c'$  and  $e'$ .

(M.U. 2005)

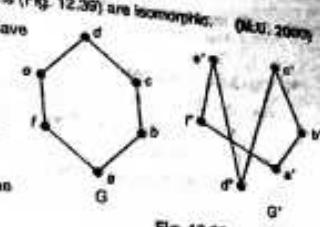


Fig. 12.39

**Example 16 :** Determine whether the following graphs are isomorphic. (M.U. 2003, 10, 11)

**Sol. :** We first note that  $G$  and  $G'$  have  
 (i) the same number of vertices viz. 6  
 (ii) but they do not have the same number of edges.  $G$  has 8 edges while  $G'$  has 9 edges.  
 (iii) In  $G'$  the vertex  $c'$  (and also  $f'$ ) is of degree 4, while in  $G$  there is no vertex of degree 4.  
 Hence,  $G$  and  $G'$  are not isomorphic.

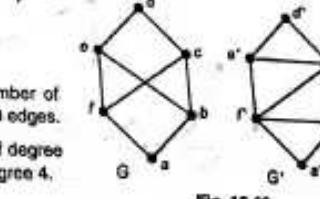


Fig. 12.40

**Example 17 :** Determine whether the following graphs [Fig. 12.41 (a) and (b)] are isomorphic. (M.U. 2004)

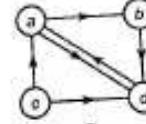


Fig. 12.41 (a)

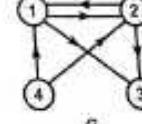


Fig. 12.41 (b)

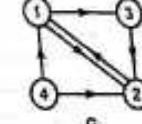


Fig. 12.41 (c)

**Sol. :** We first observe that

- (i)  $G_1$  and  $G_2$  have the same number of vertices, 4.
- (ii)  $G_1$  and  $G_2$  have the same number of edges, 6.
- (iii) Both  $G_1$  and  $G_2$  have two vertices of degree 4 and two vertices of degree 2.  
 If we interchange the positions of (2) and (3) in  $G_2$ , we get  $G_3$  as shown in the Fig. 12.41 (c).  
 Hence, the graphs are isomorphic.

**Example 18 :** Determine whether the graphs (Fig. 12.42) are isomorphic. (M.U. 2015)

**Sol. :** We first note that  $G$  and  $G'$  have

- (i) the same number of vertices (7)
- (ii) the same number of edges (9)

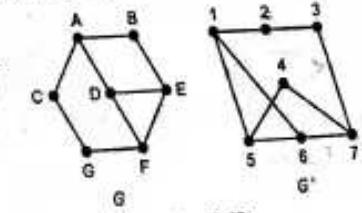


Fig. 12.42

(ii) three vertices of degree two ( $G$  has  $B, C, G$ ;  $G'$  has 2, 3, 4)  
four vertices of degree three ( $G$  has  $A, D, E, F$ ;  $G'$  has 1, 5, 6, 7).

Also adjacency is preserved.

We can define one-to-one correspondence as follows:

$$A \rightarrow 1, B \rightarrow 2, C \rightarrow 3, D \rightarrow 6, E \rightarrow 5, F \rightarrow 7, G \rightarrow 4.$$

[See Fig. 12.42 (a)]

Hence, the graphs are isomorphic.

**Example 19 :** Discuss whether the following graphs are isomorphic.

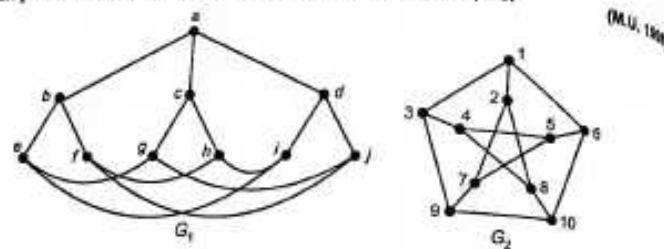


Fig. 12.43

**Sol. :** We first see that both the graphs have the same number of vertices (10) and the same number of edges (15).

In both the graphs all the 10 vertices are of degree 3.

Also the adjacency is preserved.

Consider the correspondence

$$a \rightarrow 1, b \rightarrow 2, c \rightarrow 3, d \rightarrow 4, e \rightarrow 5, f \rightarrow 6, g \rightarrow 7, h \rightarrow 8, i \rightarrow 9, j \rightarrow 10.$$

Hence, the two graphs are isomorphic.

**Example 20 :** Show that the graphs shown in the Fig. 12.44 are isomorphic. Also find the isomorphism.

**Sol. :** Both graphs have 4 vertices and 6 edges.

Each graph has 2 vertices of degree 2 and 2 vertices of degree 4. Also the adjacency is preserved.

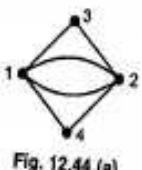


Fig. 12.44 (a)

Since all the four conditions are satisfied, the two graphs are isomorphic.

The correspondence is  $a \rightarrow 1, c \rightarrow 2, b \rightarrow 3, d \rightarrow 4$ .

If we shift the vertex 3 and place it above 1 and 2, we get the Fig. 12.44 (b).

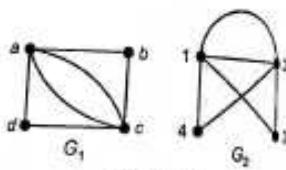


Fig. 12.44

**Example 21 :** Determine whether the adjoining graphs (Fig. 12.45) are isomorphic. (M.U. 2015)

**Sol. :** Both graphs have 5 vertices. Both graphs have 5 edges. The degree of each vertex is 2.

Also adjacency is preserved.

Hence, the both graphs are isomorphic.

Lift the side  $e' c'$ , turn it through  $180^\circ$  and place it below the points  $a', b'$ , such that  $c'$  is below  $a'$  and  $e'$  is below  $b'$ .

The correspondence is  $a \rightarrow c', b \rightarrow e', c \rightarrow b', d \rightarrow d', e \rightarrow a'$ .

**Example 22 :** Determine whether the following graphs are isomorphic. (M.U. 2017)

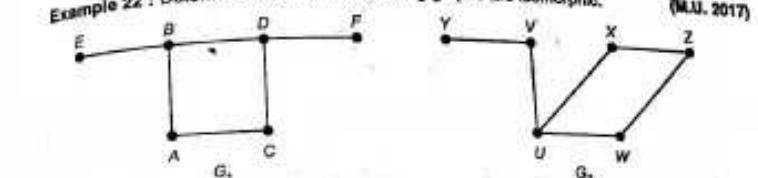


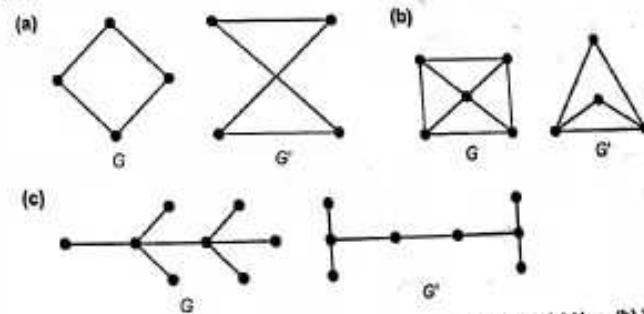
Fig. 12.46

**Sol. :** Both the graphs have 6 vertices and 6 edges.

But in  $G_1$ , there are two vertices of degree 1 and in  $G_2$ , there is only one vertex of degree 1. In  $G_1$ , there are two vertices of degree 3 and in  $G_2$ , there is only one vertex of degree 3. Hence, the graphs are not isomorphic.

**EXERCISE - V**

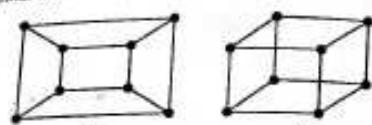
1. Determine whether the following pairs of graphs  $G$  and  $G'$  are isomorphic. Give reasons.



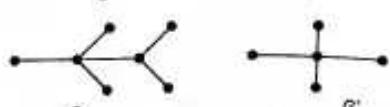
[Ans. : (a) Yes, (b) Yes, (c) No.]

2. Determine whether the following pairs of graphs are isomorphic. Give reasons.

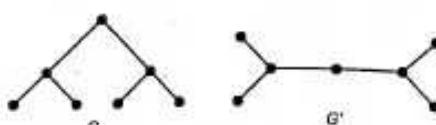
(a)



(b)

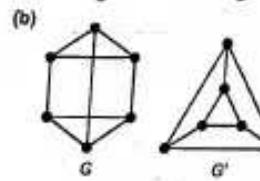
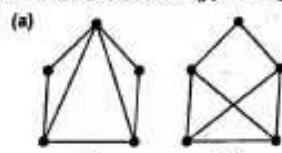


(c)



[Ans. : (a) Yes, (b) No, (c) Yes.]

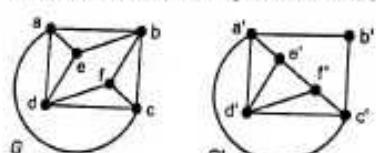
3. Find whether the following pairs of graphs are isomorphic. Give reasons.



[Ans. : (a) No, (b) Yes, (c) Yes.]

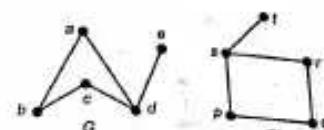
4. Find whether the following graphs are isomorphic. Give reasons.

(i)



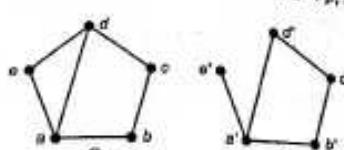
[Ans. : No. In G', b' is of degree 2 while G has no vertex of degree 2.]

(ii)



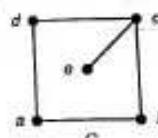
[Ans. : Yes. a → p, b → q, c → r, d → s, e → t.]

(iii)



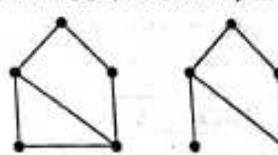
[Ans. : No. In G', a' is a pendant.]

5. Determine whether the following graphs are isomorphic. Give reasons.



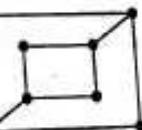
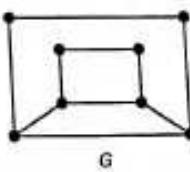
[Ans. : No. In G, there is only one vertex of degree 3, while in G', there are 3 vertices of degree 3.]

6. Determine whether the following graphs are isomorphic. Give reasons.



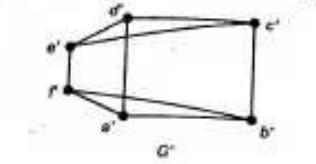
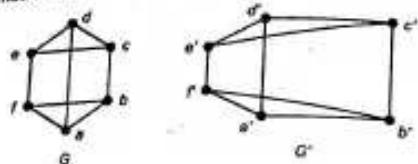
[Ans. : No. G' has a pendant while G has no pendant.]

7. Determine whether the following graphs are isomorphic. Give reasons.



[Ans. : No. Adjacency is not preserved.]

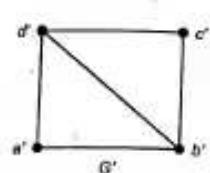
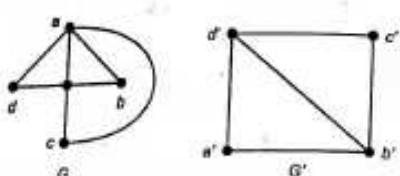
8. Determine whether the following graphs are isomorphic. Give reasons.



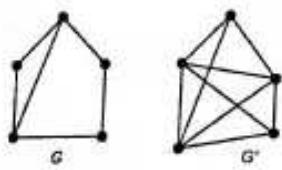
[Ans.: Yes. Bring  $a', f'$  inside the square and then stretch it on both sides.]

10. Determine whether the following pairs of graphs are isomorphic. Give reasons.

(a)



(b)



[Ans.: (a) No.  $G$  has a vertex of degree 4 but  $G'$  does not have such a vertex.

(b) No.  $G'$  has 3 vertices of degree 4.]

### EXERCISE - VI

#### Theory

1. Define the following terms giving illustrations.

- |                       |                    |                   |
|-----------------------|--------------------|-------------------|
| 1. Graph (M.U. 1998)  | 2. Loop            | 3. Multigraph     |
| 4. Adjacent Vertices  | 5. Incident Edge   | 6. Adjacent Edges |
| 7. Degree Of A vertex | 8. Isolated Vertex | 9. Pendant.       |

10. Length Of A Graph.

2. Define the following terms giving illustrations.

- |                                |   |                  |
|--------------------------------|---|------------------|
| 1. Simple Graph                | 2. Complete Graph                       | 3. Regular Graph |
| 4. Bipartite Graph (M.U. 2010) | 5. Complete Bipartite Graph (M.U. 2010) |                  |
| 6. Planar Graph.               |   |                  |

3. Define and illustrate Isomorphism of two graphs.

(M.U. 2000, 01, 05)

4. State and prove "Hand Shaking Lemma".

5. Prove that the sum of the degrees of all vertices of a graph is equal to twice the number of edges.

6. Prove that in any graph the number of vertices of odd degree is even.

7. Prove that the total number of edges in a complete graph  $K_n$  is  $n(n-1)/2$  and the degree of each vertex is  $n-1$ .

8. Explain whether  $K_4$  is a plane graph.

Graphs



## CHAPTER 13

# Eulerian and Hamiltonian Graphs

### 1. Introduction

We shall start this chapter with the famous seven bridge problem. The problem is this,

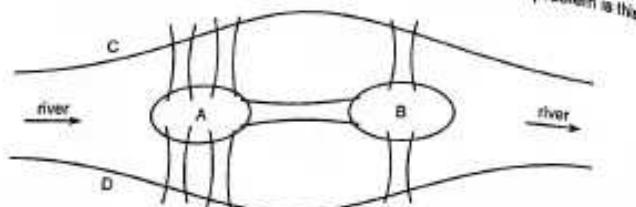


Fig. 13.1

A and B are two islands in a river and C and D are the banks of the river. There are seven bridges on the river connecting the islands and the banks as shown in the figure. The problem is: can anybody starting from any spot on land cross all bridges only once and come back to the same spot? (There were such seven bridges on the river Pregel in Königsberg in Germany before the world war II. The bridges were destroyed in the war and the name of the city also was changed to Kaliningrad after Russians occupied it.)

Euler thought of the land masses as vertices and bridges as edges and answered the above question (in the negative). Thus, graph theory was born.

The seven bridge problem can be stated in a mathematical form as :- Given the graph shown in Fig. 13.2, can we start at any one of the vertices A, B, C, D traverse all the edges exactly once and come back to the same vertex?

In this chapter we are going to study Eulerian Graphs and ideas developed by Euler. Also we shall study related graphs viz. Hamiltonian graphs.

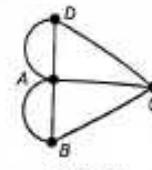


Fig. 13.2

### 2. Definitions

#### (a) Path

**Definition :** An alternating sequence of vertices and edges in a graph in which neither a vertex nor an edge is repeated is called a path.

#### Applied Mathematics - IV

(13-2)

In the graph  $G_1$  shown in the Fig. 13.3,  
We have a path  $\pi_1 : a e_1 b e_2 c$   
We have a path  $\pi_2 : b e_2 c e_3 d e_4 a$   
We have another path  $\pi_3 : a e_1 b e_2 c e_3 d e_4 a$

#### (b) Length of a path

**Definition :** The number of edges in a path is called the length of a path.  
The length of the path  $\pi_1$  is 2.  
The length of the path  $\pi_2$  is 3.  
The length of the path  $\pi_3$  is 4.

#### (c) Connected Graphs

**Definition :** A graph is said to be connected if there is a path from any vertex to any other vertex.  
If a graph is not connected, then it is called disconnected. This means in a disconnected graph, there is atleast one pair of vertices without any path between them.

Of the following graphs shown in the Fig. 13.4 (a) and (b) are connected while graphs shown in the Fig. 13.4 (c) and (d) are disconnected graphs.

#### Eulerian & Hamiltonian Graphs

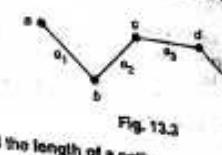


Fig. 13.3

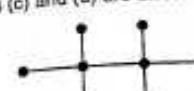


Fig. 13.4 (a)

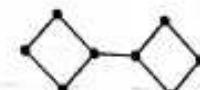


Fig. 13.4 (b)



Fig. 13.4 (c)

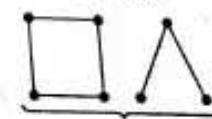


Fig. 13.4 (d)

#### (d) Circuit

**Definition :** A path that begins and ends at the same vertex is called a circuit. Since a circuit is a path, in a circuit neither a vertex nor an edge is repeated. (Except the beginning vertex.)

In the neighbouring Fig. 13.5 (a), a  $e_1 b e_2 c e_3 d e_4 a$  is a circuit ; a  $e_4 d e_3 c e_5 a$  is another circuit ; a  $e_5 c e_2 b e_1 a$  is another circuit.

#### (e) Eulerian Path

**Definition :** A path in a graph is called Eulerian Path if it includes all edges but each edge exactly ones a vertex may be repeated.

In the Fig. 13.5 (b), the path  $\pi_1 : a e_1 b e_2 c e_3 d$  is an Eulerian path because it contains all the edges of the graph and no edge is repeated.



Fig. 13.5



Fig. 13.5

(M.U. 2001, 02, 10, 11, 12, 16)

(13-3)

- (a) Eulerian Circuit  
Definition : An Eulerian path that is a circuit is called Eulerian Circuit.  
In other words, a circuit that contains all edges but each edge exactly once is called an Eulerian Circuit.

Eulerian Graph : A graph that contains an Eulerian circuit is called Eulerian Graph.

In Fig. 13.6 (a), there is an Eulerian circuit  $a \rightarrow e_1 \rightarrow b \rightarrow e_2 \rightarrow c \rightarrow e_3 \rightarrow d \rightarrow e_4 \rightarrow a$  and hence it is an Eulerian Graph.

In Fig. 13.6 (b),  $b \rightarrow e_2 \rightarrow c \rightarrow e_3 \rightarrow d \rightarrow e_4 \rightarrow e_5 \rightarrow b$  is a circuit but it is not Eulerian Circuit as it does not contain all edges of the graph.

Now, study the following table carefully.

	Repeated Vertex	Repeated Edge
Path	No	No
Circuit	No	No
Eulerian Path	Allowed	No
Eulerian Circuit	Allowed	No

#### Distinction between a Circuit and Eulerian Circuit

In the graph shown in Fig. 13.7,  $a \rightarrow e_1 \rightarrow b \rightarrow e_2 \rightarrow c \rightarrow e_3 \rightarrow a$  is a circuit but not an Eulerian circuit because it does not contain all the edges of the graph (e.g.,  $e_4$  and  $e_5$ ).

In the same graph,  $a \rightarrow e_1 \rightarrow b \rightarrow e_5 \rightarrow e_6 \rightarrow e_4 \rightarrow b \rightarrow e_2 \rightarrow c \rightarrow e_3 \rightarrow a$  is a circuit but not an Eulerian circuit because although it contains all the edges, some edges are repeated. The edge  $e_1$  is repeated.

But  $a \rightarrow e_1 \rightarrow b \rightarrow e_5 \rightarrow e_6 \rightarrow e_4 \rightarrow b \rightarrow e_2 \rightarrow c \rightarrow e_3 \rightarrow a$  is an Eulerian circuit because it contains all edges and only once though vertices are repeated.



Fig. 13.8

Example 1 : The graph given in the Fig. 13.8 is an Eulerian graph. (M.U. 2003)

Sol. : As seen above, the circuit  $v_1 \rightarrow e_1 \rightarrow v_2 \rightarrow e_2 \rightarrow v_3 \rightarrow e_3 \rightarrow v_4 \rightarrow e_4 \rightarrow v_5 \rightarrow e_5 \rightarrow v_3 \rightarrow e_6 \rightarrow v_1$  is the Eulerian circuit. Note that the Eulerian circuit contains all edges exactly once, but it may contain vertices more than once (e.g.  $v_3$ ).

Example 2 : The graph given in Fig. 13.9 is an Eulerian graph.

Sol. : The circuit  $v_1 \rightarrow e_1 \rightarrow v_4 \rightarrow e_7 \rightarrow v_6 \rightarrow e_6 \rightarrow v_5 \rightarrow e_5 \rightarrow v_4 \rightarrow e_4 \rightarrow v_3 \rightarrow e_3 \rightarrow v_5 \rightarrow e_5 \rightarrow v_1$  is an Eulerian circuit. Though the circuit contains all edges exactly once, it may contain some vertices more than once (e.g.  $v_4$ ,  $v_5$ ,  $v_6$ ). Hence, the graph is Eulerian graph.

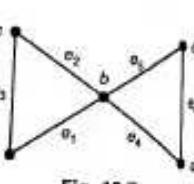


Fig. 13.7

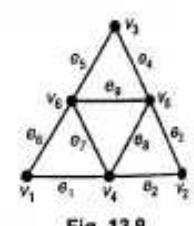


Fig. 13.9

(13-4)

Example 3 : Show that the graph given in Fig. 13.10 is not Eulerian.  
Sol. : We cannot find circuit which contains all the edges but exactly once. Hence, the graph is not Eulerian.



Fig. 13.10

#### 3. Euler's Theorem

Before we state the important theorem named after Euler, we must know Connected Graph. We repeat the definition of connected graph for the sake of completeness.

Definition : A graph in which there is a path from any vertex to any other vertex is called a connected graph.

A graph which is not connected is called a disconnected graph.

In a disconnected graph various connected pieces are called components of the graph.

In Fig. 13.11 (a), the graph is connected because there is a path from any vertex to any other vertex.

In Fig. 13.11 (b), the graph is not connected as there is no path from  $b$  to  $d'$  or from  $c$  to  $c'$ .

The connected parts of the graph  $a$ ,  $b$ ,  $c$  and  $d$ ,  $e$  are the components of the graph.

Theorem : A connected graph with  $n$  vertices has at least  $(n - 1)$  edges. (M.U. 1998)

We accept this theorem without proof but give some more explanation below.

If there are two vertices in a connected graph then there is at least one edge e.g.,  $v_1$  and  $v_2$  are two vertices and  $e_1$  is an edge.

If there are three vertices in a connected graph, then there are at least two edges e.g.,  $v_1$ ,  $v_2$  and  $v_3$  are three vertices and  $e_1$ ,  $e_2$  are the two edges and so on.

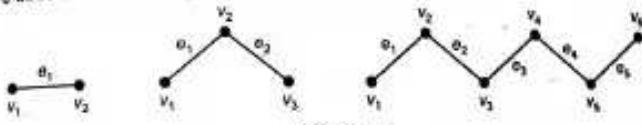


Fig. 13.11

You might have noted that the graphs in Figure 9.7 and 9.8 are Eulerian and both the graphs have all the vertices of even degree. In Fig. 13.2 and 9.10, the graphs are not Eulerian and both the graphs have vertices of odd degree.

We have a simple criterion to determine whether the given graph is Eulerian or not.

#### Criterion for Eulerian Graph

Theorem 1 : A connected graph  $G$  is an Eulerian graph if and only if all vertices of  $G$  are of even degree. (M.U. 2006, 07)

We accept this theorem without proof.

This theorem gives us a very simple criterion to determine whether the given graph is an Eulerian graph.

Check the number of edges at all vertices. If all vertices are of even degree then the graph is Eulerian and it contains an Eulerian circuit.

Conversely if a graph is Eulerian then it must have all the vertices of even degree.

### Applied Mathematics - IV

(13-5)

### Eulerian & Hamiltonian Graphs

However, if a well connected graph has only two vertices of odd degree then there is a path which includes all vertices and all edges. This is stated below in theorem 2.

**Theorem 2 :** If  $G$  is a connected graph having exactly two vertices  $u$  and  $v$  of odd degree then there is a Eulerian path from  $u$  to  $v$  which includes all the edges and all the vertices of  $G$ .

We accept this theorem without proof.

The theorem states that if in a graph there are only two vertices of odd degree then there can be an Eulerian path.

In Fig. 13.13,  $u, v$  are two vertices of odd degree and the remaining are of even degree. Hence, by Theorem 2, there is Eulerian path  $u \rightarrow v \rightarrow u \rightarrow x \rightarrow v$ . But there is no Eulerian circuit.

But if we have one more edge from  $u$  to  $v$  (dotted line) then there is, by Theorem 1, (as all vertices are even) we have an Eulerian Circuit  $u \rightarrow v \rightarrow x \rightarrow y \rightarrow u$ .

**Example 1 :** Show that the graph shown in Fig. 13.14 is Eulerian.

**Sol. :** It is clear that the graph is connected. There are two groups of vertices. In the first group, the vertices  $a, b, c, d, e$ , are of degree 2. In the second group the vertices  $p, q, r, s, t, u$  are of degree 4. Since the graph is connected and each vertex is of even degree, by theorem 1, the graph is Eulerian.

$e \rightarrow d \rightarrow s \rightarrow c \rightarrow r \rightarrow b \rightarrow q \rightarrow p \rightarrow f \rightarrow u \rightarrow t \rightarrow s \rightarrow r \rightarrow q \rightarrow p \rightarrow e$  is the Eulerian circuit.

**Example 2 :** Show that the graph given in Fig. 13.15 (a) is not Eulerian. Can you make it Eulerian by adding an edge to it? How?

**Sol. :** Although the vertices  $c, d, e$  are of even degree, the remaining two vertices  $a, b$  are of odd degree 3. Hence, the graph shown in Fig. 13.15 (a) is not Eulerian.

If we make the odd vertices even by putting a new edge between them, they become even. Now, all vertices are even. Hence, the graph is Eulerian.

$a \rightarrow e \rightarrow d \rightarrow b \rightarrow a \rightarrow d \rightarrow c \rightarrow b \rightarrow a$  is the Eulerian circuit.

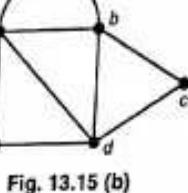
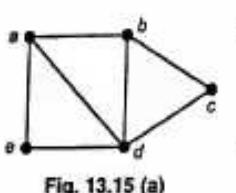


Fig. 13.15 (a)

Fig. 13.15 (b)

**Example 3 :** Show that Königsberg seven bridge problem is not solvable. What is the minimum number of bridges to be built in order to make the (new) problem solvable?

**Sol. :** By treating the four land masses as vertices and the seven bridges as edges, the seven-bridges problem can be stated as follows : Is the graph shown in Fig. 13.16 (a) Eulerian. We first note the degrees of all vertices.

$$d(A) = 5, \quad d(B) = 3, \\ d(C) = 3, \quad d(D) = 3.$$

Since all the vertices are of odd degree, the graph is not Eulerian.

Hence, the seven-bridge problem cannot be solved.



Fig. 13.16 (a)

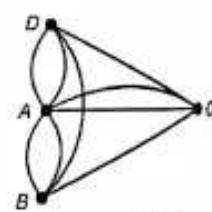


Fig. 13.16 (b)

(13-6)

### Applied Mathematics - IV

(13-6)

### Eulerian & Hamiltonian Graphs

Now to answer the question, observe that it has (all the) four vertices of odd degree. We can form two pairs out of 4 vertices and 'join' them by two additional edges. Now each vertex in 'new' graph will have even vertices and the 'new' graph becomes Eulerian.

Joining two vertices by additional edges can be done in three ways. We show in Fig. 13.18 (a) one of them leaving the remaining two to you. [See Ex. 5 of the Exercise].

In terms of bridges, this means, if we construct two more bridges then you can walk from one point and come back to the same point crossing every bridge once.

**Example 4 :** State whether the graph shown in Fig. 13.17 is Eulerian. Give reasons. (M.U. 2003)

**Sol. :** All the vertices are of odd degree 3. Hence, by the theorem 1 the graph is not Eulerian.

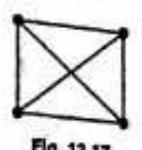


Fig. 13.17

**Example 5 :** State whether the following graph is Eulerian. (M.U. 2004, 10, 11)

**Sol. :** All the vertices are of even degree, hence, by theorem 1, the graph is Eulerian. The Eulerian circuit is

$$\pi : 6, 7, 6, 4, 3, 5, 7, 3, 2, 4, 1, 2, 1, 6.$$

[ See Fig. 13.18 ]

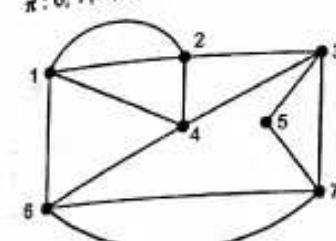


Fig. 13.18

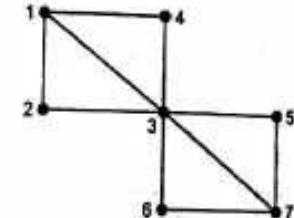


Fig. 13.19

**Example 6 :** In the adjoining graph can there be Eulerian path? (M.U. 2004)

**Sol. :** There are only two vertices 1 and 7 are of odd degree three. Hence, by theorem 2, there is a path from 1 to 7 which includes all the edges and all the vertices. That path is

$$\pi : 1, 2, 3, 1, 4, 3, 6, 7, 3, 5, 7. \quad [ \text{See Fig. 13.19} ]$$

**Example 7 :** In the adjoining graph, can there be an Eulerian circuit? (M.U. 2011)

**Sol. :** Since the three vertices A, B, D are of odd degree 1 or 3, by Theorem 1, page 13-4, the graph does not have an Eulerian circuit.

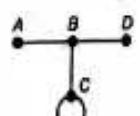


Fig. 13.20

**Example 8 :** In the adjoining graph can there be an Eulerian circuit? (M.U. 2010)

**Sol. :** Since, the vertex 4 is of odd degree 5 and the vertex 7 is of odd degree 3, the graph does not have Eulerian circuit by Theorem 1, page 13-4.

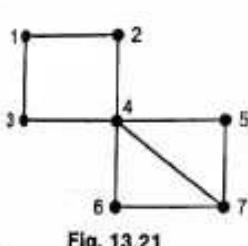


Fig. 13.21

**Example 9 :** In the adjoining graph can there be an Eulerian circuit? (M.U. 2009)

Sol. : Since the vertices A and B are of odd degree, there is no Eulerian circuit.

But since there are only two vertices of odd degree A and B, there is an Eulerian path from A to B. (By Theorem 2, page 13-5)

$$\pi : A B D C A F C E D G F G D$$

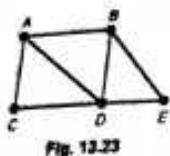


Fig. 13.23

**Example 10 :** In the adjoining graph can there be an Eulerian circuit?

Sol. : Since the vertices A, B are of odd degree, the graph does not have Eulerian circuit by Theorem 1, page 13-4.

But by Theorem 2, page 13-5. Since there are only two vertices A and B of odd degree the graph has an Eulerian Path from A to B.

$$\pi : A B E D C A D B$$

**Example 11 :** Which of the following graphs has an Eulerian Paths. Justify your answer.

Sol. : In Fig. 13.24 (i), there are two odd vertices B and D of degree 3. Hence, by Theorem 1, page 13-4, the graph does not have Eulerian Circuit, but by Theorem 2, page 13-5, it has Eulerian path from B to D.

$$\pi : B A G F E D C B G C F D$$

is an Eulerian path.

In Fig. 13.24 (ii), there are six odd vertices of degree 3 (A, B, C, D, E, F). Hence, by Theorem 1, page 13-4, the graph does not have Eulerian Circuit or an Eulerian Path.

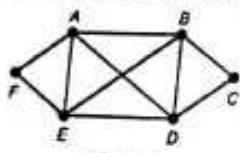


Fig. 13.24 (i)

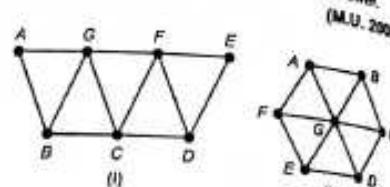


Fig. 13.24 (ii)

**Example 12 :** Determine whether the following graph has Eulerian path and Eulerian circuit. (M.U. 2016)

Sol. : Since all vertices are of even degree the graph contains Euler's circuit.

Eulerian path : A, B, C, D, E, F,

Eulerian Circuit : A B D A E D C B E F A

**Example 13 :** Determine whether the adjoining graph (Fig. 13.26) has an Eulerian path, Eulerian circuit. (M.U. 2015)

Sol. : There are four vertices a, c, f, g with odd degree three.

By Theorem 1, since there are four vertices of odd degree, there can be no Eulerian circuit.

By Theorem 2, since there are more than 2 vertices of odd degree there can be no Eulerian path.

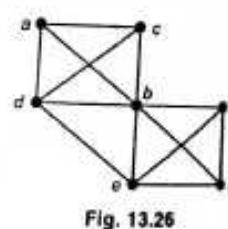


Fig. 13.26

**EXERCISE - I**

1. Draw a graph which has an Eulerian circuit and a cut vertex also.

[Ans. : (See Fig. 13.27 below)  
Eulerian circuit :  $a \rightarrow e_1 \rightarrow e_2 \rightarrow e_3 \rightarrow e_4 \rightarrow e_5 \rightarrow e_6 \rightarrow e_7 \rightarrow a$  a cut vertex b.]

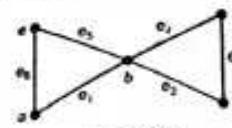


Fig. 13.27



Fig. 13.28

2. Draw a graph which contains an Eulerian path but does not contain Eulerian circuit. Explain

[Ans. : (See Fig. 13.28)  
The Eulerian path is  $d \rightarrow e_1 \rightarrow e_2 \rightarrow b \rightarrow e_1 \rightarrow e_3 \rightarrow e_4 \rightarrow d$ .  $e_1 \rightarrow b \rightarrow e_3 \rightarrow e_4$  is not Eulerian circuit because its vertices are not of even degree.]

3. State whether the following graphs are Eulerian and why?



(a)



(b)



(c)



(d)



(e)



(f)

Fig. 13.29

[Ans. : (a) No. It has 8 vertices each of odd degree 3. (b) No. It has two vertices of odd degree 3. (c) Yes. Each vertex is of even degree. 4 of degree 2 and 4 of degree 4. Connected. (d) Yes. Each vertex of degree 4. (e) No. All vertices of odd degree 5. (f) No. All the vertices of degree 3.]

4. Are the graphs shown in the Fig. 13.30 Eulerian ? If not can you make them Eulerian by adding an edge? If yes, obtain the new graph.

[Ans. : All graphs are not Eulerian. These graphs can be made Eulerian by adding an edge as shown below. We make the odd vertices even.

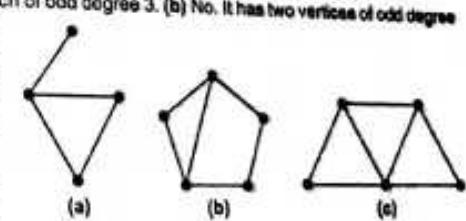


Fig. 13.30

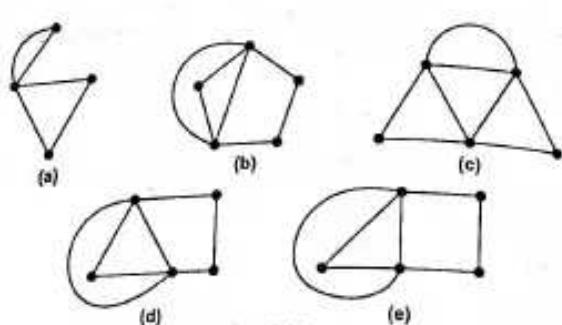


Fig. 13.31

5. Find the other two solutions by which the 7 bridge problem can be solved.

[Ans. : (i)

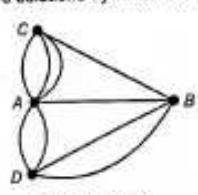


Fig. 13.32 (a)

(ii)

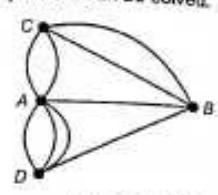


Fig. 13.32 (b)

(i) Build two additional bridges from A to C and from B to D. (ii) Build two additional bridges from B to C and from A to D.]

6. Find the conditions under which the following graphs have an Eulerian circuit. Give reasons.



Fig. 13.33

 $G_1$  $G_2$ 

Fig. 13.33

 $G_3$ 

[Ans. : All have Eulerian circuits as all have vertices of even degree.]

#### 4. Hamiltonian Graph

**Definition :** Let  $G = (V, E)$  be a graph. A path in  $G$  which contains all the vertices of  $G$  exactly once is called a Hamiltonian path. A circuit in  $G$  which contains all the vertices but exactly once in  $G$  is called a Hamiltonian circuit. If  $G$  has a Hamiltonian circuit, then  $G$  is called a Hamiltonian Graph.

(M.U. 2016, 17)

#### Notes ...

- Like an Eulerian graph, a Hamiltonian (and semi-Hamiltonian) graph is connected.
- There is a difference between an Eulerian circuit and a Hamiltonian circuit. In Eulerian circuit each edge must be traversed. Hence, in an Eulerian circuit each vertex will be visited but some vertices might be visited more than once.

But in Hamiltonian circuit all the vertices will be visited once and once only except the initial vertex. Hence, some edges may not be traversed at all.

- We have a very simple test to find out whether a graph is Eulerian viz. each vertex has even degree. But there is no such simple rule to decide whether a graph is Hamiltonian. This makes a Hamiltonian graph interesting.

- The graphs shown in the Fig. 13.34 are Hamiltonian. (In the following examples we shall show the circuit by arrows for the sake of brevity.)

Note that there may exist more than one Hamiltonian circuit. For example, in the last graph we can have following Hamiltonian circuit and some more.

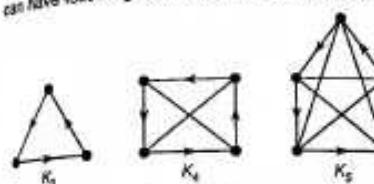


Fig. 13.34

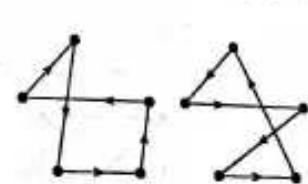


Fig. 13.35

	Repeated Vertex	Repeated Edge	Edges	Vertices
Eulerian	Allowed	No	All	All
Hamiltonian	No (Except terminal)	Allowed	Not necessarily All	All

**Theorem 1 :** If  $G$  is a simple connected graph with  $n$  vertices and if the sum of the degrees of each pair of vertices is greater than or equal to  $(n-1)$  then there exists a Hamiltonian path in  $G$ .

**Explanation :** In the graph of Fig. 13.36, the number of vertices  $n=5$ , the sum of degrees of each pair of vertices is 4 or greater than 4 equal to  $(n-1)$ .

Hence, there exists a Hamiltonian circuit viz.

$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_5 \rightarrow v_4 \rightarrow v_5 \rightarrow v_1$ .

It may be noted that the condition in the above theorem is sufficient but not necessary.

For example in the graph in Fig. 13.36, there exists a Hamiltonian circuit but the condition is not satisfied. There are  $n=6$  vertices and the sum of degrees of any pair of vertices is 4. This sum is not greater than or equal to  $(n-1)=5$ .

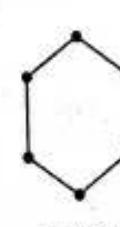


Fig. 13.36

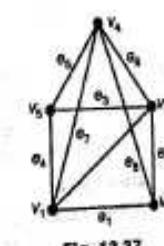


Fig. 13.37

The following theorem due to Dirac gives another sufficient condition for existence of Hamiltonian circuit in a simple connected graph.

**Theorem 2 :** In a simply connected graph  $G$  (with no loops) with  $n$  vertices if the degree of each vertex is greater than or equal to  $n/2$ , then  $G$  will contain an Hamiltonian circuit.

**Explanation :** In the graph given in Fig. 13.27 (above), the number of vertices  $n = 5$  and the degree of each vertex 3 or 4 and  $d(v) \geq n/2$ . Hence,  $G$  contains a Hamiltonian circuit viz.  $v_1 - v_2 - v_3 - v_4 - v_5 - v_1$ .

The condition given in the above theorem is again sufficient and not necessary.

**Example 1 :** Given an Example of a graph which is

- Eulerian and Hamiltonian,
- Eulerian but not Hamiltonian,
- Hamiltonian but not Eulerian,
- Neither Hamiltonian nor Eulerian.

Sol. :

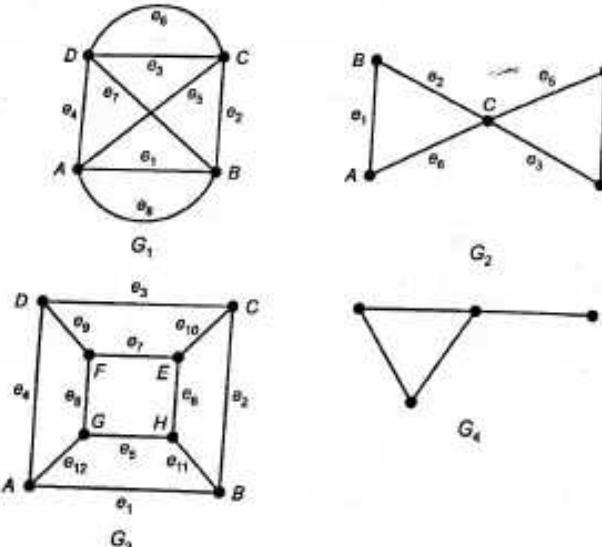


Fig. 13.38

- In Fig. 13.38, the graph  $G_1$  is Eulerian as well as Hamiltonian. The circuit  $A e_1 B e_2 C e_3 D e_4 A e_5 C e_6 D e_7 B e_8 A$  is an Eulerian circuit because it contains every edge exactly once. The circuit  $A e_1 B e_2 C e_3 D e_4 A$  is a Hamiltonian circuit as it contains all the vertices  $A, B, C, D$  once only.
- In Fig. 13.38, the graph  $G_2$  is Eulerian but not Hamiltonian. The circuit  $A e_1 B e_2 C e_3 D e_4 E e_5 C e_6 A$  is an Eulerian circuit because it contains every edge exactly once only.

The circuit is not Hamiltonian because there is no circuit which contains all the vertices once only.

(a) In Fig. 13.38, the graph  $G_3$  is not Eulerian because there is no circuit which contains all the edges once only.

But the graph is Hamiltonian because the circuit  $A e_1 B e_2 C e_3 D e_4 E e_5 F e_6 G e_7 H e_8 G e_9 A$  contains all the vertices once only.

(b) In Fig. 13.38, the graph  $G_4$  is neither Eulerian nor Hamiltonian because there is no circuit which contains all edges and there is no circuit which contains all the vertices once only.

**Example 2 :** Obtain a Hamiltonian circuit for each of the graphs shown in the Fig. 13.39.

Sol. : (a) Denote the vertices and edges as above. Then a Hamiltonian circuit is  $a e_1 b e_2 c e_3 d e_4 a$ .

(There are some other Hamiltonian circuit also, e.g.  $a e_4 d e_5 b e_2 c e_3 a$ . Find others.)

(b) Denoting the vertices and edges as above, we have a Hamiltonian circuit is  $p e_1 q e_2 r e_3 s e_4 t e_5 u e_6 v e_7 w e_8 x e_9 y e_10 z e_11 p$ .

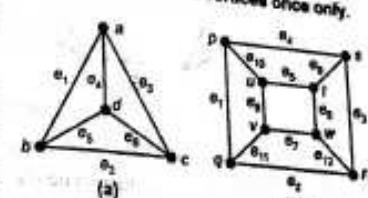


Fig. 13.39

**Example 3 :** Discuss whether the following graphs have Hamiltonian path, Hamiltonian circuit.

(M.U. 2007, 10, 11, 16)

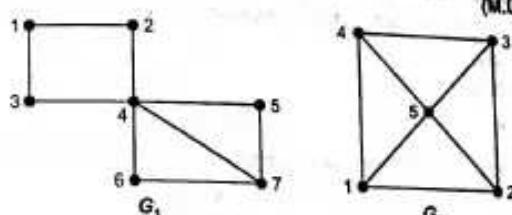


Fig. 13.40

Sol. : (a)  $G_1$  is a simple graph with  $n = 7$  vertices. The degree of the vertex 1, 2, 3, 5, 6 is 2. It is not greater than  $7/2 = 3.5$ .

Hence, by theorem 2, there is no Hamiltonian circuit.

But there is an Hamiltonian path  $\pi : 3, 1, 2, 4, 6, 7, 5$ .

(b) The graph  $G_2$  is simply connected. There are  $n = 5$  vertices. But the degree of each of the vertices 1, 2, 3, 4 is 3 and the degree of the vertex 5 is 4.

Since the degree of each vertex is greater than  $n/2 = 2.5$ , there is by Theorem 2, Hamiltonian circuit.

The Hamiltonian circuit is

$\therefore$  The graph is Hamiltonian.

$\therefore$  There is a Hamiltonian path

$\pi : 1, 2, 5, 3, 4$ .

**Example 4 :** Discuss whether the following graph has Hamiltonian path, Hamiltonian circuit. (M.U. 2000, 09)

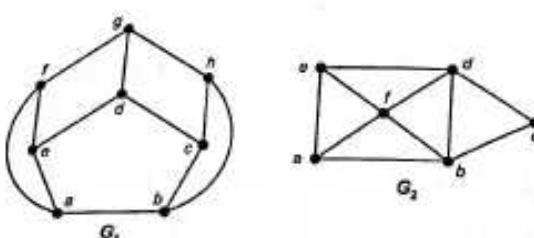


Fig. 13.41

Sol. : (a)  $G_1$  is a simple graph with  $n=8$  vertices. The degree of each vertex is  $3 \times (n/2) = 4$ . Hence, by the theorem 2, there is no Hamiltonian circuit and hence no Hamiltonian graph.

But there are Hamiltonian paths. One of them is

$$\pi : a, b, c, d, e, f, g, h.$$

- (b) The graph  $G_2$  has 6 vertices  $a, b, c, d, e, f$  with degree 3, 4, 2, 4, 3, 4. The sum of the degrees of any two vertices is greater than or equal to  $(n-1) = 5$ . Hence, by theorem 1 there is a Hamiltonian circuit and hence it is a Hamiltonian graph.

$$\pi : a, f, b, c, d, e, a.$$

Hamiltonian path is

$$\pi : a, f, b, c, d, e.$$

**Example 5 :** Discuss whether the following graphs have Hamiltonian path, Hamiltonian circuit. (M.U. 2003)

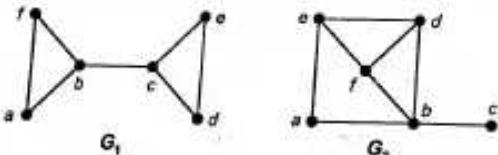


Fig. 13.42

Sol. : (a) The graph  $G_1$  has 6 vertices  $a, b, c, d, e, f$  with 2, 3, 3, 2, 2, 2 degrees respectively. Since the degree 2 of  $a, f, d, e$  is less than  $6/2 = 3$  the graph does not have Hamiltonian circuit.

∴ The graph is not Hamiltonian. However, there is an Hamiltonian path

$$a, f, b, c, d, e.$$

- (b) The graph  $G_2$  has 6 vertices  $a, b, c, d, e, f$  with 2, 4, 1, 3, 3, 3 degrees respectively. The sum of the degrees of  $a$  and  $c$  is  $2+1=3$  is less than  $(n-1)=5$ .

Hence, there is no Hamiltonian circuit.

∴ The graph is not Hamiltonian. The Hamiltonian path is

$$\pi : a, e, d, f, b, c.$$

**Example 6 :** Draw a graph which has (i) Hamiltonian path as well as Hamiltonian circuit, (ii) Hamiltonian path but not Hamiltonian circuit.

Sol. : (a) In the graph shown in Fig. 13.43 (a),

$$a-e_1-b-e_2-c-e_3-d-e_4-a$$

is a Hamiltonian circuit.

$$a-e_1-b-e_2-c-e_3-d$$

is a Hamiltonian path.

(b) In the graph shown in Fig. 13.43 (b), since the vertex  $d$  is a pendant

there is no Hamiltonian circuit.

But there is Hamiltonian path.

$$d-a-b-c-a$$

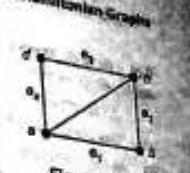


Fig. 13.43 (b)

(M.U. 2008, 09)

**Example 7 :** (a) Is every Hamiltonian graph Eulerian? Given an example.

(b) Is every Eulerian graph Hamiltonian? Give an example.

Sol. : (a) No. Every Hamiltonian graph is not Eulerian.

In the graph shown in Fig. 13.44 (a), there is Hamiltonian circuit

$$a-b-c-d-e-f-a$$

Hence, it is Hamiltonian graph.

But since all vertices are not even ( $a, c$  are of degree 3), there is no Eulerian circuit. The graph is not Eulerian.

**Fig. 13.44 (a)**

**Fig. 13.44 (b)**

(b) No. Every Eulerian graph is not Hamiltonian.

In the graph shown in Fig. 13.44 (b), there is an Eulerian circuit and hence, it is an Eulerian graph. It has all the vertices of even degree.

The circuit  $a-b-c-e-a-f-c-e-a$  is Eulerian.

But it does not have Hamiltonian circuit.

**Example 8 :** Determine whether the following graphs are Hamiltonian. Find the circuit if yes in each case. (M.U. 2012, 13)

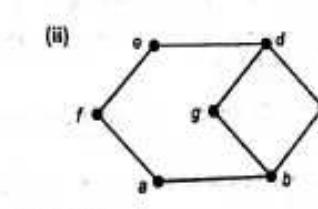
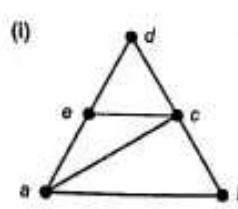


Fig. 13.45

- Sol. : (i) In (i), there are 5 vertices  $a, b, c, d, e$  of 3, 2, 4, 2, 3 degrees. The sum of the degrees of each pair of vertices is greater than or equal to  $(n-1) = (5-1) = 4$ .  
 ∴ There exists a Hamiltonian circuit.  
 The circuit is  $a, b, c, d, e, a$ .
- (ii) In (ii), there are 7 vertices  $a, b, c, d, e, f, g$  of 2, 3, 2, 3, 2, 2, 2 degrees.  
 The sum of each pair of vertices is not greater than or equal to  $(n-1) = 6$ .  
 ∴ There does not exist a Hamiltonian circuit.

**Example 9 :** Determine whether the graphs given below have a Hamiltonian circuit, Eulerian circuit, if so, find them.

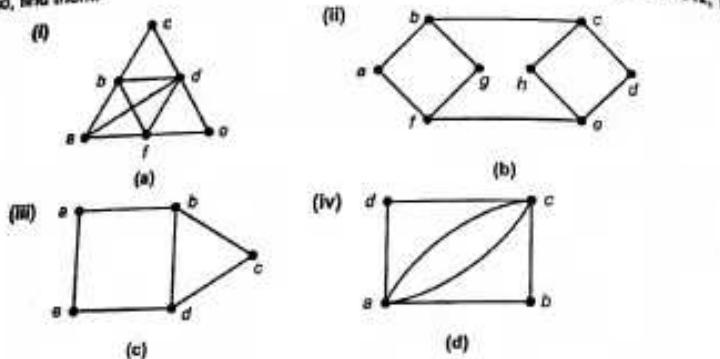


Fig. 13.46

- Sol. : (a) Yes Hamiltonian circuit.  $a - b - c - d - e - f$ . No Eulerian circuit. The vertex  $a$  is of odd degree.  
 (b) No Hamiltonian circuit. No Eulerian circuit. The vertices  $f, b, e, c$  are of odd degree.  
 (c) Yes Hamiltonian circuit  $a - e - d - c - b - a$ .  
 No Eulerian circuit. The vertices  $b, d$  are of odd degree.  
 (d) Yes Hamiltonian circuit  $a - b - c - a - c - d - a$ .  
 Yes Eulerian circuit  $a - b - c - a - c - d - a$ .

**Example 10 :** Determine if there is Hamiltonian path, Hamiltonian cycle in the adjoining graph (Fig. 13.47). (M.U. 2017)

Sol. : Since, the sum of degrees of each pair of vertices is greater than or equal to  $(n-1) = 3$ , there is a Hamiltonian path  $a, b, c, d$ .

Since, the degree of vertex  $a$  is not greater than or equal to  $n/2 = 2$ , there is no Hamiltonian circuit.

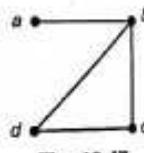


Fig. 13.47

**Example 11 :** Find Hamiltonian path and a Hamiltonian circuit in the graph  $K_{4,3}$  if possible. (M.U. 2010)

Sol. : As discussed in (4), page 12-11, the Complete Bipartite Graph  $K_{4,3}$  is given by

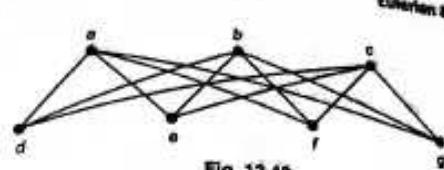


Fig. 13.48

The total number of vertices is  $n = 7$ .  
 The sum of the degrees of each pair of vertices is 7 and is greater than  $(n-1) = 6$ . Hence, by Theorem 1, page 13-10, there is a Hamiltonian path  
 $\pi : d, a, e, b, f, c, g$ .  
 Further, the graph has 7 vertices and the degree of each vertex is either 3 (or 4). But  $3 \neq (7/2)$ .  
 Hence, by Theorem 2, page 13-11, there is no Hamiltonian circuit.

**Example 12 :** Find out an Hamiltonian path and Hamiltonian circuit in a graph shown in the Fig. 13.49 with explanation. (M.U. 2010)

Sol. : The total number of vertices is  $n = 4$ . Each vertex is of 4 degree.

The sum of the degrees of each pair of vertices is  $8 > (n-1) = 3$ . Hence, by Theorem 1, page 13-10, there is a Hamiltonian Path  
 $\pi : A, B, C, D$ .

Further, the graph has 7 vertices and the degree of each vertex is 4 which is greater than  $(n/2) = 7/2 = 3.5$ .

Hence, by Theorem 2, page 13-11, there is a Hamiltonian circuit  $A, B, C, D, A$ .

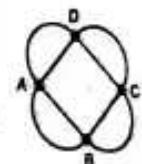


Fig. 13.49

**Example 13 :** Find out the Eulerian path, Hamiltonian path, if they exist, in the following graphs. (M.U. 2014)

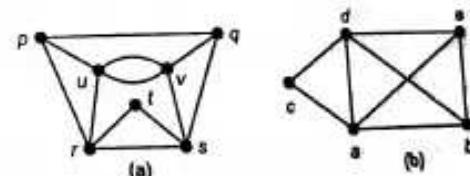


Fig. 13.50

Sol. : In (a), the Hamiltonian path is

the Eulerian path is

In (b), the Hamiltonian path is

the Eulerian path is

$\pi : p, u, v, q, s, t, r$

$\pi : p, u, v, q, s, v, u, r, t, s$

$\pi : a, b, c, d, c$

$\pi : e, d, b, a, d, c, a$

**EXERCISE - II**

1. Find a Hamiltonian circuit in the following graphs.

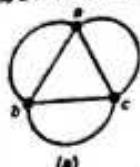


Fig. 13.51

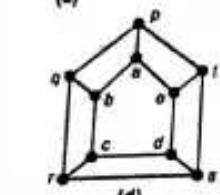
[Ans.: (a)  $a \rightarrow b \rightarrow c \rightarrow a$ , (b)  $a \rightarrow b \rightarrow c \rightarrow d \rightarrow e$ , (c)  $a \rightarrow c \rightarrow f \rightarrow d \rightarrow e \rightarrow b \rightarrow a$ ,

Fig. 13.51

(d)  $p \rightarrow q \rightarrow b \rightarrow s \rightarrow e \rightarrow d \rightarrow c \rightarrow r \rightarrow s \rightarrow l \rightarrow p$ ,(e)  $d \rightarrow a \rightarrow f \rightarrow l \rightarrow g \rightarrow k \rightarrow h \rightarrow i \rightarrow j \rightarrow a \rightarrow b \rightarrow c \rightarrow d$ .]

2. Find a Hamiltonian path and if possible a Hamiltonian circuit in the following graph.

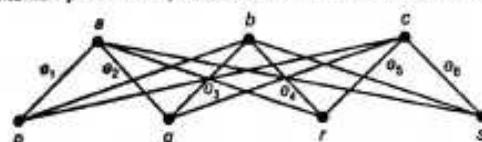


Fig. 13.52

[Ans.:  $p \rightarrow e_1 \rightarrow a \rightarrow e_2 \rightarrow q \rightarrow e_3 \rightarrow b \rightarrow e_4 \rightarrow r \rightarrow e_5 \rightarrow c \rightarrow e_6 \rightarrow s$ . Since  $m \neq n$  there is not Hamiltonian cycle.]

3. Show that the following diagram (Fig. 13.53) has no Hamiltonian cycle.

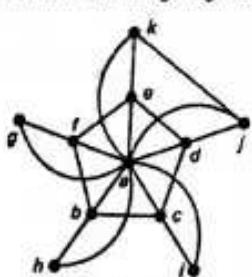


Fig. 13.53

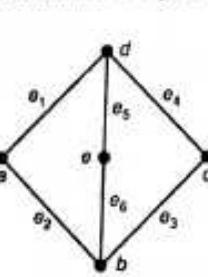


Fig. 13.54

4. Show that the above diagram (Fig. 13.54) has no Hamiltonian cycle although it has a Hamiltonian path.

[Ans.: Hamiltonian path is  $a \rightarrow d \rightarrow e \rightarrow b \rightarrow c$ ]**Travelling Salesperson Problem (T.S.P.)**

One of the problems related to Hamiltonian Circuit is Travelling Salesman Problem. A salesman is required to start from the head-quarter  $v$ , visit the retail shops located at  $a, b, c, d, \dots$  and come back to the head-quarter at  $v$ . If the distance between any place to any other place is known, what should be the order of the places in which the salesmen should visit the places so that the total distance travelled (i.e. the cost) is minimum? This is the travelling salesperson problem.

From the point of view of graph theory, this problem is equivalent to finding the Hamiltonian circuit, starting and ending at the vertex  $A$  and connecting each of the vertices  $v_1, v_2, \dots, v_n$  such that the total distance of the circuit is minimum.

**Nearest Neighbour Method**

The problem is solved by the method called nearest neighbour method which gives a better solution to Travelling Salesperson Problem. In this method the following procedure is as follows:

1. Start from the vertex  $A$  which denotes the head-quarter.
2. From  $A$  go to the vertex which has minimum distance from  $A$ . If  $v_m$  is such a vertex, join  $A$  to  $v_m$  by an edge.
3. From  $v_m$  go to the vertex which has minimum distance from  $v_m$ . If  $v_n$  is such a vertex, join  $v_m$  to  $v_n$  by an edge.
4. In this way complete the circuit joining the last vertex to  $A$ .

While solving T.S.P. it is convenient to use the matrix in which the distances of the vertices are shown. To start with, the nearest vertex is joined to the head quarter and the row and the column having these vertices are deleted from the matrix.

**Example :** By starting from the vertex  $v$  solve the T.S.P. whose graph is shown in Fig. 13.55.

**Sol.:** We start with the matrix showing the lengths of the edges joining  $v_i$  and  $v_j$ .

	$v$	$a$	$b$	$c$	$d$
$v$	0	12	8	5	4
$a$	12	0	9	10	18
$b$	8	9	0	7	15
$c$	5	10	7	0	6
$d$	4	18	15	6	0

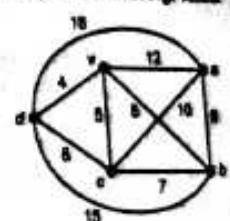


Fig. 13.55

Note that this is a symmetric matrix as expected.

In the row of  $v$  the entries are 12, 8, 5 and 4. The entry 4 is minimum and hence, the vertex  $d$  is nearest to  $v$ , so we connect  $v$  to  $d$  and get the initial path. Here, we drop the columns of  $v$  and  $d$  from our consideration and consider the row of  $d$ . In this row entries are 18, 15 and 6 (excluding those in the columns of  $v$  and  $d$ ). The minimum is 6 and hence, the vertex  $c$  is nearest to  $d$ . We connect  $d$  to  $c$  and get the path 13.56 (b). Here, we drop the column of  $c$  ( $d$  and  $v$ ) from our consideration and consider the row of  $c$ . In the row of  $c$  the remaining entries are 10 and 7. Since 7 is minimum, we connect  $c$  to  $b$  and get the graph 13.56 (c).

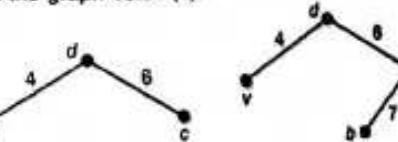
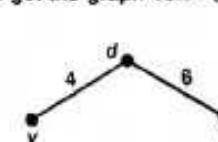
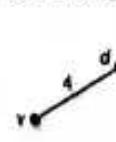


Fig. 13.56 (a)

Fig. 13.56 (b)

Fig. 13.56 (c)

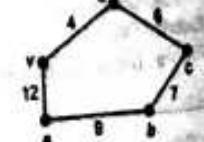


Fig. 13.56 (d)

Since now only one vertex  $a$  remains to be connected. So we connect  $b$  to  $a$  and then  $a$  to  $v$ , and get the Hamiltonian circuit  $v - d - c - b - a - v$  as in 9.54 (d).  
The length of the circuit =  $4 + 6 + 7 + 9 + 12 = 38$ .

**EXERCISE - III**

1. Solve travelling sales-person problem for the graphs shown in Fig. 13.57, treating  $v$  as the end vertex.

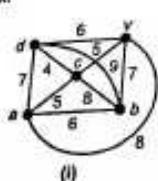


Fig. 13.57

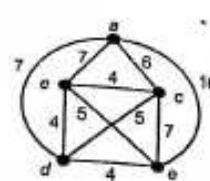
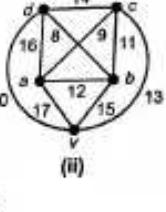


Fig. 13.58

[Ans. : (i)  $v - c - d - a - b - v$ , (ii)  $v - d - b - c - a - v$ ]

2. For the graph shown in Fig. 13.58 above, find the minimum Hamiltonian circuit (a) taking  $a$  as the starting vertex, (b) taking  $d$  as the starting vertex.

[Ans. : (a)  $a - c - b - d - a - a$ , 28; (b)  $d - a - b - e - a - d$ , 26.]

**EXERCISE - IV****Theory**

1. Define the following terms with illustrations and graphs wherever necessary.

(i) Eulerian Path, Circuit

(M.U. 2001, 02, 11)

(ii) Eulerian Graph

(M.U. 2001, 02, 11)

(iii) Hamiltonian Path, Circuit

(M.U. 2001, 16)

(iv) Hamiltonian Graph

(M.U. 2002)

2. Is every Eulerian graph Hamiltonian and is every Hamiltonian graph Eulerian? Explain with examples.

(M.U. 2008, 09, 17)

3. State the seven-bridge problem. What is its solution?

4. Prove that a connected graph  $G$  is an Eulerian graph if and only if all vertices of  $G$  are of even degree.

5. "If  $G$  is a connected graph having exactly two vertices  $u$  and  $v$  of odd degree then there is a trail from  $u$  to  $v$  which includes all the edges and all the vertices of  $G$ ." Prove this.

6. "If in a graph  $G$  there is a path from vertex  $u$  to vertex  $v$  ( $u \neq v$ ) containing all edges of  $G$  then  $G$  is connected and  $u$ ,  $v$  are the only vertices of odd degree in  $G$ ." Prove it.

7. What is Travelling Sales-person Problem (T.S.P.)? How is it solved?

8. State the necessary and sufficient conditions for a graph to have an Eulerian Circuit and an Eulerian Path.

(M.U. 2002, 04, 06, 07, 12)

9. Define Hamiltonian path and Hamiltonian circuit. State the condition for Hamiltonian circuit.

(M.U. 2016)

**1. Introduction**

The concept of tree is highly important in graph theory. Relations in a family starting from one couple, development of a stream into a big river etc. can be shown very effectively by a graph which looks like a tree with its branches.

**Definition 1 :** A connected graph which does not have a circuit or cycle is called a tree.

The following graphs with vertices 1, 2, 3, 4, 5, 6 are trees.

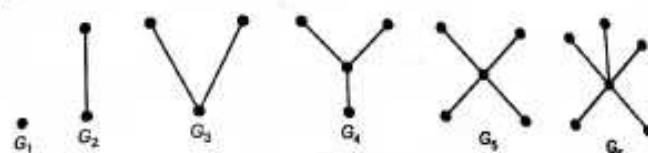


Fig. 14.1

**Definition 2 :** A vertex of degree 1 is called a terminal node or a leaf.

**Definition 3 :** A vertex of degree greater than 1 is called an internal node or a branch node.

Note ...

1. A tree is a simple graph. It has no cycles. Hence, it has no loops and no parallel edges.
2. A tree is a plane graph. It has no crossing edges.
3. It has at least one (in fact atleast two) vertex of degree 1. A tree must "start" from a vertex and "end" at a vertex.
4. It is always a bipartite graph.
5. In a tree we can always find a path joining any two vertices because it is a connected graph. Such a path is unique, otherwise it will be a cycle.
6. If we add an edge (but not a vertex) to a tree, we will get a cycle. If we delete an edge (but not a vertex) from a tree we will get a disconnected graph. Every addition of an edge to a tree creates one cycle in a tree and every deletion of an edge creates one component in it.

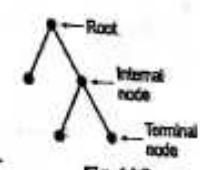


Fig. 14.2

**2. Isomorphism of Trees**

We have already seen what we meant by isomorphism in graphs. The concept of isomorphisms can be extended to trees also. If two trees are isomorphic they are called isomorphic trees.

**Example 1 :** Are the following trees isomorphic?

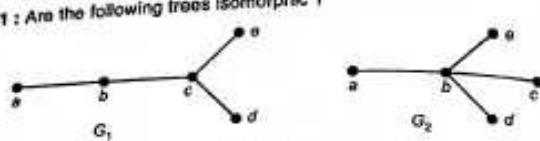


Fig. 14.3

**Sol. :** Both trees have 5 vertices and 5 edges. But in  $G_1$  there are three vertices of degree one and in  $G_2$  there are four vertices of degree one. Hence, the trees are not isomorphic.

**Example 2 :** Find all non-isomorphic trees having (i) 2, (ii) 3, (iii) 4, (iv) 5 vertices.

**Sol. :** (i) With two vertices there is only one tree.

Hence, there is only one non-isomorphic tree.

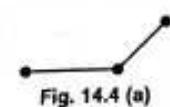


Fig. 14.4 (a)

(ii) With three vertices also there is only one tree. Hence, again there is only one non-isomorphic tree.

(iii) When the number of vertices is four the possible non-isomorphic trees are shown below. In  $G_1$  there are two vertices of degree two and two vertices of degree one. In  $G_2$  there is one vertex of degree three and three vertices of degree one. Hence, there are two non-isomorphic trees.

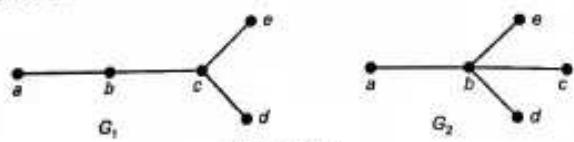


Fig. 14.4 (b)

(iv) When the number of vertices is five the possible non-isomorphic trees are shown below.

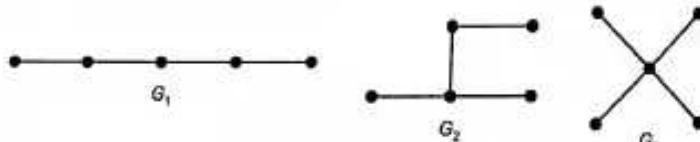


Fig. 14.4 (c)

In  $G_1$  there are two vertices of degree one and three vertices of degree two. In  $G_2$ , there are three vertices of degree one, one vertex of degree two and one vertex of degree three. In  $G_3$ , there are four vertices of degree one and one vertex of degree four. Hence, there are three non-isomorphic trees.

(v) When  $n = 6$  (and 5 edges) there are six non-isomorphic trees. (Explanation is left to you).

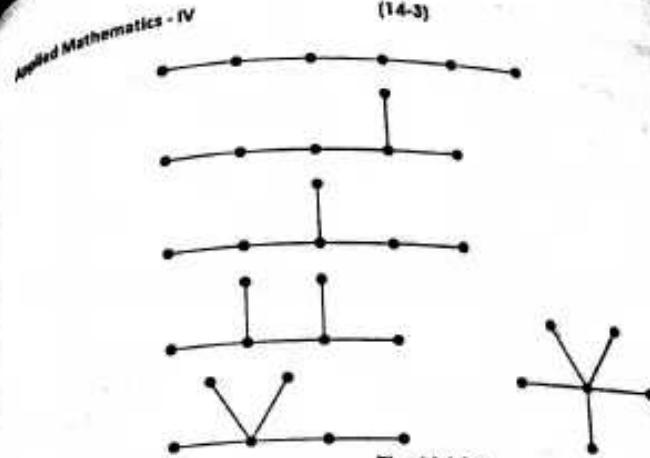


Fig. 14.4 (d)

### 3. Some Properties of Trees

We shall prove below some properties of trees as theorems.

**Theorem 1 :** In a tree there is one and only one path between every pair of vertices.

**Proof :** Let a graph  $G$  be a tree. Then by definition,  $G$  is a connected graph and  $G$  has no circuits. Since  $G$  is a connected graph, there exists a path between every pair of vertices of  $G$ . If possible suppose there are two distinct paths between two vertices say  $u$  and  $v$  of  $G$ . Now, the union of these two paths forms a circuit in  $G$ ; which is a contradiction.

Hence, there is one and only one path between every pair of vertices in a tree  $G$ .

**Theorem 2 :** If in a graph  $G$  there is one and only one path between every pair of vertices, then  $G$  is a tree.

**Proof :** Since by data there is a path between every pair of vertices of  $G$ ,  $G$  is a connected graph.

Further if a graph has a circuit there must be at least one pair of vertices with two distinct paths. But by data again there is one and only one path between every pair of vertices. Hence,  $G$  is circuit-free.

Since  $G$  is connected and circuit-free,  $G$  is a tree.

**Theorem 3 :** A tree with  $n$  vertices has  $(n - 1)$  edges.

We shall accept this theorem without proof.

**Theorem 4 :** Any connected graph  $G$  with  $n$  vertices and  $(n - 1)$  edges is a tree.

We shall accept this theorem without proof.

**Theorem 5 :** A graph with  $n$  vertices is a tree if and only if it is circuit-free and it has  $(n - 1)$  edges.

We shall accept this theorem without proof.

**Theorem 6 :** In any tree with two or more vertices, there are at least two pendant vertices.

**Proof :** Let  $G$  be a tree with  $n$  vertices where  $n \geq 2$ .  
Since  $G$  is a tree with  $n$  vertices by theorem 4, it has  $(n-1)$  edges.

$$\text{Total number of degree of } G = 2 \text{ (number of edges)}$$

$$= 2(n-1) = 2n-2$$

Since,  $G$  is a tree, it is a connected graph and there is no vertex with degree zero.  
If, now, we assign one degree to each vertex, there remain  $(2n-2) - n = n-2$  degrees, again we assign one degree to each vertex (Since there are  $n$  vertices and  $(n-2)$  degrees) there will be at least two vertices not getting any degree in the second round.

$\therefore$  There will be at least two pendant vertices.

**Example 1 :** A tree  $T$  has some vertices of degree one, two vertices of degree two, three vertices of degree four and four vertices of degree three. Find the number of vertices of degree one in the tree.

**Sol. :** Let the tree  $T$  have  $m$  vertices of degree one. If  $n$  is the total number of vertices in  $T$ , then

$$n = m + 2 + 3 + 4 = m + 9$$

Further, the sum of degrees in  $T$

$$= 1 \times m + 2 \times 2 + 3 \times 4 + 4 \times 3$$

$$= m + 28$$

$$\text{i.e., } \sum d(v_i) = m + 28$$

Let the tree  $T$  have  $k$  number of edges.

Since  $T$  is a tree with  $n$  vertices,  $k = n-1$  (See Theorem 3 above).

But the sum of degrees of all vertices of a graph is equal to twice the number of edges.

$$\therefore \sum d(v_i) = 2k = 2(n-1)$$

Now, using (1),

$$\sum d(v_i) = 2n-2 = 2(m+9)-2$$

$$\therefore \sum d(v_i) = 2m+16$$

From (2) and (3), we get

$$m+28 = 2m+16 \quad \therefore m=12.$$

$\therefore$  There are twelve vertices of degree one.

**Example 2 :** A tree has  $2n$  vertices of degree 1,  $3n$  vertices of degree 2, and  $n$  vertices of degree 3. Determine the number of vertices and edges.

**Sol. :** Let the tree have  $V$  vertices and  $E$  edges. By data the tree has  $n+3n+2n$  vertices

$$\therefore V = 6n$$

By data the total number degrees in the tree,

$$\sum d_i = 2n + (3n) \times 2 + (n) \times 3 = 11n$$

But by Theorem 3 the number edges in a tree is one less than the number vertices

$$\therefore E = 6n-1$$

But the total number of degrees is twice the edges

$$\therefore \sum d_i = 2E = 2(6n-1) = 12n-2$$

From (2) and (3), we get

$$11n = 12n-2$$

$$n = 2$$

Putting  $n = 2$ , from (1), we get the number of vertices  
= 12 and from (2), we get the number of edges = 11.

One such tree is shown in Fig. 14.5.  
The vertices  $a, d, f, l$  are of degree 1, the vertices  $c, g, h, i, k$  are of degree 2, the vertices  $b, e$  are of degree 3. The number of vertices = 12, the number of edges = 11.

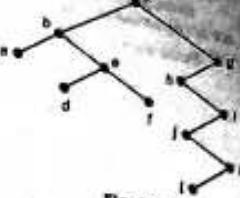


Fig. 14.5

**Example 3 :** A tree has 50 edges. The removal of certain edge from the tree yields two disjoint trees  $T_1$  and  $T_2$ . Find the number of edges in  $T_2$  if the number of vertices in  $T_1$  is equal to the number of edges in  $T_2$ .

**Sol. :** If  $e_1$  and  $e_2$  denote the number of edges in  $T_1$  and  $T_2$ , then

$$e_1 + e_2 = 49$$

because the original tree has 50 edges and one edge is now removed.

But the number of vertices in  $T_1$  is equal to the number of edges in  $T_2$ , i.e.,  $e_2$ .

Hence, the number of edges in  $T_1$ ,

$$\text{i.e., } e_1 = (\text{number of vertices}) - 1$$

$$= e_2 - 1$$

Hence, from (1), we get

$$e_2 - 1 + e_2 = 49 \quad \therefore 2e_2 = 50 \quad \therefore e_2 = 25$$

Hence, the number of edges in  $T_2$  is 25.

#### 4. Rooted Trees

We shall now study a particular class of trees called rooted trees which play a significant role in computer science.

**Definition :** A tree in which exactly one vertex is distinguishable from all other vertices is called a rooted tree. The particular distinguishable vertex is called the root of the tree.

In the following diagram we have shown rooted trees having three, four and five vertices.

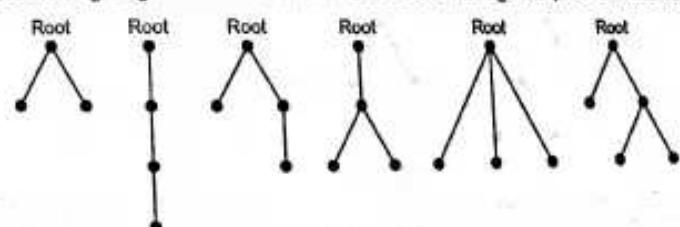


Fig. 14.6

In the first and the last trees we observe that (i) the number of vertices is odd (three or five), (ii) from each vertex there is either no branch (edge) or there are two branches (edges), (iii) the degree of the starting vertex (root) is two, (iv) the degree of an internal vertex is three and (v) the degree of the terminal vertices (leaves) is one. Such a tree is called a binary tree.

**Definition :** A tree in which one and only one vertex has degree two and the remaining vertices are of degree one or three is called a **binary tree**.

Below we have shown some binary trees with seven vertices.

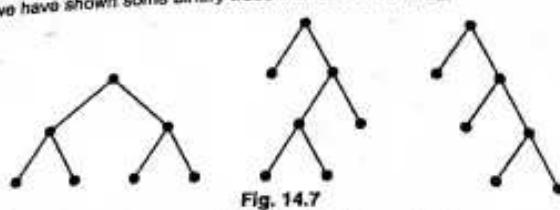


Fig. 14.7

**Definition :** If in a binary tree every internal node has exactly two branches, it is called a **full binary tree**. [ Last of Fig. 14.7 ]

It is easy to see that for the same number of vertices we can have trees of different heights. In the above diagram the number of vertices in the two trees is the same viz. nine. But the height of the second tree is three while the height of the first tree is four.

**Property 4 :** The maximum height of a binary tree having  $n$  vertices is equal to  $(n-1)/2$ , and minimum height is equal to the smallest integer greater than or equal to  $\log_2(n+1)-1$ .

**Example 1 :** Find the maximum and minimum height of the tree with 21 vertices.

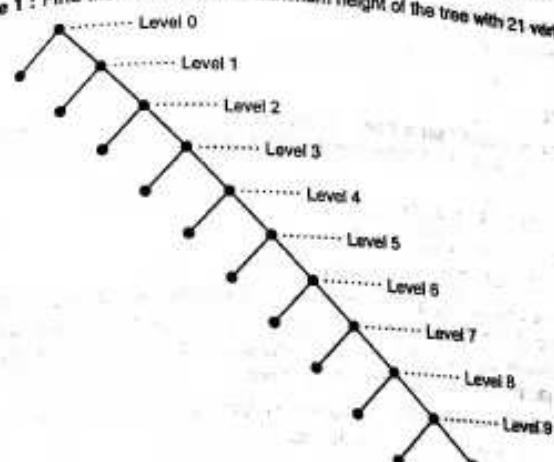


Fig. 14.9 (a)

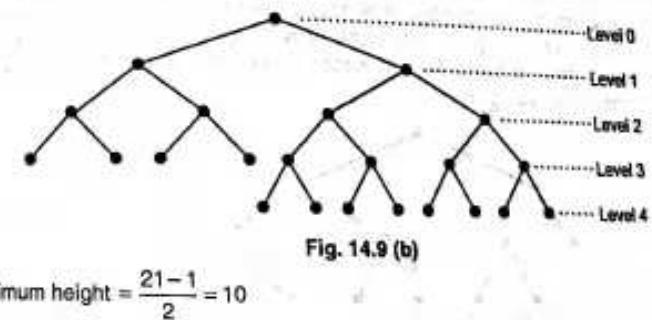


Fig. 14.9 (b)

$$\text{Sol. : Maximum height} = \frac{21-1}{2} = 10$$

$$\text{Now, } \log_2(21+1)-1 = \log_2 22 - 1$$

$$= \frac{\log_{10} 22}{\log_{10} 2} - 1 = \frac{1.3424}{0.3010} - 1 \\ = 4.4598 - 1 = 3.4598$$

$\therefore$  Minimum height = Smallest integer greater than 3.4598 = 4  
(Also note that there are not enough vertices left for the last level.)

## 5. Properties of Binary Trees

**Property 1 :** The number of vertices in a binary tree is always odd.

**Property 2 :** In a binary tree with  $n$  vertices the number of pendant vertices is  $(n+1)/2$ .

**Definition :** The intermediate vertices of degree three together with the root (having degree two) i.e., non-pendant vertices are called **internal vertices**.

**Property 3 :** The number of (non-pendant) internal vertices in a binary tree with  $n$  vertices is  $\frac{n+1}{2} - 1$ .

## 6. Height of a Binary Tree

Consider the following binary tree.

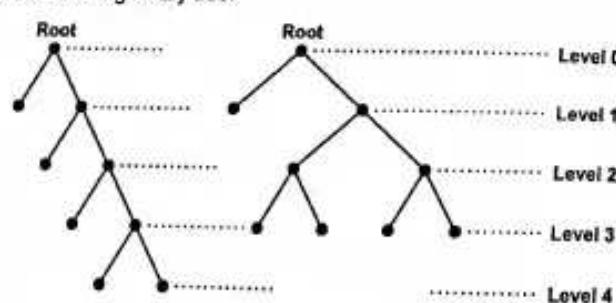


Fig. 14.8

In a binary tree we say that a vertex  $v$  is at a level  $r$  if  $v$  is at a distance  $r$  from the root. The level of the root itself is considered as zero. We have shown above the levels of all the vertices of the tree. The highest level of the tree is called the **height of the tree**.

**Definition :** The distance of a vertex from the root is called the **level of the vertex**.

**Definition :** The maximum level in a tree is called the **height of the tree**.

**Example 2 :** Find the maximum and minimum height of a binary tree with 11 vertices.

Sol. : Maximum height =  $\frac{11-1}{2} = 5$

Minimum height = Smallest integer greater than  $\log_2(11+1) - 1$ ,

Now,  $\log_2 12 = \frac{\log_{10} 12}{\log_{10} 2} - 1 = 3.5849 - 1 = 2.53$ .

$\therefore$  Minimum height = 3.

Figures are left to you.

### 7. Prefix Code

We know that an ordered set is called a sequence e.g. 232, 40873, ..., axiom, triangle, ... are sequences of digits and letters. Now, observe the following sets of sequences formed by two digits 0 and 1.

- (01, 10, 001, 110, 1111)
- (00, 101, 100, 0101, 1101)
- {11, 00, 001, 0011, 110, 1110}

In the first set no sequence is a prefix in (occurs before) any other sequence. Same is true for the second sequence. But in the third set, the sequence {11} is a prefix in the sequence {110} and also in {1110}. Also the sequence {00} is a prefix in the sequences {001} and {0011}. The first two sets are called (binary) prefix codes while the third is not.

**Definition :** A set of sequences formed from two digits 0 and 1 is called a binary prefix code if no sequence is a prefix of any sequence in the set.

Using digits 0 and 1, we can represent a binary tree by binary prefix code and conversely from a binary prefix code, we can construct a binary tree. Consider a full binary tree in which from each vertex including the root there are two branches. Let us agree to assign 0 to the branch going to the left and assign 1 to the branch going to the right. In this way we go on assigning numbers to all edges and reach the terminal nodes. Terminal nodes then can be represented by sequences of 0, 1 as shown in the following diagram.

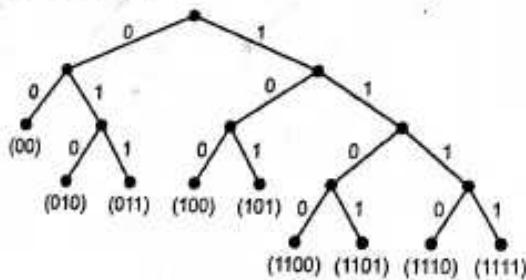


Fig. 14.10

Starting from the root, we trace a path to each terminal node and construct a sequence of digits 0, 1 assigned to the edges. The collection of these sequences represents the tree.

The prefix code of the above tree is

{00, 010, 011, 100, 101, 1100, 1101, 1110, 1111}.

Conversely from a prefix code we can obtain a binary tree by exactly reversing the process. Consider the following prefix code  
(000, 001, 01, 10, 110, 111).

Since the longest sequence is of length three we first construct a full binary tree of height 3 as shown below.

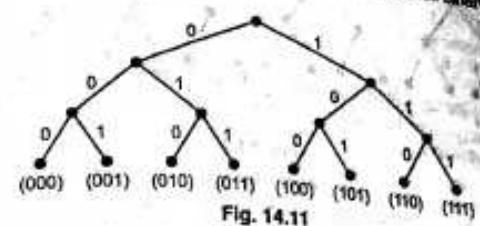


Fig. 14.11

Now, we delete those vertices whose sequences are not included in the given prefix code. We also delete the incident edges. Thus, we get the following tree.

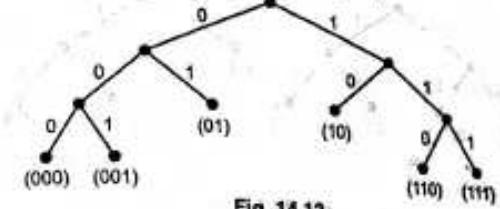


Fig. 14.12

**Example 1 :** Obtain the prefix code of the following binary tree.

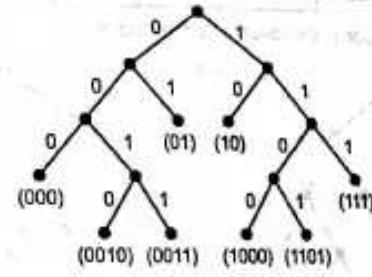


Fig. 14.13

Sol. : The top most node is the root of the tree. Assign 0 to the left branch and 1 to the right branch and continue the process. Lastly write the prefix code of the terminal nodes.

{000, 0010, 0011, 01, 10, 100, 1101, 111}.

**Example 2 :** Construct the binary tree from the following prefix code of the terminal nodes

{10, 000, 010, 011, 110, 0010, 0011, 1110, 111}.

Sol. : Since the longest sequence of length four, we first construct a full binary tree of height 4 and write the prefix code of all terminal nodes.

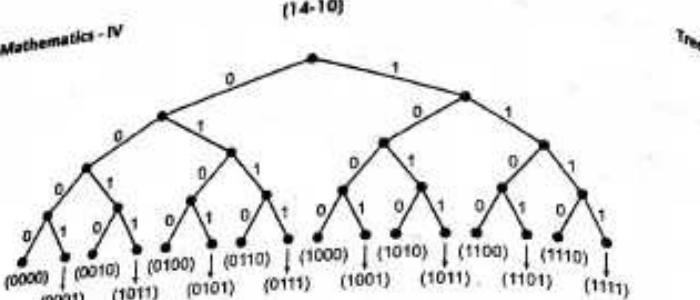


Fig. 14.14

Now, from this tree we delete all the nodes along with their edges whose prefix codes are not given. We retain only those terminal nodes whose prefix codes are given and get the following tree.

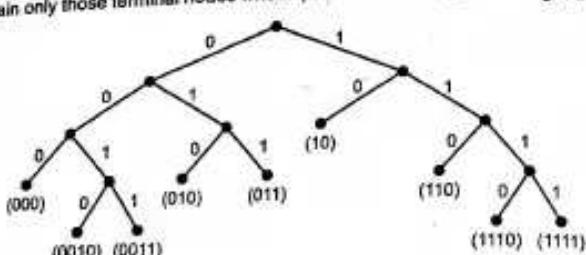
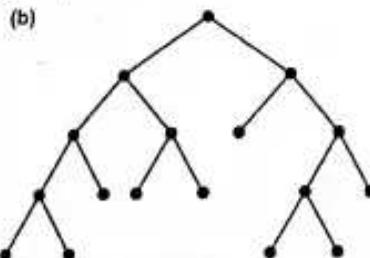
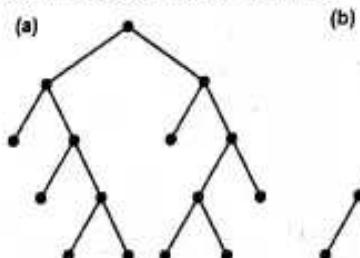


Fig. 14.14 (a)

**EXERCISE - I**

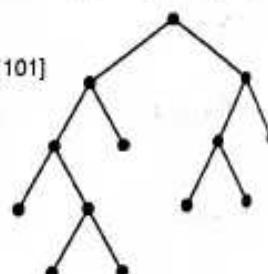
1. Obtain the prefix code of the following binary trees.



[Ans. : (a) [00, 10, 010, 111, 0110, 0111, 1100, 1101]  
 (b) [10, 001, 010, 011, 111, 0000, 0001, 1100, 1101]

2. Obtain the prefix code of the adjoining binary tree.

[Ans. : [000, 11, 0010, 100, 01, 101, 0011]]

**15. Coding and Decoding of a Message**

Using the prefix code studied above we shall now see how to encode a message in prefix code and also how to decode a message given in prefix code.

**Encoding :** How to encode a message when code of characters are known is illustrated below.

**Example :** Using the code given by the following table encode the words (i) *sam*, (ii) *year*.

(i) <i>treaty</i>	Character : o a e n r t y
	Code : 1100 1101 01 1110 10 0 1111

**Sol.:** To encode a word we just go on writing the codes of the characters in the word serially.

(i) '*sam*' is coded as code of *s* then code of *a*, then code of *r* and lastly code *n*.

01 1101 10 1110

(ii) '*year*' is coded as *y + e + a + r + y*

i.e. 1111 01 1101 10

(iii) *treaty* is coded as *t + r + e + a + t + y*

i.e. 0100 1110 10 1111

**Decoding :** Now we shall consider the reverse problem i.e. of decoding a given message in binary system.

**Example 1 :** If the codes of the characters are as given below,

Character : u c f o e d
Code : 00 010 011 10 110 111

**Sol.:** The first bit is 1. From the table we find that the first character must be 0, *e*, *d* as the code of these characters start with 1.

The second bit is 1. The character must be *e* or *d* because 11 does not occur in the code of 0. Since the third bit is 1, the character is *d*.

Now, the next bit is 1. Hence, the character must be again *o* or *a* or *d*.

Since the next bit is 0, the character is *o*.

Now the next bit is 1. Hence, as before the character again can be *o*, *e*, *d*.

The next bit is 1. Hence, the character can be *e*, *d*.

The next is 0. Hence, the character is *e*.

∴ The message is *doe*.

The discussion can be summarised as follows.

1 → o, e, d	11 → e, d
111 → d,	1 → o, e, d
10 → 0	1 → o, e, d
11 → e, d	110 → e.

**Example 2 :** Using the Huffman tree given in Fig. 14.15 decode the message  
0 10 100 110 1111 0 110

Sol. : From the tree, we first prepare the table of the Huffman code of the characters.

Character	: u	c	f	o	e	d
Code	: 00	010	011	10	110	111

As explained in details above since the first digit is 0, the first character is u, c or f.  
Second digit is 1. Hence, c or f.  
Third digit is 0. Hence c.  
Fourth digit is 1. Hence, o, e or d.  
Fifth digit is 0. Hence, o.  
Sixth digit is 0. Hence, u, c or f.  
Seventh digit is 1. Hence, c or f.  
Eighth digit is 1. Hence, f.  
Ninth digit is 0. Hence, u, c or f.  
Tenth digit is 1. Hence, c or f.  
Eleventh digit is 1. Hence, f.  
Twelfth digit is 1. Hence, o, e or d.  
Thirteenth digit is 1. Hence, e or d.  
Fourteenth digit is 0. Hence, e.  
The last sequence is 110 again. Hence, e.  
Hence, the message is 'coffee'.

This can be summarised as

0 → u, c, f	01 → c, f	010 → c
1 → o, e, d	10 → o	0 → u, c, f
01 → c, f	011 → f	0 → u, c, f
01 → c, f	011 → f	1 → o, e, d
11 → e, d	110 → e	110 → e

### EXERCISE - II

1. Using the table given below

Character	:	A	E	N	R	T
Code	:	1101	01	1110	10	00

decode the message

- (a) 00100101, (b) 1110011110110, (c) 001001110100.

[Ans. : (a) TREE, (b) NEAR, (c) TREAT.]

2. Using the table given in the above Ex. 1, encode the following message.

- (i) TEAR, (ii) TENT, (iii) RENT.

[Ans. : (i) 0001 110110, (ii) 0001 111000, (iii) 1001 111000.]

3. Using the Huffman tree given in Fig. A find the Huffman code for the characters.

Character	:	R	M	A	N	O	D
Code	:	00	010	011	10	110	111

4. Using the tree (Fig. A) encode each of the following words.

- (a) ROAD, (b) DOOR, (c) RAMA

[Ans. : (a) 00 100 011 111, (b) 111 110 110 00

(c) 00 011 010 011]

5. Using the tree (Fig. A) decode the following messages.

- (a) 00 110 010 011 10, (b) 10 011 10 111 011

(c) 10 110 00 010 011 10

(b) NANDA,

[Ans. : (a) ROMAN,

(c) NORMAN.]

6. Using the Huffman tree given in Fig. B, find the Huffman code for the characters.

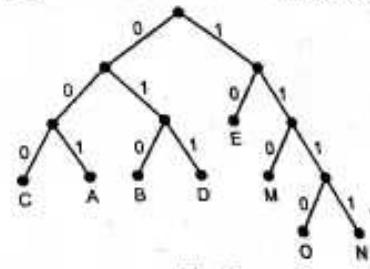


Fig. B

Character	:	C	A	B	D	E	M	O	N
Code	:	000	001	010	011	10	110	1110	1111

7. Using the above tree (Fig. B) encode each of the following words.

- (a) BEED, (b) MADE, (c) DEEMED

[Ans. : (a) 010 1010 011, (b) 110 001 011 10, (c) 011 10 10 110 10 011.]

8. Using the above tree (Fig. B) decode the following messages.

- (a) 000 001 1111 10, (b) 110 111 011 10 011, (c) 1111 1110 011 10.

[Ans. : (a) CANE, (b) MOOD, (c) NODE.]

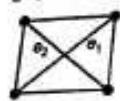


## Planar Graphs

### 1. Introduction

We know that a planar graph is a graph that can be drawn on the plane of paper without crossing any two edges. In this chapter we shall study some properties of planar graphs and the colouring problem. The planar graphs are useful in designing and printing of integrated circuits.

**Definition 1 :** A graph (or a multigraph) that can be drawn on a plane (or on a sphere) without crossing edges is called a **planar graph**. Clearly, the graphs on the right are planar graphs. (The second graph is isomorphic to the first).



The graph drawn in the Fig. 15.1 (a) looks like a non-planar graph. Its edges  $e_1$  and  $e_2$  look like crossing each other.

But with little imagination, it can be redrawn as on the right such that the edges  $e_1$  and  $e_2$  do not cross each other. Thus, the graph is a planar graph.

Two more illustrations are given below. The graphs [15.3 (a) and 15.4 (a)] on the left can be redrawn as on the right [15.3 (b) and 15.4 (b)], so that the edges do not cross. In the Fig. 15.4 (a), if we lift the triangle  $abc$  from the plane of the paper and put the point  $b$  below  $a$ , we get the Fig. 15.4 (b).

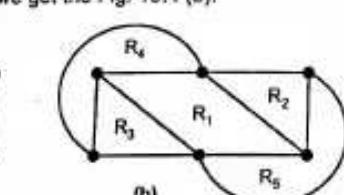
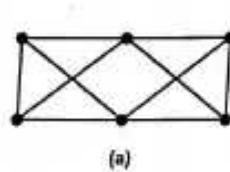


Fig. 15.3

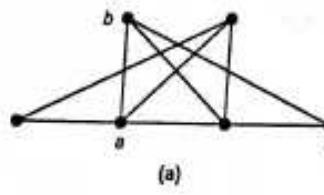


Fig. 15.4

It maybe noted that trees are important class of planar graphs.

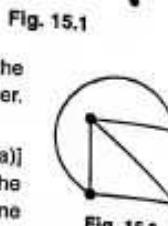
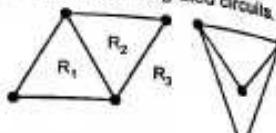


Fig. 15.1

Fig. 15.2

### 2. Maps and Regions

A particular planar representation of a graph is called a map. A map is said to be connected if its graph is connected. (i.e. has cycles)

A given connected map (with cycles) divides the plane into various regions. The connected map shown in Fig. 15.5 divides the plane into two regions  $R_1$  and  $R_2$ . The region  $R_1$  is bounded by the edges  $e_1$ ,  $e_2$ , and  $e_3$ , while the region  $R_2$  is unbounded. The graph shown in Fig. 15.6 is a tree and as such has no cycles. It does not divide the plane. It has only one unbounded region  $R$ .



Fig. 15.5

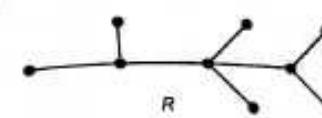


Fig. 15.6

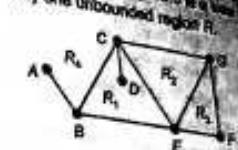


Fig. 15.7

The connected map on the right divides the plane into four regions. It has seven vertices and nine edges. The border of each region of a map consists of edges. The edges of some regions form cycles. But some edges do not form cycles. For example, in the above diagram the borders of the regions  $R_2$  and  $R_3$  are cycles. But the border of  $R_1$  is not a cycle (although it is a closed path) while  $R_4$  is unbounded.

#### Degree of a Region

**Definition :** The degree of a region  $R$  is defined as the length (the number of edges) of the boundary of the region. It is denoted as  $\deg(R)$ . Sometimes the boundary is a cycle. If not, some edges may occur twice in the path as for the region  $R_1$ .

The following theorem state the relation between the sum of degrees of the regions and the number of edges. The theorem is analogous to the theorem for vertices.

**Theorem :** The sum of the degrees of all the vertices of all the regions of a map is equal to twice the number of edges i.e.  $\sum d(v_i) = 2e$ .

**Proof :** Each edge  $e$  of a map either borders two regions (See above Fig. 15.7) or is contained in a region like the edge  $(CD)$  in the region  $R_1$ . If an edge is a border, it will be counted twice for two regions. If it is contained in a region it will be again counted twice in any path along the border of that region.

Hence, the sum of the degrees of all the vertices of all the regions in a map is equal to twice the number of edges of the map.

**Example 1 :** Can we have a map such that the sum of the all degrees of the regions is odd?

**Sol.:** Since the number of edges is an integer  $n$  and the sum of the degrees of the regions is  $2n$ , this number cannot be odd.

**Example 2 :** Verify the above theorem for the above Fig. 15.7.

**Sol.:** The degrees i.e. the number of edges forming the boundaries of the regions are :  $\deg(R_2) = 3$ ,  $\deg(R_3) = 3$ ,  $\deg(R_1) = 5$  and  $\deg(R_4) = 7$ . Sum = 18. Since there are nine edges the theorem is verified.

[The degree of  $R_1$  is 5 because in the path  $(B, C, D, C, E, B)$  the edge  $CD$  occurs twice. For the same reason degree of  $R_4$  is 7  $(A, B, C, G, F, E, B, A)$ .]

**3. Euler's Formula**

In connected planar graphs considered above, let  $V$  denote the number of vertices,  $E$  denotes the number of edges and  $R$  denote the number of regions then observe the following.

In the Fig. 15.1,  $V = 4$ ,  $E = 5$  and  $R = 3$  and  $V - E + R = 4 - 5 + 3 = 2$ .

In the Fig. 15.3,  $V = 6$ ,  $E = 10$  and  $R = 6$  and  $V - E + R = 6 - 10 + 6 = 2$ .

In the Fig. 15.4,  $V = 6$ ,  $E = 9$  and  $R = 5$  and  $V - E + R = 6 - 9 + 5 = 2$ .

(Verify this in Fig. 15.5 and 13.7)

But this is not an accident. The well-known Mathematician Euler proved the concerned theorem.

**Euler's Theorem :** In a connected map  $M$  with  $V$  vertices,  $E$  edges and  $R$  regions

$$V - E + R = 2.$$

**Proof :** Suppose the connected map  $M$  consists of a single vertex  $P$ . Then we have  $V = 1$ ,  $E = 0$ , and  $R = 1$ .

$$\therefore V - E + R = 1 - 0 + 1 = 2$$

We can build a connected map  $M$  from a single vertex (*i*) by adding a new vertex and connecting it to the existing vertex by an edge which does not cross any existing edge or (*ii*) by adding an edge by connecting existing two vertices which does not cross any existing edge.

This is shown in the Fig. 15.8.

(i) In the first case where (in an intermediate stage) a vertex  $Q_2$  is added and connected to  $Q_1$ .  $V$  increases by 1 and  $E$  increases by 1 but  $R$  does not change.

Hence,  $V - E + R$  remains the same [See Fig. 15.8 (a) or (a')].

(ii) In the second case where (in an intermediate stage) the vertices  $Q_1$  and  $Q_2$  are connected,  $E$  is increased by 1,  $R$  is increased by 1 but  $V$  does not change.

∴ Hence,  $V - E + R$  remains the same. [See Fig. 15.8 (b) or (b')]

Thus,  $V - E + R = 2$ .

**Example :** A connected planar graph has 10 vertices each of degree 3. In how many regions does a representation of this planar graph split the plane. (M.U. 2012)

**Sol. :** We know that if in a connected planar graph there are  $V$  vertices,  $E$  edges and  $R$  regions, then

$$V - E + R = 2.$$

Now, the sum of the degrees of all regions is equal to twice the number of edges.

$$\sum d(v_i) = 2E$$

$$\text{But here } \sum d(v_i) = 30 \quad \therefore 30 = 2E \quad \therefore E = E = 15$$

$$\therefore V - E + R = 2 \text{ gives } 10 - 15 + R = 2 \quad \therefore R = 7$$

∴ There will be seven regions.

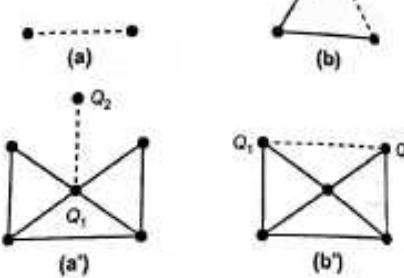


Fig. 15.8

**Theorem :** If  $G$  is a simple connected planar graph with  $v$  vertices and  $e$  edges then

$v \geq 2$  then  $3v - 6 \geq e$ .

**Proof :** Let us first note that the theorem is not true for  $K_1$  where  $v = 1$  and  $e = 0$  and for  $K_2$  where  $v = 2$  and  $e = 1$ . Hence, the condition  $v \geq 3$ .

Let  $r$  be the regions in the planar representation of the graph. Then by Euler's theorem,  $v - e + r = 2$ .

But the sum of the degrees of all regions is equal to  $2e$  by the theorem, page 15-3.

But each region has a degree three or more. Hence,

$$2e \geq 3r \quad \therefore \frac{2e}{3} \geq r$$

Now, from (1) putting the value of  $r$ , we get

$$v - e + \frac{2e}{3} \geq 2 \quad \therefore 3v - e \geq 6 \quad \therefore 3v - 6 \geq e$$

**Corollary 1 :** The graph shown in Fig. 15.5 is non-planar.

**Proof :** For the graph shown in Fig. 15.9,  $v = 5$ ,  $e = 10$ .

$$3v - 6 = 9$$

Hence,  $3v - 6 \geq e$ .

Hence, by the above theorem  $K_5$  is not a planar graph. ( $K_5$  is known as Kuratowski's first graph. The above figure shows that it is impossible to draw the edges  $e_9$  and  $e_{10}$  without crossing each other or other edges.)

The condition in the above theorem  $3v - 6 \geq e$  is necessary but sufficient. This means if the graph is planar then  $3v - 6 \geq e$ . But we can have the condition satisfied but the graph is not planar. See the graph shown in Fig. 15.10.

In this graph we have  $v = 6$  and  $e = 9$ .

$$\therefore 3v - 6 = 12$$

$$\therefore 3v - 6 \geq e$$

satisfied. Yet the graph is not a planar.

This graph  $K_{3,3}$  is known as Kuratowski's second graph.

**Example 1 :** Verify Euler's Formula for the following graphs.

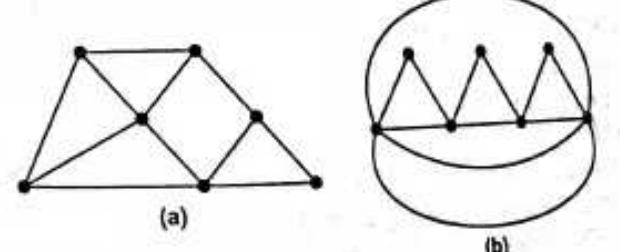


Fig. 15.11

(15-5)

Sol.: We show first show the different regions of the graphs and then verify the formula.

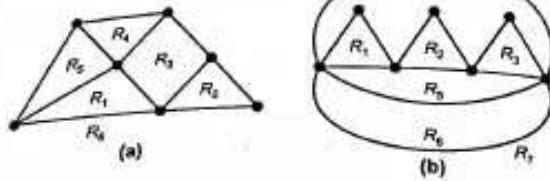


Fig. 15.12

$$(a) V=7, R=6, E=11 \\ V-E+R = 7-11+6=2 \\ \therefore$$

$$(b) V=7, R=7, E=12 \\ V-E+R = 7-12+7=2 \\ \therefore$$

**Example 2:** A connected planar graph has seven vertices and the sum of the degrees of these regions is eighteen. Find the number of edges and the number of regions. Draw the graph.

Sol.: If  $e$  is the number of edges by the above theorem (page 15-3),

$$\text{Sum of the degrees} = 2e = 18$$

$$\therefore e = E = 9. \quad \text{But } V = 7.$$

By Euler's formula,

$$V-E+R = 2$$

$$7-9+R = 2 \quad \therefore R = 4$$

There are nine edges and four regions and seven vertices.

**Example 3 :** Draw a planar graph which has 7 regions and 5 vertices.

Sol.: Since the graph is a planar it satisfies Euler's formula. If  $E$  is the number of edges then by Euler's formula

$$V-E+R = 2 \quad \text{But } V=5, R=7$$

$$\therefore 5-E+7=2 \quad \therefore E=10$$

Since  $V=5$  draw a pentagon and then add 5 more edges as shown in Fig. 15.14.

For a long time mathematician were trying to find a criteria to distinguish between planar and non-planar graphs. The problem was solved by polish mathematician Kuratowski in 1930.

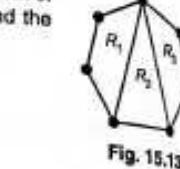


Fig. 15.13

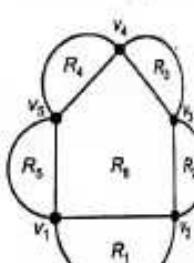


Fig. 15.14

To check whether the given graph is planar, we try to "remove" the edges which cross other edges for maximum number of times. We try to draw such edges from outside the graph as per the steps.

**Example 1 :** State with reasons which of the graphs shown in Fig. 15.15 are planar graphs.

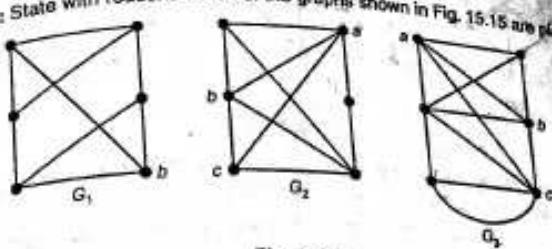


Fig. 15.15

Sol.: (i) The graph  $G_1$  is a planar graph. It can be redrawn as shown in the Fig. 15.16 (a) by taking the edge  $(a, b)$  outside the square.

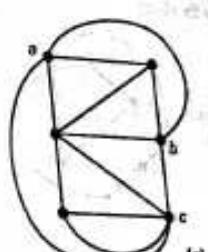
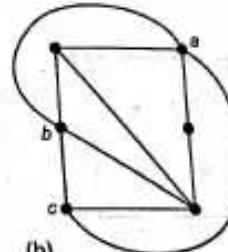
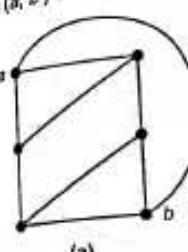


Fig. 15.16

(ii) The graph  $G_2$  is also a planar graph. It can be redrawn as shown in Fig. 15.16 (b) by taking two edges  $(a, b)$  and  $(a, c)$  outside the square.

(iii) The graph  $G_3$  is a planar graph as it can be redrawn as shown in the Fig. 15.16 (c) by taking the edges  $(a, b)$  and  $(a, c)$  outside the square.

**Example 2 : Three Utility Problem :** There are three houses  $H_1, H_2, H_3$  which are to be connected to three utility centres  $E$  (electricity),  $G$  (gas) and  $W$  (water) by means of pipes. Is it possible to have connections without crossing of pipes?

Sol.: If we denote houses by  $H_1, H_2, H_3$  and utility centres  $U_1, U_2, U_3$  then the houses can be connected with the utility centres as shown in the Fig. 15.17.

But this graph is non-planar. Hence, it is not possible to connect the houses without crossing of pipes.

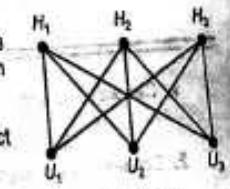


Fig. 15.17

**Example 3 :** Which of the following graphs are planar graphs.

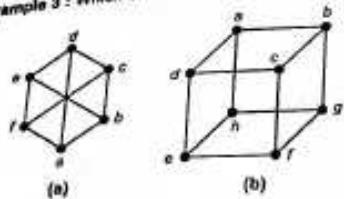


Fig. 15.18

**Sol. :** (a) The graph in Fig. 15.18 (a) is not planar. Even if we take the edges  $ad$  and  $fc$  outside  $P_6$ , the edges intersect.

(b) The graph  $G_2$  is a planar graph because it can be drawn on a plane such that the edges do not cross as shown in Fig. 15.19 (b).

(c) The graph  $G_3$  can be redrawn with the positions of the vertices  $v_2$  and  $v_5$  interchanged as shown in figure below. Since the edges do not cross each other,  $G_3$  is a planar graph as shown in Fig. 15.19 (c).

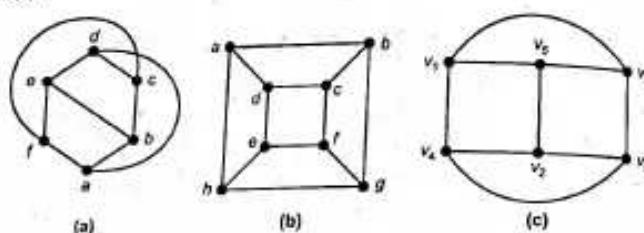


Fig. 15.19

**Example 4 :** A connected planar graph has 9 vertices having degrees 2, 2, 2, 3, 3, 3, 4, 4 and 5. How many edges are there in the graph ?

(M.U. 2002, 06, 07, 11)

**Sol. :** By the theorem proved above [page 15-3]

$$\sum d(v_i) = 2e.$$

$$\text{But } \sum d(v_i) = 2 + 2 + 2 + 3 + 3 + 3 + 4 + 4 + 5 = 28$$

$$\therefore 2e = 28 \quad \therefore e = 14.$$

### EXERCISE - I

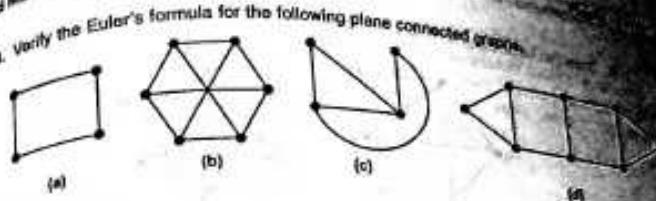
1. Can we have a planar graph with 9 vertices, 12 edges and 6 regions ? Why ?

[ Ans. : No.  $V - E + R = 3 \neq 2$  ]

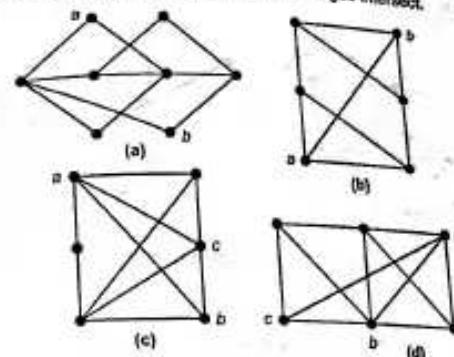
2. Can we have a simple connected planar graph with 4 vertices and 7 edges ? Why ?

[ Ans. : No.  $30 - 6 = 6 \not\geq e = 7$  ]

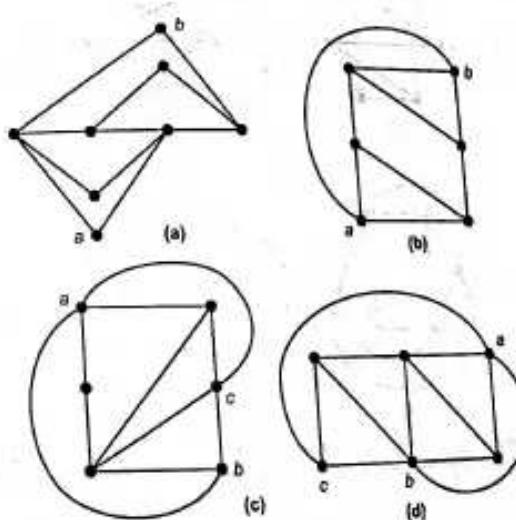
3. Verify the Euler's formula for the following plane connected graphs.



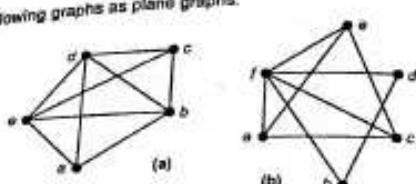
4. Draw the following planar graphs, so that no two edges intersect.



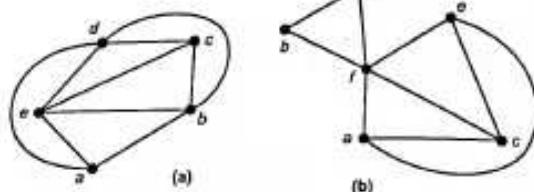
[Ans. 1]



5. Draw the following graphs as plane graphs.

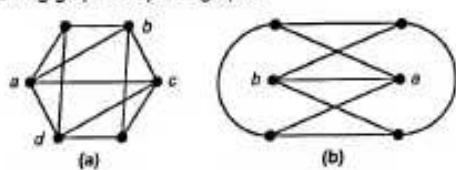


[Ans. :

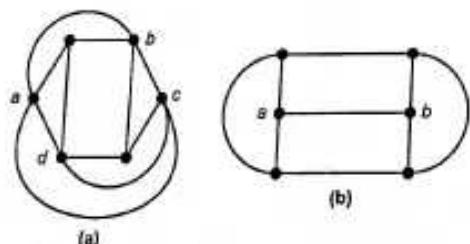


(Hint : In the graph (b) the triangle fbd is 'shifted' to the new position.) ]

6. Draw the following graphs as plane graphs.



[Ans. :



(Hint : In the graph (b) the vertex (a) is 'shifted' to the position of (b) and vice versa.) ]

### Graph Colouring

You have seen maps on a plane or a sphere coloured to show different nations or different areas within a nation. Have you thought over the question - how many colours are required to colour a map in such a way that two adjacent states will not have the same colour? This is a problem in graph theory. Suppose we want to colour the following map.

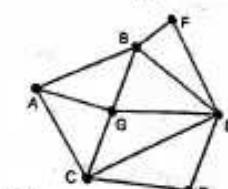
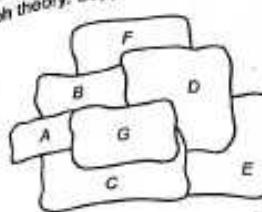


Fig. 15.20

We can represent the states by vertices and connect these vertices by edges if the corresponding states have common borders. Since A and B have common borders there will be an edge between A and B. So there will be edges between A and G; A and C; B and F; B and D; B and G; C and G; C and E; D and F; D and G; D and E and we will get a graph as shown above.

A colouring problem of a simple graph is to assign colours to vertices in such a way that no two adjacent vertices will have the same colour. Obviously if a graph has  $n$  vertices, it can be coloured in this way with  $n$  colours. But what if we want the least number of colours? In Fig. 15.20, the vertices A, B, G are adjacent as they form a triangular subgraph. Hence, minimum three colours will be required to colour a graph. But will three colours be sufficient? The vertices A, B, D and C can be coloured by three such that two adjacent vertices will not have the same colour. But since no vertex G is adjacent to all the four vertices A, B, C, D, if we use any of the three colours the condition will not be satisfied. We need fourth colour for the vertex G. This shows at least four colours are required to colour a graph.

In the Fig. 15.21, we have shown one such colouring (i.e. no adjacent vertices do not have the same colours). Here B stands for Blue, G for Green, R for Red and Y for yellow.

The map-colouring problem had occupied the minds of mathematicians for a long time since mid-nineteenth century. It was conjectured that four colours are sufficient to colour any map. The problem was ultimately solved by two American mathematicians in 1976 using exhaustive computer analysis. They proved that at least four colours are required to colour a map.

The problem of finding the minimum number of colours required to paint any given graph is not solved.

**Definition 1 :** An assignment of colours to the vertices of a graph  $G$  such that no two adjacent vertices have the same colour is called colouring of  $G$ , (or vertex colouring of  $G$ ).

**Definition 2 :** If a graph can be coloured by  $n$  colours it is called  $n$  colourable.

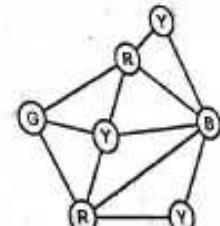


Fig. 15.21

**Definition 3 :** The minimum number of colours required to colour a graph is called its chromatic number of  $G$  and is denoted by  $\chi(G)$ . If the chromatic number of a graph is  $k$  then the graph is said to be  $k$ -chromatic.

**Example :** Find  $\chi(G)$  for  $K_6$ ,  $K_{10}$  and in general  $K_n$  where  $K_n$  denotes a graph with  $n$  vertices and in which each vertex is connected to the other vertices.   
 Sol. : Since in  $K_6$  each vertex is adjacent to every other vertex and since there are six vertices (minimum) six colours will be required to paint a  $K_6$  graph. Similarly, ten colours will be required to colour a  $K_{10}$  graph and  $n$  colours will be required to colour a  $K_n$  graph.

$$\therefore \chi(K_6) = 6, \chi(K_{10}) = 10, \chi(K_n) = n.$$



Fig. 15.22

### 6. Rules of Chromatic Numbers

There is no easy way to find the chromatic number of a graph i.e.,  $\chi(G)$ . However, the following results are useful to find  $\chi(G)$ .

1. A graph consisting of isolated vertices is 1-chromatic. (If we want to paint a group of islands one colour is sufficient)
2. If a graph is  $k$ -chromatic then  $k \leq v$  where  $v$  is the number of vertices of  $G$ .
3. If  $K_n$  is graph with  $n$  vertices each connected to another, then  $k = n$  (See above example)
4. If a subgraph of  $G$  requires  $m$  colours then  $\chi(G) \geq m$ .
5. If the degree of a vertex of  $G$  is  $d$  then at most  $d$  colours are required to colour vertices adjacent to it.

For the graph shown in the Fig. 15.23 the vertex  $v_5$  is of degree 3. Observe that depending upon the nature of the graph at most 3 colours will be required to paint the vertices [one for  $v_5$ , second for (1) and (3) and third for (2)].

6. For a cycle graph of  $n$  vertices either  $\chi(G) = 2$  or  $\chi(G) = 3$  according as  $n$  is even or odd. (See the following figures)

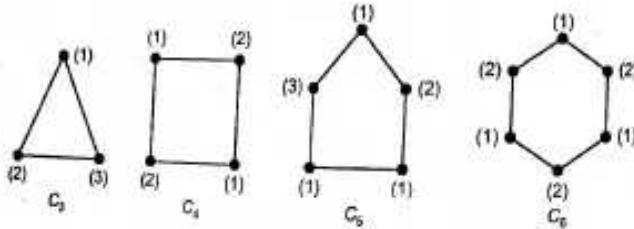


Fig. 15.24

### 7. Welch-Powell Algorithm

This algorithm helps us to find the number of colours required to paint a given graph. But it may be noted that it does not always give us the minimum number of colours required.

1. Order the vertices in decreasing order of degrees. (This order may not be unique since more than one vertices may have the same degree).
2. Assign colour  $C_1$  to the first vertex and then assign the colour  $C_1$  to each vertex which is not adjacent to this vertex.
3. Repeat 2 with a colour  $C_2$  for uncoloured vertices.
4. Repeat 3 with a colour  $C_3$  and then a fourth colour  $C_4$  and so on until all vertices are coloured.

**Example 1 :** Use the Welch-Powell algorithm to colour the following graph. Also find the minimum number of colours required.

Sol. : We first find the degrees of the vertices and write them in decreasing order of degrees as follows.

Vertex	$v_5$	$v_1$	$v_2$	$v_3$	$v_4$
Degree	4	3	3	3	3
Colour	$a$	$b$	$c$	$b$	$c$

The vertex of highest degree is  $v_5$ . Assign the colour  $a$  to it. All other vertices are adjacent to it. So the same colour cannot be assigned to any other vertex. The next vertex is  $v_1$ . Assign second colour  $b$  to  $v_1$ . The vertices  $v_2$  and  $v_4$  are adjacent to it but  $v_3$  is not. Assign the same colour  $b$  to  $v_2$ .

Now, the next vertex in order of magnitude of the degrees is  $v_2$ . Assign the third colour  $c$  to  $v_2$ . Since  $v_4$  is the last vertex not adjacent to it assign the colour  $c$  to it.

Since, the three vertices  $v_1$ ,  $v_2$ ,  $v_5$  (and also  $v_2$ ,  $v_3$ ,  $v_5$ , ...) are connected at least three colours are required to colour  $G$ .

$$\therefore \chi(G) = 3.$$

**Example 2 :** Use the Welch-Powell algorithm to colour the graph shown in Fig. 15.26. Also find the chromatic number of  $G$ .

Sol. : We first find the degrees of the vertices and write them in decreasing order of the degrees.

Vertex	$v_1$	$v_5$	$v_2$	$v_6$	$v_3$	$v_4$
Degree	4	4	3	3	2	2
Colour	$a$	$b$	$b$	$c$	$c$	$a$

$v_1$  is the vertex with highest degree. Assign colour  $a$  to  $v_1$ . Now  $v_3$ ,  $v_5$ ,  $v_6$ ,  $v_2$  are adjacent to it.  $v_4$  is not adjacent. So assign the same colour  $a$  to  $v_4$ . Now come to the next highest vertex  $v_5$ . Assign the colour  $b$  to  $v_5$ . Now  $v_3$ ,  $v_1$ ,  $v_6$  and  $v_4$  are adjacent to it. But  $v_2$  is not adjacent to it. So assign the same colour  $b$  to  $v_2$ . Now come to the next highest vertex (which is not assigned any colour) viz.  $v_6$ . Assign another colour  $c$  to  $v_6$ . The only remaining vertex is  $v_3$ . Since it is not adjacent to  $v_6$ , assign the same colour  $c$  to  $v_3$ .

Since the three vertices  $v_1$ ,  $v_2$ ,  $v_6$  (so are  $v_1$ ,  $v_3$ ,  $v_5$  and  $v_1$ ,  $v_5$ ,  $v_6$ ) are connected at least three colours are required to colour  $G$ .

$$\text{Hence, } \chi(G) = 3.$$

**Example 3 :** Use Welch-Powell algorithm to colour the graph shown in Fig. 15.27. Also find the chromatic number of  $G$ .

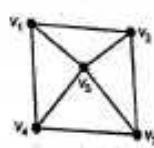


Fig. 15.25

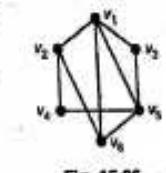


Fig. 15.26

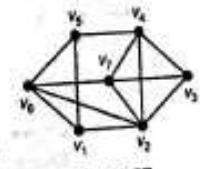


Fig. 15.27

### Applied Mathematics - IV

(15-13)

**Planar Graphs**

Sol.: We first find the degrees of the vertices and write them in decreasing order as follows.

Vertex	$v_2$	$v_7$	$v_8$	$v_4$	$v_3$	$v_5$	$v_1$
Degree	5	4	4	4	3	3	3
Colour	a	b	c	d	c	a	b

Since  $v_2$  has the highest degree assign a colour a to it. Since the vertices  $v_1, v_8, v_7, v_4$  and  $v_3$  are adjacent to it, leave them. Since  $v_5$  is not adjacent so assign a colour a to  $v_5$ . Next highest vertex is  $v_1$ . Assign colour b to it. Vertices  $v_2, v_4, v_3, v_6$  are adjacent to it,  $v_1$  and  $v_6$  are not adjacent.  $v_6$  is already assigned a colour. Hence, assign colour b to  $v_1$ . Next highest vertex is  $v_8$ . Assign a colour c to it. Vertices  $v_1, v_2, v_5$  and  $v_7$  are adjacent to it. But  $v_3$  and  $v_4$  are not adjacent to it. Assign the colour c to  $v_3$ . Now, assign the colour d to the last vertex  $v_4$ .

Since,  $v_2, v_3, v_4, v_6$  are connected to each other, four colours are required.

$$\therefore \chi(G) = 4.$$

**Example 4 :** Write Welch-Powell algorithm to determine chromatic number of the graph shown in Fig. 15.28.

Sol.: We first find the degrees of the vertices and write them in decreasing order of their degrees.

Vertex	A	F	H	B	C	D	E	G
Degree	4	4	4	3	3	3	3	2
Colour	a	a	b	b	c	a	a	a

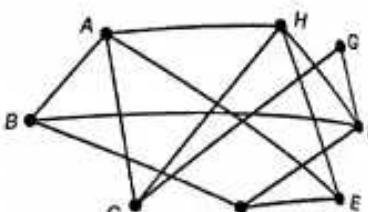


Fig. 15.28

A is the vertex of the highest degree. Assign a colour a to it.

Since vertices D, E, F, G are not adjacent to it, assign the same colour a to them.

The next highest vertex is H. Assign a colour b to it. Since the vertex B is not adjacent to it assign the same colour b to it.

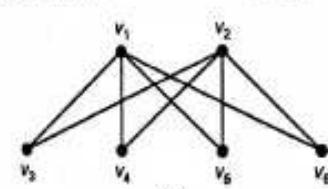
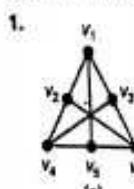
The next highest vertex is C (which is adjacent to both A and H) assign a different colour c to it.

Thus, three different colour are required.

$$\therefore \chi(G) = 3.$$

### EXERCISE - II

Use the Welch-Powell algorithm to colour the following graphs. Also write down  $\chi(G)$ .



Ans. : (a) Vertex	$v_1$	$v_2$	$v_3$	$v_4$	$v_5$	$v_6$
Degree	3	3	3	3	3	3
Colour	a	b	b	a	b	a

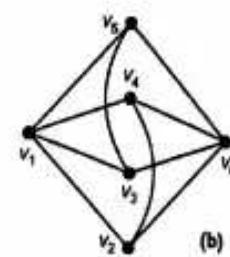
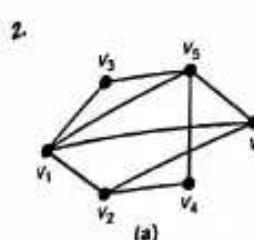
### Applied Mathematics - IV

(15-14)

**Planar Graphs**

(b) Vertex	$v_1$	$v_2$	$v_3$	$v_4$	$v_5$	$v_6$
Degree	4	4	2	2	2	2
Colour	a	a	b	b	b	b

$$\chi(G) = 2]$$



[Ans. : (a) Vertex	$v_1$	$v_5$	$v_2$	$v_3$	$v_4$	$v_6$
Degree	4	4	3	3	2	2
Colour	a	b	b	c	c	a

(b) Vertex	$v_1$	$v_3$	$v_4$	$v_6$	$v_2$	$v_5$
Degree	4	4	4	4	3	3
Colour	a	b	c	a	b	c

$$\chi(G) = 3]$$

### EXERCISE - III

#### Theory

- Define the following terms.
  - (1) Planar Graph, (M.U. 2004, 06, 07) (2) Map, (3) Connected Map
  - (4) Degree of a Region, (5) Colouring of a graph,
  - (6) n-colourable graph, (7) Chromatic number.
- Prove that the sum of the degrees of all regions of a map is equal to twice the number of edges.
- State and prove Euler's theorem about the relation between the vertices, edges and regions of a connected map.
- Prove that if  $G$  is a simple connected planar graph with  $v$  vertices and  $e$  edges then  $3v - 6 \geq e$ , ( $v \geq 3$ ).
- Explain graph colouring problem.
- State Welch-Powell algorithm.



## CHAPTER 16

# Some Algebraic Structures

### 1. Introduction

In this chapter we shall define groups, rings, fields and prove some of their elementary properties. These concepts are as basic to Modern Mathematics as the operations of addition and multiplication are to school mathematics. In fact the basic operations in arithmetic are generalised in Modern Mathematics to abstract level.

### 2. Binary Operation

(a) Definition : Let  $A$  be a non-empty set. A function  $f : A \times A \rightarrow A$  is called a **binary operation**.

#### Example of Binary Operation

It should be noted that since a binary operation is a function, one and only one element of  $A$  is assigned to one ordered pair of  $A \times A$ . Further, we shall denote binary operations by  $*$  or  $(+)$  instead of  $f$ . Since, a binary operation is a function to each  $(a, b) \in A \times A$ , there exists a unique element  $a * b \in A$ . We describe this property by saying that  $A$  is closed under  $*$ .

Example 1 : Let  $A = \mathbb{Z}$  and  $a * b$  be  $a + b$ . Then  $*$  is a binary operation on  $\mathbb{Z}$ .

Example 2 : Let  $A = \mathbb{Z}^+$  and  $a * b$  be  $a - b$ .

Then  $*$  is not a binary operation on  $\mathbb{Z}^+$  since  $a - b$  may not be an element of  $A$  for some  $a, b \in A$ . e.g.  $3 * 7 = 3 - 7 = -4$  does not belong to  $\mathbb{Z}^+$ .

Example 3 : Let  $A = R$  and  $a * b$  be  $a/b$ .

Then  $*$  is not a binary operation on  $R$  since  $a/b$  may not be an element of  $R$  for some  $a, b \in A$ . e.g.  $5 * 0 = 5/0 \notin A$ .

However, if  $A = R - \{0\}$  then  $a * b = a/b$  is a binary operation.

Example 4 : Let  $L$  be a lattice and  $a * b$  be  $a \wedge b$  (GLB of  $a, b$ ).

Then  $a * b$  is a binary operation because for every ordered pair  $a, b$  of  $L$ , there exists a unique  $a \wedge b$ .

Example 5 : Let  $L$  be a lattice  $a * b$  be  $a \vee b$  (LUB of  $a, b$ ).

Then  $a * b$  is a binary operation for the reason given above.

#### (b) Identity and Inverse

Definition : Given a non-empty set  $A$  and a binary operation  $\oplus$  if there is an element  $e \in A$ , such that for every  $a \in A$ ,  $a \oplus e = e \oplus a = a$ , then  $e$  is called the **Identity element** for the operation  $\oplus$ .

For example, in the set of real numbers, zero is identity element for usual addition because  $a + 0 = 0 + a = a$  for every  $a \in R$ .

In the set of real numbers, unity is identity element for usual multiplication because  $a \times 1 = 1 \times a = a$  for every  $a \in R$ .

### 16-2

#### Some Algebraic Structures

**Definition :** Given a non-empty set  $A$  and a binary operation  $\otimes$  if  $A$  has an identity element  $e$  and for any two elements  $a, b \in S$ ,  $a \otimes b = b \otimes a = e$ , then  $b$  is called the **inverse** of  $a$  and is denoted by  $a^{-1}$ .

**Example :** If a binary operation in  $\mathbb{Q}^+$  (set of positive rational numbers) is defined by  $a \otimes b = ab/2$  then  $2$  is an identity and  $4/a$  is the inverse of  $a$  under  $\otimes$ .

State true or false with proper justification.

Sol. : If  $e$  is an identity element under  $\otimes$ , we must have

$$a \otimes e = e \otimes a = a$$

But by data,  $a \otimes e = \frac{ae}{2}$

$$\therefore \frac{ae}{2} = a \quad \therefore e = 2 \text{ is identity.}$$

If  $b$  is the inverse of  $a$ , we must have

$$a \otimes b = b \otimes a = e \quad (\text{identity})$$

But by data,  $a \otimes b = \frac{ab}{2}$

$$\therefore \frac{ab}{2} = e \quad \therefore b = \frac{4}{a} \quad \therefore a^{-1} = \frac{4}{a}$$

Hence, the statement is true.

### 2. Properties of Binary Operations

#### 1. Commutativity

**Definition :** A binary operation on set  $A$  is called **commutative** if

$$a * b = b * a \quad \text{for all element } a \text{ and } b \text{ of } A.$$

**Example 1 :** The binary operation of usual addition in  $\mathbb{Z}$  is commutative?

**Example 2 :** The binary operation of usual subtraction (division) on  $\mathbb{Z}$  is not commutative.

#### 2. Associativity

**Definition :** A binary operation  $*$  on a set  $A$  is said to be **associative**, if

$$a * (b * c) = (a * b) * c \quad \text{for all } a, b, c \in A.$$

**Example 1 :** Is the binary operation of usual addition on  $\mathbb{Z}$  associative?

Sol. : Because  $a + (b + c) = (a + b) + c$  for all  $a, b, c \in \mathbb{Z}$ , the operation of addition is associative.

**Example 2 :** Show that the relation  $*$  given by  $a * b = a^b$  on the set of natural numbers is a binary operation. Is it associative?

(M.U. 2005, 07)

Sol. : If  $a$  and  $b$  are natural numbers, then  $a^b$  is also a natural number.

Hence,  $a * b$  is binary.

Since,  $a^{b^c} \neq a^{c^b}$ , the operation is not associative.

**Example 3 :** Is the binary operation of usual subtraction (division) on  $\mathbb{Z}$  associative? Commutative?

Sol.: Because  $a - (b - c) = (a - b) - c$ , e.g.,  $5 - (6 - 4) = 5 - 2 = 3$  and  $(5 - 6) - 4 = -1 - 4 = -5$ , the usual subtraction is not associative on  $\mathbb{Z}$ .

Also  $5 - 8 \neq 8 - 5$ .

It is not commutative on  $\mathbb{Z}$ .

**Example 4 :** Is the operation  $*$  on  $A = \{a, b, c\}$  defined by the adjoining table associative?

Sol.: Although  $(a * c) * b = c * b = a$  and  $a * (c * b) = a * a = a$  but  $a * (b * c) = a * a = a$  and  $(a * b) * c = a * c = c$ , the operation  $*$  is not associative.

*	a	b	c
a	a	a	c
b	a	b	a
c	c	a	c

**Example 5 :** Is the operation  $a * b = a \times |b|$ , associative on  $R$ ?

Sol.: Because  $(a * b) * c = (a \times |b|) * c = a \times |b| \times |c|$  and  $a * (b * c) = a * (b \times |c|) = a \times |b \times |c|| = a \times |b| \times |c|$

We see that  $*$  is associative. (But note that  $*$  is not commutative).

**Example 6 :** Is the operation  $a * b = ab / 5$  on  $R$  associative?

Sol.: Because  $(a * b) * c = (ab / 5) * c = abc / 25$  and  $a * (b * c) = a * (bc / 5) = abc / 25$ ,

the operation  $*$  is associative. (Note that  $*$  is also commutative.)

**Example 7 :** Let  $L$  be a lattice and let  $a * b = a \wedge b$  (the greatest lower bound). Then  $*$  is associative.

Sol.: Since  $(a * b) * c = (a \wedge b) \wedge c$  and  $a * (b * c) = a \wedge (b \wedge c)$

But,  $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ .

Hence, the result.

Similarly, we can prove that  $a * b = a \vee b$  (the least upper bound of  $a$  and  $b$ ) is also associative.

### EXERCISE - I

- Show that  $\circ$  given by  $a \circ b = a^b$  is a binary operation on the set of natural numbers. (M.U. 2005, 07)
- Verify whether the following binary operations are commutative and associative.
  - Usual subtraction / division on  $\mathbb{Z}$ . [Ans.: Neither commutative nor associative]
  - $a * b = a + b + 3$  on  $\mathbb{Z}^+$ . [Ans.: Commutative and Associative]
  - $a * b = a/b$  on non-zero real numbers. [Ans.: Neither commutative, nor associative]
  - $a * b = ab$  on  $\mathbb{Z}$ . [Ans.: Commutative and Associative]
  - $a * b = \max(a, b)$  maximum (minimum) of  $a$  and  $b$  on  $R$ . [Ans.: Commutative and Associative]
  - $a * b = ab/7$ . [Ans.: Commutative and Associative]
  - $a * b = ab + 3b$  on  $R$ . [Ans.: Neither Commutative nor Associative]

3. Consider the set  $A = \{0, 1, 2, 3\}$ . Give one example for each of the following.

- A relation  $R$  on  $A$  that is neither symmetric, nor anti-symmetric.
- A relation  $R$  on  $A$  that is symmetric, transitive but not reflexive.
- A binary operation on  $A$  that is commutative but not associative.

(M.U. 2005)

- [Ans.: (i)  $R = \{(1, 3), (1, 0), (2, 0), (0, 1)\}$ ,  
 (ii)  $R = \{(0, 1), (1, 0), (1, 2), (2, 1), (2, 3), (3, 2), (0, 0), (1, 3), (3, 1)\}$ ,  
 (iii) See adjoining Table.]

*	0	1	2	3
0	0	1	2	3
1	1	2	3	2
2	2	3	2	0
3	3	0	2	1

### 4. Semi-Group

#### (i) Definition

A non-empty set  $S$  together with a (i) binary and (ii) associative operation,  $*$  is called a semi-group.

We denote the semi-group by  $(S, *)$ . Thus, a non-empty set  $S$  is a semi-group if

- $*$  is binary i.e.  $a * b \in S$  for every  $a, b \in S$ .

- $*$  is associative i.e.  $a * (b * c) = (a * b) * c$  for every  $a, b, c \in S$ .

Definition : A semi-group  $(S, *)$  is called commutative semi-group if  $*$  is commutative. Thus,  $(S, *)$  will be a commutative semi-group if  $*$  is (i) binary, (ii) associative and (iii) commutative.

#### Examples of Semi-groups

**Example 1 :**  $(\mathbb{Z}, +)$  is a commutative semi-group.

**Example 2 :** If  $A$  is a set and  $\mathcal{P}(A)$  is its power set then  $\mathcal{P}(A)$  with the operation of union is a commutative semi-group.

**Example 3 :** Prove that the set  $\mathbb{Q}$  of rational numbers with the binary operation  $*$  defined by  $a * b = a + b - ab$ ;  $a, b \in \mathbb{Q}$  is a semi-group. Is it commutative?

Sol.: With usual multiplication addition and subtraction for any two rational numbers  $a * b = a + b - ab$  belongs to  $\mathbb{Q}$ . Hence,  $*$  is a binary operation.

$$\begin{aligned} \text{Now, } (a * b) * c &= (a + b - ab) * c \\ &= (a + b - ab) + c - (a + b - ab) * c \\ &= a + b - ab + c - ac - bc + abc \\ &= a + b + c - ab - bc - ca + abc. \end{aligned}$$

$$\begin{aligned} \text{Also, } a * (b * c) &= a * (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc \\ &= a + b + c - ab - bc - ca + abc. \end{aligned}$$

Hence,  $*$  is associative.

Further,  $b * a = b + a - ba = a + b - ab$

Hence,  $a * b = b * a$ .  $\therefore *$  is also commutative.

### Applied Mathematics - IV

(16-5)

### Some Algebraic Structures

**Example 4 :** Let  $Z_n = \{0, 1, 2, \dots, (n-1)\}$  and  $*$  be the operation on  $Z_n$  such that  $a * b =$  the remainder when  $ab$  is divided by  $n$ .

(a) Construct the table for the operation  $*$  when  $n = 4$ .

(b) Show that  $(Z_4, *)$  is a semigroup.

Sol. : (a) We have  $Z_4 = \{0, 1, 2, 3\}$  and  $a * b =$  remainder when  $ab$  is divided by 4.

With this understanding, we get the adjoining table.

(b) (i) From the table it is clear the  $Z_4$  is closed under  $*$  because  $a * b$  belongs to  $Z_4$ .

(ii) Now consider associativity. Let  $a = 1, b = 2, c = 3$  then using the table we see that

$$(a * b) * c = 2 * 3 = 2$$

$$a * (b * c) = 1 * 2 = 2$$

$$\therefore (a * b) * c = a * (b * c)$$

It can be verified for all the elements.

Hence,  $*$  is associative. Hence,  $(Z_4, *)$  is a semigroup for any  $n$ .

**Example 5 :** Let  $(A, +)$  be a semigroup. Consider a binary operation  $*$  on  $A$  such that for  $x$  and  $y$  in  $A$ ,  $x + y = x * a * y$  where  $a$  is in  $A$ .

Show that  $*$  is an associative operation.

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(M.U. 1997)

Sol. : To prove associativity, we shall prove that

$$(x + y) + z = x + (y + z) \text{ where } x, y, z \in A$$

Now, L.H.S. =  $(x + y) + z = (x * a * y) + z$

$$= (x * a * y) * a * z = x * a * y * a * z$$

And R.H.S. =  $x + (y + z) = x + (y * a * z)$

$$= x * a * (y * a * z) = x * a * y * a * z$$

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

$\therefore +$  is an associative operation.

#### (b) Product of Semi-groups

Let  $(S_1, *_1)$  and  $(S_2, *_2)$  be two semi-groups. We can obtain a new semi-group  $S = S_1 \otimes S_2$  called the product of  $S_1$  and  $S_2$  as follows.

(i) The elements of  $S$  come from  $S_1 \times S_2$  i.e. if the ordered pair  $(a, b)$  is an element of  $S$ , then  $a \in S_1$  and  $b \in S_2$ .

(ii) The operation  $*$  on  $S$  is defined on the two components as

$$(a, b) * (a', b') = (a *_1 a', b *_2 b') \quad [\text{See Ex. 1, page 16-11}]$$

### 5. Monoid

(M.U. 2000, 10)

(a) Definition : A semi-group  $(S, *)$  which has identity is called a monoid.

Thus, we can say that there are semi-groups which have identity (in which case we call them monoids) and there are semi-groups without identity element.

(b) Theorem : The identity element of a semi-group is unique.

Proof : If possible let  $e'$  be another identity element of the semi-group  $(S, *)$ . Since  $e'$  is an identity,  $a * e' = e' * a = a$  for each  $a$ .

(16-6)

### Some Algebraic Structures

#### Applied Mathematics - IV

In particular, let  $a = e$ .

Also since  $e$  is an identity,

in particular let  $a = e'$ ,

From (i) and (ii), it follows that  $e = e'$ .

$\therefore$  The identity element is unique.

(16-6)

### Some Algebraic Structures

$e * e' = e' * e = e$

$e * e = e * e' = e$  for each  $e$ .

$\therefore$  (1)

$e' * e = e * e' = e$

$\therefore$  (2)

#### Examples of Monoid

**Example 1 :** The semi-group  $(Z, +)$  is a monoid because 0 is the identity element.

But note that the semi-group  $(Z^+, +)$  is not a monoid as it has no identity element.

**Example 2 :** The semi-group  $(Z^+, \times)$  is a monoid because 1 is its identity element.

**Example 3 :** Let  $S$  be a finite set. Let  $F(S)$  be the set of all functions  $f : S \rightarrow S$  and let  $*$  be operation of composition of functions.

$F(S)$  is a monoid because  $*$  is associative and identity function is the identity of this semi-group.

**Example 4 :** Verify that if  $A$  is any set then the power set  $P(A)$  with the operation of union is a monoid.

Sol. As seen before in Ex. 2, page 16-4 for union  $(P(A), \cup)$  is a commutative semi-group.

If  $\Phi$  is the null-set then  $\Phi$  is the identity element because

$$\Phi \cup A = \Phi \cap A = A \quad \text{and} \quad A \cup \Phi = A \cap \Phi = A$$

Hence,  $(P(A), \cup)$  is a monoid.

Note that  $P(S)$  with  $*$  as intersection of two subsets of  $P(S)$  is also a monoid with  $P(S)$  itself as identity. It is also commutative.

**Example 5 :** If  $a + b = a$  and  $S$  is the set of all positive integers  $Z^+ = \{1, 2, 3, \dots\}$ , verify whether  $(S, +)$  is a semi-group or a monoid.

Sol. Since for every  $a, b$ ,  $a + b = a$  is in  $S$ ,  $*$  is binary.

$$\text{Further, } (a + b) + c = a + c = a \quad \text{and} \quad a + (b + c) = a + b = a$$

$\therefore +$  is associative.

Hence,  $(S, +)$  is a semi-group.

$$\text{But } a + 1 = a \text{ and } 1 + a = 1.$$

Hence,  $(S, +)$  has no identity element.  $\therefore (S, +)$  is not a monoid.

### 6. Isomorphism, Automorphism And Homomorphism

We have already studied isomorphism between two posets. In general, two algebraic systems are called isomorphic if they preserve special characteristics of the system. We shall now consider isomorphism between two semi-groups.

#### Isomorphism

**Definition :** Let  $(S, +)$  and  $(S', +')$  be two semi-groups. A function  $f : S \rightarrow S'$  is called an isomorphism from  $(S, +)$  to  $(S', +')$  if  $f$  is one-to-one and onto and if

$$f(a + b) = f(a) +' f(b) \quad \text{for all } a, b \in S.$$

Note carefully the  $+$  on the left side and  $+'$  on the right side.

**Theorem 1:** If  $(S, *)$  and  $(S', *')$  are two semi-groups and if  $f : S \rightarrow S'$  is a isomorphism from  $(S, *)$  to  $(S', *')$  then  $f^{-1} : S' \rightarrow S$  is also an isomorphism from  $(S', *')$  to  $(S, *)$ .

**Proof:** Since by definition of isomorphism,  $f$  is a one-to-one correspondence hence  $f^{-1}$  exists and is a one-to-one correspondence from  $(S', *')$  to  $(S, *)$ .

Let  $a'$  and  $b'$  be any two elements of  $S'$ . Since  $f$  is onto there exist elements  $a$  and  $b$  in  $S$  such that  $f(a) = a'$  and  $f(b) = b'$ .

$$\therefore a = f^{-1}(a') \text{ and } b = f^{-1}(b)$$

$$\text{Now, } f^{-1}(a'*b') = f^{-1}(f(a)*'f(b)) = f^{-1}(f(a*b))$$

[ $\because f$  is a isomorphism  $f(a*b) = f(a)*'f(b)$  by definition above.]

$$\therefore f^{-1}(a'*b') = (f^{-1}\circ f)(a*b) \\ = a+b = f^{-1}(a') + f^{-1}(b')$$

Hence,  $f^{-1}$  is an isomorphism.

#### Procedure To Prove An Isomorphism

To prove an isomorphism between two semi-groups  $(S, *)$  and  $(S', *')$  we shall follow the following procedure.

(i) Step 1 : We define the function  $f : S \rightarrow S'$  with domain of  $f = S$ ,

(ii) Step 2 : We shall show that  $f$  is one-to-one.

(iii) Step 3 : We shall show that  $f$  is onto.

(iv) Step 4 : We shall show that  $f(a*b) = f(a)*'f(b)$ .

**Example 1:** Let  $S$  be the set of all even integers. Show that the semi-groups  $(Z, +)$  and  $(S, +)$  are isomorphic. (M.U. 2016)

**Sol.:** We shall follow the above procedure.

Step 1 : We define the function  $f : Z \rightarrow S$  where  $f(a) = 2a$ .

Step 2 : Suppose  $f(a_1) = f(a_2)$ . Then  $2a_1 = 2a_2$ . Hence,  $f$  is one-to-one.

Step 3 : Suppose  $b$  is an even integer.

Then  $a = b/2 \in Z$  and  $f(a) = f(b/2) = 2(b/2) = b$ . Hence,  $f$  is onto.

Step 4 : We have  $f(a+b) = 2(a+b) = 2a+2b$

$$= f(a) + f(b)$$

Hence,  $(Z, +)$  and  $(S, +)$  are iso-morphic semi-groups.

**Example 2:** Let  $R^+$  be the set of all positive real numbers. Show that the function  $f : R^+ \rightarrow R$  defined by  $f(x) = \log x$  is an isomorphism from the semigroup  $(R^+, \times)$  to the semigroup  $(R, +)$  where  $\times$  and  $+$  are the usual multiplication and addition respectively. (M.U. 2004, 05)

**Sol.:** Step 1 : The function is defined by  $f(x) = \log x$ .

Step 2 : If  $f(a_1) = f(a_2)$ , then  $\log a_1 = \log a_2$

$$\therefore a_1 = a_2. \quad f \text{ is one-to-one.}$$

Step 3 : Suppose  $b$  is a real number then

$$e^b \in R \quad \text{and} \quad f(e^b) = \log e^b = b \in R^+.$$

$\therefore$  Each element of  $R$  is an image of some element of  $R^+$ .

$\therefore f$  is onto.

Step 4 : We have  $f(ab) = \log ab = \log a + \log b = f(a) + f(b)$

$\therefore f$  is an isomorphism.

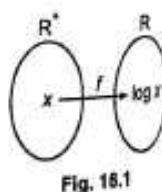


Fig. 16.1

**Example 3 :** Let  $S = \{a, b, c\}$  and  $S' = \{p, q, r\}$  and consider the following operations.

*	a	b	c	p	q	r
a	a	b	c	p	r	p
b	b	c	a	q	p	q
c	c	a	b	r	q	r

Let  $f(a) = q$ ,  $f(b) = p$ ,  $f(c) = r$ . Show that  $S$  and  $S'$  are isomorphic.

Step 1 : The function  $f$  is defined by  $f(a) = q$ ,  $f(b) = p$ ,  $f(c) = r$ .

Step 2 : Clearly  $f$  is one-to-one.

Step 3 : Clearly  $f$  is onto.

Step 4 : Now, from the first table above since  $a * b = b$

$$f(a * b) = f(b) = p$$

Also, since  $f(a) = q$ ,  $f(b) = p$ ,

$$f(a) *' f(b) = q *' p = p \quad \therefore f(a * b) = f(a) *' f(b)$$

This can be shown to be true for all possible products of  $a$ ,  $b$  and  $c$ . In fact we can obtain the table of operation  $*$  on  $f(a)$ ,  $f(b)$  and  $f(c)$  by replacing in the first table, the images of  $a$ ,  $b$ ,  $c$  i.e. by replacing  $a$  by  $f(a) = q$ ,  $b$  by  $f(b) = p$  and  $c$  by  $f(c) = r$ . Thus, we get

*	q	p	r
q	q	p	r
p	p	r	q
r	r	q	p

Interchanging the first and second rows we get the left table. Then interchanging the first and second columns we get the table on the right which is the same as the table given for  $*'$  on  $S'$ . This shows that  $S$  and  $S'$  are isomorphic.

*	q	p	r	p	q	r
p	p	r	q	p	p	p
q	q	p	r	p	q	r
r	r	q	p	r	q	p

**Example 4 :** Let  $S = \{a, b, c, d\}$  and  $S' = \{p, q, r, s\}$  and consider the following operations.

*	a	b	c	d	p	q	r	s
a	a	b	c	d	p	p	q	r
b	b	a	a	c	q	q	p	p
c	b	d	d	c	r	q	s	r
d	a	b	c	d	s	p	q	r

Let  $f(a) = p$ ,  $f(b) = q$ ,  $f(c) = r$ ,  $f(d) = s$ . Show that  $f$  is an isomorphism.

Step 1 : The function is defined by  $f(a) = p$ ,  $f(b) = q$ ,  $f(c) = r$ ,  $f(d) = s$ .

Step 2 : Clearly  $f$  is one-to-one.

Step 3 : Clearly  $f$  is onto.

Step 4 : Now  $a * b = b$ ,  $\therefore f(a * b) = f(b) = q$

Since  $f(a) = p$  and  $f(b) = q$ ,

$$f(a) *' f(b) = p *' q = q \quad \therefore f(a * b) = f(a) *' f(b)$$

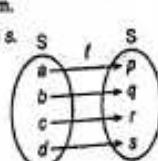


Fig. 16.3

This can be shown to be true for all possible products of  $a, b, c$  and  $d$ .  
Hence,  $f$  is isomorphic.

**Theorem 2:** Let  $(S, *)$  and  $(S', *')$  be monoids with identity elements  $e$  and  $e'$  respectively. Let  $f : S \rightarrow S'$  be an isomorphism from  $(S, *)$  to  $(S', *')$ . Prove that  $f(e) = e'$ .  
(M.U. 2003)

**Proof:** Let  $b$  be any element of  $S$ .

Since  $f$  is onto there is an element  $a$  in  $S$  such that  $b$  is the image of  $a$ . i.e.,  $f(a) = b$ .

Now,  $b = f(a) = f(a * e) = f(a) *' f(e)$

because  $S$  and  $S'$  are isomorphic.

But  $f(a) = b$ .

∴ From (1), we get  $b = b *' f(e)$

Similarly, since  $a = e * a$

$b = f(a) = f(e * a) = f(e) *' f(a)$

because  $S$  and  $S'$  are isomorphic.

$\therefore b = f(e) *' b$

From (2) and (3), we see that  $f(e)$  is the identity element of  $S'$ .

But since identity element is unique, we get,  $f(e) = e'$ .

**Corollary:** If  $(S, *)$  and  $(S', *')$  are two semi-groups such that  $S$  has an identity element while  $S'$  does not have the identity element then  $(S, *)$  and  $(S', *')$  cannot be isomorphic.

**Proof:** For isomorphism of two semi-groups we must have, for all  $a, b, S$ ,

$$f(a * b) = f(a) *' f(b)$$

If we take  $b = a$ , the identity element in  $S$ , then we must have,

$$f(a * a) = f(a) *' f(a) = f(a) *' a'$$

where,  $a'$  is the identity element of  $S'$  by the above theorem.

Since, by data  $a'$  does not exist,  $S$  and  $S'$  cannot be isomorphic.

**Example:** Let  $Z$  be the set of all integers and  $S'$  be the set of all even integers. If  $X$  is the usual multiplication then prove that  $(Z, X)$  and  $(S', X)$  are semi-groups which are not isomorphic.

**Sol.:** We can easily prove that  $(Z, X)$  and  $(S', X)$  are semi-groups because multiplication is binary and associative in both  $Z$  and  $S'$ .

But  $Z = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$  has multiplicative identity 1  
and  $S' = \{..., -6, -4, -2, 2, 4, 6, ...\}$  has no multiplicative identity.

Hence, by the above corollary  $(Z, X)$  and  $(S', X)$  are not isomorphic.

#### Automorphism

**Definition:** An isomorphism from a semigroup  $(S, *)$  to  $(S, *)$  itself is called an automorphism (auto = self) on  $(S, *)$ .

**Example 1:** Let  $S = \{a, b, c, d\}$  and consider the following operations  $*$ .

*	a	b	c	d
a	a	b	c	d
b	b	a	a	c
c	b	d	d	c
d	a	b	c	d

Let  $f(a) = d, f(b) = c, f(c) = b$  and  $f(d) = a$ .

Show that  $f$  is an automorphism.

**Sol.:** Step 1 : The function is defined by

$$f(a) = d, f(b) = c, f(c) = b, f(d) = a.$$

Step 2 : Clearly  $f$  is one-to-one.

Step 3 : Clearly  $f$  is onto.

Step 4 : From the table

$$a * b = b$$

$$\therefore f(a * b) = f(b) = c$$

$$\text{Since } f(a) = d, f(b) = c$$

$$f(a) * f(b) = d * c = c \quad \therefore f(a * b) = f(a) * f(b)$$

This can be shown to be true for all products of  $a, b, c$  and  $d$ .

Hence,  $f$  is isomorphic.

∴  $(S, *)$  is an automorphism.

If we drop the conditions of one-to-one and onto from the definition of isomorphism we get another property, called homomorphism of the algebraic structures of two semi-groups.

#### Homomorphism

**Definition :** Let  $(S, *)$  and  $(S', *')$  be two semi-groups. A function  $f : S \rightarrow S'$  is called a homomorphism from  $(S, *)$  to  $(S', *')$  if

$$f(a * b) = f(a) *' f(b) \quad \text{for all } a, b \in S.$$

Further if  $f$  is also onto  $S'$  is called a homomorphic image of  $S$ .

We note that for isomorphism as well as for homomorphism, the image of the product is equal to the product of the images

$$\text{i.e., } f(a * b) = f(a) *' f(b)$$

And the difference is that, in isomorphism  $f$  is one-to-one and also onto.

**Theorem 3:** Let  $(S, *)$  and  $(S', *')$  be monoids with identity elements  $e$  and  $e'$  respectively. Let  $f : S \rightarrow S'$  be homomorphism from  $(S, *)$  to  $(S', *')$ .

Prove that  $f(e) = e'$ .

**Proof:** Similar to the proof of Theorem 2, page 16-9 and as such is left to you.

**Theorem 4:** If  $f$  is a homomorphism from a commutative semi-group  $(S, *)$  onto a semi-group  $(S', *')$  then  $(S', *')$  is also commutative.

**Proof:** Let  $s_1'$  and  $s_2'$  be any two elements of  $S'$ . Since  $f$  is onto there exist two elements  $s_1$  and  $s_2$  in  $S$  whose images are  $s_1'$  and  $s_2'$  respectively i.e.  $f(s_1) = s_1'$  and  $f(s_2) = s_2'$ .

$$\begin{aligned} s_1' *' s_2' &= f(s_1) *' f(s_2) \\ &= f(s_1 * s_2) = f(s_2 * s_1) \end{aligned}$$

[∴  $(S, *)$  is a commutative semi-group.]

$$= f(s_2) *' f(s_1)$$

$$= s_2' *' s_1'$$

∴  $(S', *')$  is also commutative.

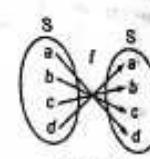


Fig. 16.4

**Example 1:** Let  $S = N \times N$ . Let  $*$  be the operation on  $S$  defined by  $(a, b) * (a', b') = (a + a', b + b')$ . Further, let  $f : (S, *) \rightarrow (\mathbb{Z}, +)$  defined by  $f(a + b) = a - b$ .

Show that  $(S, *)$  is a semi-group and  $f$  is a homomorphism.

**Sol.:** (a) Let  $x = (a, b)$ ,  $y = (c, d)$ ,  $z = (e, f)$  where  $a, b, c, d, e, f \in N$ .

(M.U. 2004)

$$\begin{aligned} (i) \quad x * y &= (a, b) * (c, d) \\ &= (a + c, b + d) \end{aligned}$$

But  $a + c \in N$  and  $b + d \in N$

$\therefore (a + c, b + d) \in N \times N$ .  $*$  is binary.

$$\begin{aligned} (ii) \quad x(yz) &= (a, b) * [(c, d) * (e, f)] \\ &= (a, b) * (c + e, d + f) \\ &= [a + (c + e), b + (d + f)] \\ (xy)z &= [(a, b) * (c, d)] * (e, f) \\ &= (a + c, b + d) * (e, f) \\ &= [(a + c) + e, (b + d) + f] \end{aligned}$$

But as  $a, b, c, d, e, f \in N$ ,

$$\begin{aligned} a + (c + e) &= a + c + e = (a + c) + e \\ b + (d + f) &= b + d + f = (b + d) + f \end{aligned}$$

$\therefore *$  is associative. Hence,  $(S, *)$  is a semi-group.

(b) Further, we have

$$\begin{aligned} f(x * y) &= f(a + c, b + d) \\ &= (a + c) - (b + d) = (a - b) + (c - d) \\ &= f(a, b) + f(c, d) = f(x) + f(y) \end{aligned}$$

But  $f : S \rightarrow \mathbb{Z}$  is not onto. Hence,  $f$  is homomorphism.

**Example 2:** Let  $S = N \times N$  and  $*$  be the operation on  $S$  defined by  $(a, b) * (a', b') = (aa', bb')$ . Show that  $(S, *)$  is a semi-group. If  $f$  is defined by  $f : (S, *) \rightarrow (\mathbb{Q}, +)$  by  $f(a, b) = a/b$ , show that  $f$  is homomorphism.

**Sol.:** Left to you.

If  $x = (a, b)$ ,  $y = (c, d)$ ,  $z = (e, f)$ , note that

$$\begin{aligned} f(x * y) &= f(ac, bd) = (ac) / (bd) \\ &= (a/b)(c/d) = f(x) + f(y). \end{aligned}$$

## 7. Group

(M.U. 2000, 01, 10)

**Definition:** An ordered pair  $(G, *)$  is called a **group**, if  $G$  is a non-empty set and  $*$  is a **binary operation** on  $G$  satisfying the following axioms.

G1: For all  $a, b, c \in G$ ,  $a * (b * c) = (a * b) * c$ .  
(i.e.,  $*$  is associative in  $G$ )

G2: There exists an element  $e \in G$ , such that  $a * e = e * a = a$  for all  $a \in G$ . The element  $e$  is called identity for  $*$ .  
(i.e., identity  $e$  for  $*$  exists in  $G$ .)

**d3:** For every  $a \in G$  there exists an element  $b \in G$  such that  $a * b = b * a = e$ . The element  $b$  is called the inverse of  $a$  and is denoted by  $a'$  or by  $a^{-1}$ .  
(i.e., for every element in  $G$  inverse exists.)

**Abelian or Commutative Group :** A group  $(G, *)$  is called commutative or Abelian if  $a * b = b * a$  for all  $a, b \in G$ .

Most of the groups that we shall be dealing with are commutative i.e. Abelian groups. But all groups are not commutative. If  $M$  is the set of non-singular  $n \times n$  matrices then the set forms a non-commutative group under multiplication. You might have noticed that in general  $A * B \neq B * A$  where  $A$  and  $B$  are non-singular square matrices of the same order.

### Examples of Groups

**Example 1:** Let  $G = \{x \mid x$  is a real number and  $a * b = a + b$ , the usual addition. Then  $(G, +)$  is an Abelian group with 0 as identity and  $-a$  as  $a^{-1}$ .

**Example 2:** Let  $G = \{x \mid x$  is a rational number excluding zero) and  $a * b = a \times b$ , the usual multiplication.

$G$  is group with 1 as identity and  $q/p$  as inverse of  $p/q$ .

**Example 3:** Let  $G = \{0, \pm 1, \pm 2, \dots\}$  and  $a * b = a + b$  the usual sum of integers. Then  $(G, +)$  is an Abelian group with 0 as identity and  $-a$  is  $a^{-1}$ .

**Example 4:** Let  $G = \{x \mid x$  a non-zero real number } and  $a * b = a \times b$ , the usual multiplication. Then  $(G, *)$  is an Abelian group with 1 as identity and  $1/a$  as  $a^{-1}$ .

**Example 5:** Let  $G = \{z \mid z$  is a complex number } and  $a * b = a + b$ , the addition of complex numbers. Then  $(G, +)$  is an Abelian group with  $0 + i0$  as identity and  $-x - iy$  as the inverse of  $x + iy$ .

**Example 6:** Let  $G = \{z \mid z$  is a non-zero complex number }  $a * b = a \times b$ , the multiplication of complex numbers. Then  $(G, *)$  is an Abelian group with  $1 + i0$  as identity and  $(x - iy)/(x^2 + y^2)$  as inverse of  $x + iy$ .

**Example 7:** Let  $G = \{z \mid z = e^{i\theta}\}$  and  $a * b = a \times b$  usual multiplication of complex numbers. Then  $(G, *)$  is an Abelian group with  $e^{i\theta}$  as unity and  $e^{-i\theta}$  as inverse of  $e^{i\theta}$ .

**Example 8:** Let  $G = \{1, -1\}$  and  $a * b = a \times b$  with usual multiplication. Then  $(G, *)$  is a group with 1 as identity and each element is inverse of itself.

### Examples of Non-Commutative Groups

**Example 1:** Let  $G = \{M \mid M$  is a  $2 \times 2$  non-singular matrix } and  $A * B$  be the usual matrix multiplication. Then  $(G, *)$  is a group but not an Abelian group. (We shall discuss this problem in detail on page 16-18 in Ex. 12.)

**Example 2:** Let  $G = \{(a, b) \mid (a, b)$  is an ordered pair of real numbers,  $a \neq 0\}$  and  $(a, b) * (c, d) = (ac, bc + d)$ . Then  $(G, *)$  is a group but not an Abelian group. (See Ex. 11, page 16-17.)

### To prove that $G$ is a group

**Example 1:** Prove that  $G = \{1, -1, i, -i\}$  is a group under usual multiplication  $*$  of complex numbers.

**Sol.:** The adjoining table shows the result of multiplication of elements of  $G$ .

"Since for every pair  $a, b \in G$  there exists a unique element  $a * b$  in  $G$ ,  $*$  is a binary operation in  $G$ .

*	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

**G1 :** Since multiplication of complex numbers is associative, the multiplication  $*$  is associative in  $G$ .

**G2 :** From the first column (or row) we see that 1 is an identity element. Hence,  $1 \in G$  is an identity element.

**G3 :** Since  $1 * 1 = 1$ ,  $(-1) * (-1) = 1$ ,  $(i) * (-i) = 1$ ,  $(-i) * (i) = 1$ , inverse exists for every elements in  $G$ . We have  $1^{-1} = 1$ ,  $-1^{-1} = -1$ ,  $i^{-1} = -i$ ,  $-i^{-1} = i$ . Hence,  $G$  is a group under multiplication.

**Example 2 :** Prove that the set of cube-roots of unity is a group under multiplication of complex numbers. (M.U. 2005)

**Sol. :** We know that the three cuberoots of unity are  $1$ ,  $\omega$ ,  $\omega^2$ , where  $\omega = e^{2\pi i/3}$ ,  $\omega^2 = e^{4\pi i/3}$ .

The multiplication table is given on the right. The table shows that  $G$  is closed under  $*$ .

**G1 :** Since multiplication of complex numbers is associative, multiplication is associative in  $G$ .

**G2 :** From the first row (or column) we find that 1 is the identity element.

**G3 :** Since the identity element 1 appears in each row (column) each element has its inverse.  
 $\therefore (1)^{-1} = 1$ ,  $(\omega)^{-1} = \omega^2$ ,  $(\omega^2)^{-1} = \omega$ .

$\therefore$  Cube-roots of unity is a group under multiplication.

**Example 3 :** Prove that the set of real numbers is a group under  $*$  defined by

$$a * b = a + b - 2.$$

**Sol. :** Since for every  $a, b \in R$ , there exists a unique element  $a * b = a + b - 2$  in  $R$ ,  $*$  is a binary operation in  $R$ .

$$\text{G1 : } (a * b) * c = (a + b - 2) * c = (a + b - 2) + c - 2 \\ = a + b + c - 4$$

$$\text{And } a * (b * c) = a * (b + c - 2) = a + (b + c - 2) - 2 \\ = a + b + c - 4$$

$$\therefore (a * b) * c = a * (b * c) \text{ for all } a, b, c \in R.$$

$\therefore$   $*$  is associative in  $R$ .

**G2 :** To find identity  $e$ , consider  $a * e = a$

$$\text{But } a * e = a + e - 2$$

$$\therefore a + e - 2 = a \quad \therefore e = 2. \quad \therefore 2 \text{ is the identity element.}$$

**G3 :** To find inverse of  $a$ . Let  $b$  be the inverse. Then  $a * b = e = 2$

$$\therefore a + b - 2 = 2 \quad \therefore b = 4 - a.$$

$\therefore 4 - a$  is the inverse of  $a$ .  $\therefore$  Hence,  $G$  is a group under  $*$ .

**Example 4 :** Determine whether the following set together with the binary operation  $*$  is a semi-group, monoid or a group. Justify your answer.

(a) Set of real numbers with  $a * b = a + b + 2$ .

(b) The set of  $m \times n$  matrices under the operation of multiplication. (M.U. 2005)

*	1	$\omega$	$\omega^2$
1	1	$\omega$	$\omega^2$
$\omega$	$\omega$	$\omega^2$	1
$\omega^2$	$\omega^2$	1	$\omega$

**Sol. :** (a) Since for every  $a, b \in R$ , there exists a unique element  $a * b = a + b - 2$  in  $R$ ,  $*$  is a binary operation.

$$\text{G1 : } (a * b) * c = (a + b - 2) * c = (a + b - 2) + c - 2 = a + b + c - 4$$

$$\text{and } a * (b * c) = a * (b + c - 2) = a + (b + c - 2) - 2 = a + b + c - 4$$

$$\therefore (a * b) * c = a * (b * c) \quad \therefore *$$
 is associative in  $R$ .

**G2 :** To find identity, consider  $a * e = a$ .

$$a + e - 2 = a \quad \therefore e = 2$$

$\therefore 2$  is the identity element.

**G3 :** To find the inverse. Let  $b$  be the inverse of  $a$ . Then by definition of the inverse

$$a * b = e \quad \therefore a + b - 2 = -2 \quad \therefore a + b = -4 \quad \therefore b = -4 - a$$

Hence,  $-4 - a$  is the inverse of  $a$ .

$\therefore G$  is a group under  $*$ .

(b) If  $A$  and  $B$  are two  $m \times n$  matrices, then we know that  $AB$  is not defined.

$\therefore$  The operation of multiplication is not binary and hence the set of  $m \times n$  matrices under multiplication is not a monoid, a subgroup or a group.

**Example 5 :** Let  $G$  be the set of rational numbers different from 1.

Let  $a * b = a + b - ab$  for all  $a, b \in G$ . Prove that  $(G, *)$  is a group. (M.U. 2005, 12)

**Sol. :** Let  $a, b \in G$ . We shall prove that  $a * b = a + b - ab$  is a rational number different from 1 by reduction-ad-absurdum method.

If possible, let  $a + b - ab = +1$

$$\therefore a - b + b - ab = 0 \quad \therefore (a - 1) - b(a - 1) = 0$$

$$\therefore (a - 1)(-b + 1) = 0.$$

Hence,  $a = +1$ ,  $b = +1$  which is absurd since  $a, b \in G$ , the set of rational numbers different from 1.

$\therefore a * b$  is a rational number different from 1 i.e.  $a * b \in G$ .

$\therefore *$  is a binary operation.

$$\text{G1 : } a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a(b + c - bc)$$

$$= a + b + c - bc - ab - ac + abc$$

$$\text{And } (a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c$$

$$= a + b + c - ab - ac - bc + abc.$$

Hence,  $a * (b * c) = (a * b) * c$ .  $\therefore *$  is associative.

**G2 :** Now  $a * 0 = a + 0 - a \cdot 0 = a$

Also  $0 * a = 0 + a - 0 \cdot a = a \quad \therefore 0 \in G$  is the identity element.

**G3 :** For a given  $a, b \in G$  consider the equation  $a * b = 0$

$$\text{i.e., } a + b - ab = 0. \quad \therefore b = \frac{a}{1-a}.$$

Since  $a * b = a + b - ab = 0$ ,  $b$  is the inverse of  $G$ . Since  $a \in G$ ,  $a \neq 1$ .

$\therefore b$  is rational. Further  $b = -\frac{a}{1-a} \neq 1$  because if  $b = -\frac{a}{1-a} = 1$

$$\text{i.e., } -a = 1 - a \text{ i.e., } 0 = 1 \text{ which is absurd.}$$

Hence,  $b$  is different from one.

$$\therefore b = -\frac{a}{1-a} \in G \quad \therefore b \text{ is the inverse of } a.$$

$$\therefore a^{-1} = -\frac{a}{1-a}. \quad \text{Hence, } G \text{ is a group under } *.$$

**Example 6 :** Prove that if  $G$  is the set of all subsets of  $A$ , a non-empty set  $A$  and  $*$  the operation of union, then  $(G, *)$  is not a group.

**Sol. :** If  $A, B$  are the subsets of  $A$  then  $A \cup B$  is also a subset of  $A$ .

(M.U. 2001)

$\therefore G$  is closed under  $*$ .

$$G1 : A \cup (B \cup C) = (A \cup B) \cup C.$$

$\therefore *$  is associative.

**G2 :** If  $\Phi$  denotes empty set.

$$A \cup \Phi = A \text{ and } \Phi \cup A = A \quad \therefore \Phi \in G \text{ is identity element.}$$

**G3 :** But the inverse of a set  $A \in G$  does not exist because we cannot find a non-empty set  $B$  such that  $A \cup B = \Phi$ .

$\therefore$  Inverse does not exist.  $\therefore (G, *)$  is not a group.

**Example 7 :** Let  $G$  be a set of all square matrices of type  $\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$  where  $m \in \mathbb{Z}$ . Prove that  $G$  is a group under multiplication. Is it a Abelian group?

(M.U. 2002, 03)

$$\text{Sol. : Let } A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$$

$$\therefore AB = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} \in G$$

$\therefore$  Multiplication is binary operation.

**G1 :** Since matrix multiplication is associative, multiplication in the example is associative.

$$G2 : \text{Let } I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$AI = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}. \quad \text{Also} \quad IA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$$

$\therefore I$  is identity element.

**G3 :** Since  $|A| = 1 \neq 0$ , inverse of  $A$  exists for every  $A \in G$ .

$\therefore (G, *)$  is a group under multiplication.

$$\text{Now, } AB = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} \text{ as seen above and } BA = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$$

$\therefore AB = BA. \quad \therefore (G, *)$  is an Abelian group.

**Example 8 :** Let  $G$  be the set of complex numbers for which  $|z| = 1$ . Is  $(G, *)$  a group where  $*$  is multiplication of complex numbers?

(M.U. 2002)

**Sol. :** Let  $z_1 = x_1 + iy_1, z_2 = x_2 + iy_2$  where  $|z_1| = 1, |z_2| = 1$  i.e.  $x_1^2 + y_1^2 = 1, x_2^2 + y_2^2 = 1$ .

NOW,

$$\begin{aligned} z_1 z_2 &= (x_1 + iy_1)(x_2 + iy_2) = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1) \\ |z_1 z_2|^2 &= (x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + x_2 y_1)^2 \\ &= x_1^2 x_2^2 + y_1^2 y_2^2 - 2x_1 x_2 y_1 y_2 + x_1^2 y_2^2 + x_2^2 y_1^2 + 2x_1 x_2 y_1 y_2 \\ &= x_1^2 x_2^2 + x_1^2 y_2^2 + y_1^2 x_2^2 + y_1^2 y_2^2 \\ &= x_1^2 (x_2^2 + y_2^2) + y_1^2 (x_2^2 + y_2^2) \\ &= (x_1^2 + y_1^2)(x_2^2 + y_2^2) = 1 \times 1 = 1 \end{aligned}$$

$$|z_1 z_2| = 1$$

$\therefore *$  is a binary operation.

**G1 :** Multiplication of complex numbers is associative.

$\therefore *$  is associative.

**G2 :** For any complex number  $z = x + iy, (x + iy)(1 + i0) = z + iy$

$\therefore (1 + i0)$  whose modulus 1 is the identity element.

**G3 :** Let  $z = x + iy$  and  $z^{-1} = x - iy$

$$z * z^{-1} = (x + iy)(x - iy) = x^2 + y^2 = 1$$

$\therefore$  For every  $z \in G$  the inverse exist.

$\therefore$  Further, since for complex numbers  $z_1 z_2 = z_2 z_1$ ,

$\therefore (G, *)$  is an Abelian group.

**Example 9 :** If  $R$  is the set of all real numbers other than zero and  $a * b = 2ab$ , prove that  $(R, *)$  is an Abelian group.

**Sol. :** Since  $a * b = 2ab \in R$ ,  $*$  is a binary operation in  $R$ .

$$G1 : a * (b * c) = a * (2bc) = 2a(2bc) = 4abc$$

$$\text{And } (a * b) * c = (2ab) * c = 2(2ab)c = 4abc.$$

$\therefore *$  is associative.

$$G2 : \text{Let } a * e = a \quad \therefore 2ae = a \quad \therefore e = \frac{1}{2}$$

$$\text{Now, } a * \frac{1}{2} = 2a * \frac{1}{2} = a, \quad \frac{1}{2} * a = 2 * \frac{1}{2} a = a.$$

$\therefore \frac{1}{2}$  is identity element.

$$G3 : \text{Let } a * b = e = \frac{1}{2} \quad \therefore 2ab = \frac{1}{2} \quad \therefore b = \frac{1}{4a}$$

Hence,  $\frac{1}{4a}$  is the inverse of  $a$  i.e.  $a^{-1} = \frac{1}{4a}$ .

$\therefore$  For every  $a \in R$ , inverse exists.

Further,  $a * b = 2ab$  and  $b * a = 2ab$ .

$\therefore a * b = b * a. \quad \therefore (R, *)$  is an Abelian group.

**Example 10 :** Let  $G$  be the set of all non-zero real numbers and let  $a * b = \frac{ab}{2}$ . Show that  $(G, *)$  is an Abelian group.

**Sol. :** Since  $a * b = \frac{ab}{2}$  and  $\frac{ab}{2} \in R$ , if  $a, b \in R$ ,  $*$  is a binary operation in  $R$ .

**G1 :**  $a * (b * c) = a * \frac{bc}{2} = \frac{a(bc)}{4} = \frac{abc}{4}$  and  $(a * b) * c = \frac{ab}{2} * c = \frac{(ab)c}{4} = \frac{abc}{4}$

$\therefore *$  is associative.

**G2 :** Let  $a * a = a$   $\therefore \frac{aa}{2} = a$   $\therefore aa = 2a$   $\therefore a = 2$

Now,  $a * 2 = \frac{a2}{2} = a$   $\therefore 2$  is identity element.

**G3 :** Let  $a * b = a = 2$   $\therefore \frac{ab}{2} = 2$   $\therefore ab = 4$   $\therefore b = \frac{4}{a}$

$\therefore \frac{4}{a}$  is the inverse of  $a$  i.e.,  $a^{-1} = \frac{4}{a}$ .

Further  $a * b = \frac{ab}{2}$  and  $b * a = \frac{ba}{2}$ ,

$\therefore a * b = b * a$   $\therefore (R, *)$  is an Abelian group.

**Example 11 :** Determine whether the set  $A$  of all ordered pairs  $(a, b)$  of real numbers ( $a \neq 0$ ) under  $*$  defined by  $(a, b) * (c, d) = (ac, bc + d)$  is an Abelian group. (M.U. 2003)

**Sol. :** If  $a, b, c, d$  are real numbers, we have

$$(a, b) * (c, d) = (ac, bc + d) \quad \text{and} \quad ac \in R, bc + d \in R.$$

$\therefore *$  is a binary operation.

**G1 :** Consider

$$[(a, b) * (c, d)] * (e, f) = (ac, bc + d) * (e, f) = (ace, bce + de + f)$$

$$(a, b) * [(c, d) * (e, f)] = (a, b) * [(ce, de + f)] = (ace, bce + de + f)$$

$$[(a, b) * (c, d)] * (e, f) = (a * b) * [(c, d) * (e, f)]$$

$\therefore *$  is associative.

**G2 :** Let  $(a, b) * (x, y) = (a, b)$  so that  $(x, y)$  is identity element.

$$\therefore (ax, bx + y) = (a, b)$$

This equality will hold if  $x = 1$  and  $y = 0$ .

$\therefore (1, 0)$  is identity element.

**G3 :** Let  $(a, b) * (x, y) = (1, 0)$

$$\therefore (ax, bx + y) = (1, 0) \quad \therefore ax = 1, bx + y = 0$$

$$\therefore x = \frac{1}{a}, y = -bx = -\frac{b}{a} \quad \therefore (a, b)^{-1} = (x, y) = \left( \frac{1}{a}, -\frac{b}{a} \right).$$

It can be verified that

$$(a, b) \left( \frac{1}{a}, -\frac{b}{a} \right) = \left( 1, \frac{b}{a} - \frac{b}{a} \right) = (1, 0)$$

Further,  $(a, b) * (c, d) = (ac, bc + d)$  and  $(c, d) * (a, b) = (ca, da + b)$

$$\therefore (a, b) * (c, d) \neq (c, d) * (a, b)$$

$\therefore (R, *)$  is a group but not an Abelian group.

**Example 12 :** Let  $M$  be the set of all  $2 \times 2$  non-singular matrices. Prove that  $M$  is a non-commutative group under usual multiplication of matrices. Is  $M$  a group under addition of matrices?

**Sol. :** If  $A, B \in M$  then clearly  $AB$  is defined and is a  $2 \times 2$  matrix. Further,  $(AB)^{-1} = B^{-1}A^{-1}$ . Since the inverse of  $AB$  exists,  $AB$  is non-singular.

$\therefore$  Multiplication is a binary operation on  $M$ .

**G1 :** The matrix multiplication is associative.

**G2 :** The identity matrix is  $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ . It is non-singular.

Also  $I \in M, A I = I A = I$  for all  $A \in M$ .

**G3 :** By definition of a non-singular matrix, for  $A \in M$  there exist  $A^{-1}$  ( $\in M$ ) the inverse of  $A$  such that

$$AA^{-1} = A^{-1}A = I. \quad \therefore M$$
 is a group under multiplication.

Now, to demonstrate that it is a non-abelian group, let

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Since  $|A| = |B| = -1$ , both  $A, B$  are non-singular.

$$\text{But } AB = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ and } BA = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$\therefore AB \neq BA. \quad \therefore G$$
 is not Abelian.

For the last part, let  $A \in M$  be any matrix. Then  $|A| \neq 0$ . Also  $|-A| = -|A| \neq 0$ .

$\therefore (-A)$  is also a non-singular matrix. But  $(A) + (-A) = 0$ . Hence, the determinant of the sum is zero. The sum is not non-singular and does not belong to  $M$ . i.e.,  $M$  is not closed under addition.

$\therefore M$  is not a group under addition (where  $M$  is the set of non-singular matrices.)

If  $M$  is any matrix then  $(M, \times)$  is not a group because inverse does not exist always.

**Example 13 :** Prove that the set of matrices  $A_\alpha = \begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix}$

where  $\alpha$  is real, forms a group under usual matrix multiplication. Is the group Abelian?

(M.U. 1997, 98, 2004, 05)

**Sol. :** Let  $A_\alpha, A_\beta \in G$ .

$$\begin{aligned} A_\alpha * A_\beta &= \begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix} \begin{bmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{bmatrix} \\ &= \begin{bmatrix} \cos(\alpha + \beta) & -\sin(\alpha + \beta) \\ \sin(\alpha + \beta) & \cos(\alpha + \beta) \end{bmatrix} = A_{\alpha+\beta} \in G \end{aligned}$$

$\therefore *$  is a binary operation.

**G1 :** We know that matrix multiplication is associative.

**G2 :** The unit matrix  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix}$  is identity element.

**G3 :** Since  $|A_\alpha| = \cos^2 \alpha + \sin^2 \alpha = 1$ ,  $A_\alpha$  is non-singular, inverse exists.

$$A^{-1} = \frac{1}{|A_\alpha|} \text{adj. } A = \begin{bmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{bmatrix} = \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix} = A_{(-\alpha)} \in G$$

Further, matrix multiplication is commutative.

$\therefore (A_\alpha, *)$  is an Abelian group.

**Example 14 :** Let  $(G, +)$  be a group. Prove that  $G$  is an Abelian group if and only if  $(a + b)^2 = a^2 + b^2$  where  $a^2$  stands for  $a * a$ . (M.U. 1999, 2002, 08, 14, 15)

**Sol. :** (i) Let  $(G, +)$  be an Abelian group.

Hence,  $a + b = b + a$ .

Now, consider

$$\begin{aligned} (a + b)^2 &= (a + b) * (a + b) \\ &= (a + b) * (b + a) \quad [\text{By (1)}] \\ &= a + (b + b) + a \\ &= a + b^2 + a = a + a + b^2 \quad [\text{By (1)}] \\ &= a^2 + b^2. \end{aligned}$$

(ii) Let  $(a + b)^2 = a^2 + b^2$

Pre-multiplying by  $a^{-1}$  and post-multiplying by  $b^{-1}$ .

$$\begin{aligned} a^{-1} * (a + b)^2 * b^{-1} &= a^{-1} * (a^2 + b^2) * b^{-1} \\ \therefore a^{-1} * (a + b) * (a + b) * b^{-1} &= a^{-1} * (a + a + b + b) * b^{-1} \\ \therefore (a^{-1} * a) * (b * a) * (b * b^{-1}) &= (a^{-1} * a) * (a + b) * (b + b^{-1}) \\ \therefore a * (b * a) * a &= a * (a + b) * a \\ \therefore b * a &= a * b. \quad \therefore G \text{ is an Abelian group.} \end{aligned}$$

**Example 15 :** If  $(G, +)$  is an Abelian group, then prove that  $(a + b)^n = a^n + b^n$  where  $a, b \in G$ . (M.U. 2001, 13, 15)

**Sol. :** We shall prove the result by the method of mathematical induction.

**Step 1 :** By data  $(a + b)^1 = a^1 + b^1 \quad \therefore a + b = a * b$ .

$\therefore$  The result is true for  $n = 1$ .

**Step 2 :** Let the result be true for  $n = k$ .

$\therefore (a + b)^k = a^k + b^k$ .

Now, multiply both sides by  $a + b$ .

$$\begin{aligned} \therefore (a + b)^k * (a + b) &= a^k * b^k * a + b \\ \therefore (a + b)^{k+1} &= a^k * a + b^k * b \\ &= a^{k+1} + b^{k+1} \quad [\because G, + \text{ is an Abelian group}] \end{aligned}$$

Hence, the result is true for  $n = k + 1$ .

**Step 3 :** Since it is true for  $n = 1$ , by step 2, it is true for  $n = 2$  and since it is true for  $n = 2$  again by step 3, it is true for  $n = 3$  and so on.

It is true for all  $n$ .

**Example 16 :** Prove that a set of  $2 \times 2$  rook matrices form a group under matrix multiplication.

**Sol. :** A rook matrix is a square matrix which has only two elements, 0 and 1 such that each row or each column has exactly one 1.

Obviously there will be only two  $2 \times 2$  rook matrices given below,

$$M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

There will be four products of the above matrices.

$$M_1 \cdot M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = M_1$$

$$M_1 \cdot M_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = M_2$$

$$M_2 \cdot M_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = M_2$$

$$M_2 \cdot M_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = M_1$$

Thus, we have the following multiplication table.

*	M <sub>1</sub>	M <sub>2</sub>
M <sub>1</sub>	M <sub>1</sub>	M <sub>2</sub>
M <sub>2</sub>	M <sub>2</sub>	M <sub>1</sub>

The table shows that  $M_1$  is the identity element.

**G1 :** Since there are only two elements,  $*$  is trivially associative.

**G2 :**  $M_1$  is the identity element.

**G3 :** Since  $M_1 \cdot M_1 = M_1$  (Identity),  $M_1$  is the inverse of  $M_1$ .

Since  $M_2 \cdot M_2 = M_1$  (Identity),  $M_2$  is the inverse of  $M_2$ .

Further, since  $M_2 \cdot M_1 = M_1 \cdot M_2 \quad \therefore (M, *)$  is an Abelian Group.

**Example 17 :** Prove that a set of bijective functions from  $A$  to  $A$  where  $A = \{1, 2\}$  is a group under composition of functions. Is it Abelian?

**Sol. :** Let  $A = \{1, 2\}$  then we have the following two bijective functions on  $A$ .

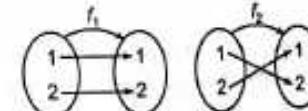


Fig. 16.5

We can obtain four compositions from  $f_1$  and  $f_2$  viz.  $f_1 \circ f_1$ ,  $f_1 \circ f_2$ ,  $f_2 \circ f_1$ ,  $f_2 \circ f_2$ . Now, prove the remaining part as above.

**Example 18 :** Prove that  $\mathbb{Z}_4$  where  $\mathbb{Z}_4$  denotes the set of integers  $z$  modulo 4 is a group under addition but is not a group under multiplication.

**Sol. :** We first prepare the addition and multiplication tables.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(1) For  $(\mathbb{Z}_4, \oplus)$  we see that

(i)  $\oplus$  is associative.

$$\text{For example, } (1 \oplus 2) \oplus 3 = 3 \oplus 3 = 2 \\ \text{and } 1 \oplus (2 \oplus 3) = 1 \oplus 1 = 2$$

(ii) 0 is the identity element.

This can be seen to be true from the first row or the first column.

$$0 + 0 = 0, \quad 1 + 0 = 1, \quad 2 + 0 = 2, \quad 3 + 0 = 3.$$

(iii) Additive inverse exists for each element

$$0^{-1} = 0, \quad 1^{-1} = 3, \quad 2^{-1} = 2, \quad 3^{-1} = 1$$

Hence,  $(\mathbb{Z}_4, \oplus)$  is a group.

(2) For  $(\mathbb{Z}_4, \otimes)$ , we see that multiplicative inverse does not exist.

For example,  $2 \times 0 = 0, \quad 2 \times 1 = 2, \quad 2 \times 2 = 0, \quad 2 \times 3 = 2$

The product of 2 with no element of  $\mathbb{Z}_4$  is unity.

Hence,  $2^{-1}$  does not exist.  $\therefore (\mathbb{Z}_4, \otimes)$  is not a group.

In general, if  $\mathbb{Z}_m$  denotes the set of integers modulo  $m$ , then  $\mathbb{Z}_m$  is a group under addition but it is not a group under multiplication.

However, if  $U_m$  denotes a reduced residue system modulo  $m$  which consists of those integers which are relatively prime to  $m$  (i.e. which are not factors or multiples of factors of  $m$ ), then  $U_m$  is a group under multiplication. See the next example.

**Example 19:** Show that  $U_{12} = \{1, 5, 7, 11\}$  which denotes the reduced residue system modulo 12 is a group under multiplication.

Sol.: We first prepare the multiplication table.

(1)  $(U_{12}, \otimes)$  is associative.

For example,  $5 \times (7 \times 11) = 5 \times (5) = 1$

$$\text{and } (5 \times 7) \times 11 = (11) \times 11 = 1$$

(2) 1 is the identity element.

This is clear from the first row or from the first column.

(3) Every element has the inverse and the element itself is its inverse.

This is so because all diagonal elements are unity.

$$\therefore 5 \otimes 5 = 1, \quad 5^{-1} = 5$$

$$\therefore 7 \otimes 7 = 1, \quad 7^{-1} = 7$$

$$\text{Similarly, } 1^{-1} = 1, \quad 11^{-1} = 11.$$

Hence,  $(U_{12}, \otimes)$  is a group.

$\otimes$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

**Example 20:** Let  $S = \{x \mid x \text{ is real and } x \neq 0, x \neq -1\}$ .

Consider the following functions  $f_i: S \rightarrow S, i = 1, 2, \dots, 6$

$$f_1(x) = x, \quad f_2(x) = \frac{1}{x}, \quad f_3(x) = 1-x, \quad f_4(x) = \frac{x}{1-x}, \quad f_5(x) = \frac{1}{1-x}, \quad f_6(x) = \frac{x-1}{x}.$$

Show that  $G = \{f_1, f_2, f_3, \dots, f_6\}$  is a group under the operation of composition. Give the multiplication table for  $G$ .

Sol.: We shall first obtain  $f_i \circ f_j$  for all  $i$  and  $j$ .  
(M.U., 2008, 06, 15)

$$f_1 \circ f_1 = f_1 \circ (x) = x = f_1$$

$$f_1 \circ f_2 = f_1 \circ \left(\frac{1}{x}\right) = \left(\frac{1}{x}\right) = f_2$$

$$f_1 \circ f_3 = f_1 \circ (1-x) = 1-x = f_3$$

$$f_1 \circ f_4 = f_1 \circ \left(\frac{x}{1-x}\right) = \frac{x}{1-x} = f_4$$

$$f_1 \circ f_5 = f_1 \circ \left(\frac{1}{1-x}\right) = \frac{1}{1-x} = f_5$$

$$f_1 \circ f_6 = f_1 \circ \left(\frac{x-1}{x}\right) = \frac{x-1}{x} = f_6$$

Further,  $f_2 \circ f_1 = f_2 \circ (x) = \frac{1}{x} = f_2$

$$f_2 \circ f_2 = f_2 \circ \left(\frac{1}{x}\right) = \frac{1}{1/x} = x = f_1$$

$$f_2 \circ f_3 = f_2 \circ (1-x) = \frac{1}{1-x} = 1-x = f_3$$

$$f_2 \circ f_4 = f_2 \circ \left(\frac{x}{1-x}\right) = \frac{x}{x-1} = \frac{x}{x-1} = f_4$$

$$f_2 \circ f_5 = f_2 \circ \left(\frac{1}{1-x}\right) = 1 - \frac{1}{1-x} = \frac{x-1}{x} = f_5$$

$$f_2 \circ f_6 = f_2 \circ \left(\frac{x-1}{x}\right) = 1 - \frac{x-1}{x} = \frac{1}{x} = f_6$$

Further since  $f_3 = 1 - x$ ,

$$f_3 \circ f_1 = f_3 \circ (x) = 1 - x = f_3$$

$$f_3 \circ f_2 = f_3 \circ \left(\frac{1}{x}\right) = 1 - \frac{1}{x} = \frac{x-1}{x} = f_6$$

$$f_3 \circ f_3 = f_3 \circ (1-x) = 1 - (1-x) = x = f_1$$

$$f_3 \circ f_4 = f_3 \circ \left(\frac{x}{1-x}\right) = 1 - \frac{x}{1-x} = \frac{-x}{1-x} = \frac{x}{x-1} = f_5$$

$$f_3 \circ f_5 = f_3 \circ \left(\frac{1}{1-x}\right) = 1 - \frac{1}{1-x} = \frac{x-1}{x} = f_4$$

$$f_3 \circ f_6 = f_3 \circ \left(\frac{x-1}{x}\right) = 1 - \frac{x-1}{x} = \frac{1}{x} = f_2$$

Also since  $f_4 = \frac{x}{1-x}$ ,

$$f_4 \circ f_1 = f_4 \circ (x) = \frac{x}{1-x} = f_4$$

$$f_4 \circ f_2 = f_4 \circ \left(\frac{1}{x}\right) = \frac{1/x}{(1/x)-1} = \frac{1}{1-x} = f_5$$

$$\begin{aligned}f_4 \circ f_3 &= f_4 \circ (1-x) = \frac{1-x}{(1-x)-1} = \frac{1-x}{-x} = \frac{x-1}{x} = f_6 \\f_4 \circ f_4 &= f_4 \circ \left(\frac{x}{x-1}\right) = \frac{x(x-1)}{x(x-1)-1} = x = f_1 \\f_4 \circ f_5 &= f_4 \circ \left(\frac{1}{1-x}\right) = \frac{1/(1-x)}{1/(1-x)-1} = \frac{1}{x} = f_2 \\f_4 \circ f_6 &= f_4 \circ \left(\frac{x-1}{x}\right) = \frac{(x-1)/x}{(x-1)/x-1} = \frac{x-1}{-1} = 1-x = f_3\end{aligned}$$

To find  $f_5 \circ f_1, \dots, f_6 \circ f_1$  and  $f_6 \circ f_1, \dots, f_6 \circ f_6$  is left to you.

Now we shall see the following.

#### $G_1$ : Associativity

$$\begin{aligned}f_2 \circ f_3 &= f_2 \circ (1-x) = \frac{1}{1-x}, & f_1 \circ (f_2 \circ f_3) &= f_1 \circ \left(\frac{1}{1-x}\right) = \frac{1}{1-x} \\ \text{Also, } f_1 \circ f_2 &= f_2 \circ \frac{1}{x} = \frac{1}{x} & \therefore (f_1 \circ f_2) \circ f_3 &= (f_1 \circ f_2) \circ (1-x) = \frac{1}{1-x} \\ \text{Hence, } f_1 \circ (f_2 \circ f_3) &= (f_1 \circ f_2) \circ f_3 & \therefore \circ \text{ is associative in } G.\end{aligned}$$

#### $G_2$ : Identity

From the above calculations, we find that  $f_1$  is the identity.

#### $G_3$ : Inverse

From the above calculations, we see that every element has an inverse.

For instance inverse of  $f_1$  is  $f_1$ , inverse of  $f_2$  is  $f_2$ , inverse of  $f_3$  is  $f_3$  and so on. Hence,  $G$  is a group under composing.

You can prepare the multiplication table.

**Example 21 :** Write down all permutations taken 3 at a time of the elements of the set  $\{1, 2, 3\}$ .

Show that this set of permutations of the elements of  $\{1, 2, 3\}$  forms a group under the composition of permutations. (M.U. 1997, 99, 2000)

**Sol. :** The permutations of the elements of the set  $\{1, 2, 3\}$  are

- (i)  $(1, 2, 3)$ ;      (ii)  $(1, 3, 2)$ ;      (iii)  $(2, 1, 3)$ ;
- (iv)  $(2, 3, 1)$ ;      (v)  $(3, 1, 2)$ ;      (vi)  $(3, 2, 1)$ .

With  $A = \{1, 2, 3\}$  we define the six (functions) permutations as follows.

$$\begin{aligned}P_1(A) &= 1, 2, 3; & P_2(A) &= 1, 3, 2; & P_3(A) &= 2, 1, 3; \\P_4(A) &= 2, 3, 1; & P_5(A) &= 3, 1, 2; & P_6(A) &= 3, 2, 1.\end{aligned}$$

$P_1(A)$  means keeping the same order

e.g., if  $A = \{3, 2, 1\}$  then  $P_1(A) = 3, 2, 1$ .

$P_6(A)$  means interchanging the first and the last elements

e.g., if  $A = \{3, 2, 1\}$  as above, then  $P_6(A) = \{1, 2, 3\}$ .

Let us denote the set of six permutations (functions) by  $P$ .

$$\therefore P = \{P_1(A), P_2(A), \dots, P_6(A)\}$$

With  $A = \{1, 2, 3\}$  and  $P$  defined as above we consider the following.

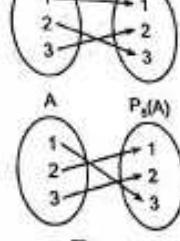
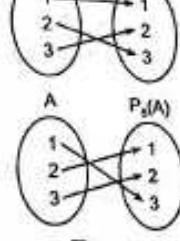
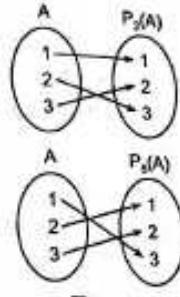
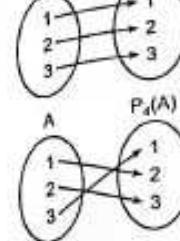
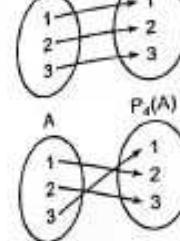
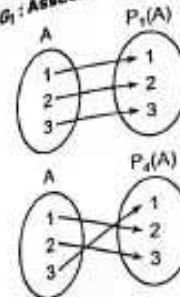


Fig. 10.6

We have, if  $A = \{1, 2, 3\}$ , then:

$$\begin{aligned}P_1(A) &= \{1, 2, 3\}, & P_2(A) &= \{1, 3, 2\}, & P_3(A) &= \{2, 1, 3\} \\P_1(A) \circ P_2(A) &= \{1, 3, 2\} & [\because P_1 \text{ maintains the order}]\end{aligned}$$

Thus, if  $A = \{1, 2, 3\}$ ,  $P_1(A) \circ P_2(A) = \{1, 3, 2\}$ .

$P_1 \circ P_2$  interchanges the last two.

$$\text{But } P_3(A) = \{2, 1, 3\}.$$

$$\therefore (P_1 \circ P_2) \circ P_3 = \{2, 3, 1\}$$

$$\text{Now, } P_2(A) \circ P_3(A) = \{2, 3, 1\} \quad [\because P_2 \text{ interchanges the last two}]$$

$$\therefore P_1 \circ (P_2 \circ P_3) = \{2, 3, 1\} \quad [\because P_1 \text{ maintains the order}]$$

$$\therefore (P_1 \circ P_2) \circ P_3 = P_1 \circ (P_2 \circ P_3)$$

$\therefore \circ$  is associative.

#### $G_2$ : Identity

Since, if  $A = \{1, 2, 3\}$ ,  $P_1(A) = \{1, 2, 3\}$ , we see that  $P_1$  maintains the order

$$\therefore P_1 \circ P_2 = P_2, \quad P_1 \circ P_3 = P_3, \dots, \quad P_1 \circ P_k = P_k$$

#### $G_3$ : Inverse

We see that  $P_1 \circ P_1 = P_1$

$$\begin{aligned}P_2 \circ P_2 &= P_2 \circ (1, 3, 2) = \{1, 2, 3\} \\&= P_1 \quad [\because P_2 \text{ interchanges the last two elements}]\end{aligned}$$

$$P_3 \circ P_3 = P_3 \circ (2, 1, 3) = \{1, 2, 3\} \quad [\because P_3 \text{ interchanges the first two elements}]$$

and so on.

Each function is the inverse of itself.  $\therefore (G, \circ)$  is a group.

**Example 22 :** Let  $Q$  be the set of all positive rational numbers which can be expressed as  $2^a 3^b$  where  $a, b$  are integers.

Prove that  $(Q, *)$  is a group where  $*$  is usual multiplication.

**Sol. :** We have  $2^{a_1} 3^{b_1} * 2^{a_2} 3^{b_2} = 2^{a_1+a_2} 3^{b_1+b_2} = 2^a 3^b$

$\therefore Q$  is closed under  $*$ .

(M.U. 2002, 06, 12)

**G<sub>1</sub> : Associativity**

Consider  $(2^{a_1} 3^{b_1}) * (2^{a_2} 3^{b_2} * 2^{a_3} 3^{b_3}) = (2^{a_1} 3^{b_1}) * (2^{a_2 + a_3} 3^{b_2 + b_3})$   
 $= 2^{a_1 + a_2 + a_3} 3^{b_1 + b_2 + b_3} = 2^a 3^b$

Again  $(2^{a_1} 3^{b_1} * 2^{a_2} 3^{b_2}) * 2^{a_3} 3^{b_3} = (2^{a_1 + a_2} 3^{b_1 + b_2}) * 2^{a_3} 3^{b_3}$   
 $= 2^{a_1 + a_2 + a_3} 3^{b_1 + b_2 + b_3} = 2^a 3^b$

$\therefore (G, *)$  is associative.

**G<sub>2</sub> : Identity**

If  $a = 0, b = 0, 2^0 3^0 = 1$   
 $\therefore (2^0 3^0) * (2^0 3^0) = 2^0 3^0 \cdot 1 = 2^0 3^0 \quad \therefore 2^0 3^0$  is an identity.

**G<sub>3</sub> : Inverse**

Consider  $(2^a 3^b) * (2^{-a} 3^{-b}) = 2^{a-a} 3^{b-b} = 2^0 3^0 = 1$   
 $\therefore 2^{-a} 3^{-b}$  is the inverse of  $2^a 3^b$ .  $\therefore (G, *)$  is a group.

**Example 23 :** If  $S$  is a non-empty set, prove that the  $P(S)$  (power set of  $S$ ) with  $*$  where  $A * B$  is defined as symmetric difference is an Abelian group.

**Sol. :** Clearly, if  $A, B \in S$ , then  $A * B$  also belongs to  $S$ .

(M.U. 2006)

$\therefore P(S)$  is closed under  $*$ .

**G<sub>1</sub> : Associativity**

$$\begin{aligned} A * B &= \{x \mid x \text{ belongs to } A \text{ or } B\} \\ (A * B) * C &= \{x \mid x \text{ belongs to } A \text{ or } B \text{ or } C\} \\ (B * C) &= \{x \mid x \text{ belongs to } B \text{ or } C\} \\ A * (B * C) &= \{x \mid x \text{ belongs to } A \text{ or } B \text{ or } C\} \\ (A * B) * C &= A * (B * C) \end{aligned}$$

$\therefore *$  is associative.

**G<sub>2</sub> : Identity**

$\Phi$  is an identity element.

$$\begin{aligned} A * \Phi &= \{x \mid x \text{ belongs to } A \text{ or } \Phi\} \\ &= \{x \mid x \text{ belongs to } A\} \quad [\because \Phi \text{ has no elements}] \\ \therefore A * \Phi &= A \text{ for each } A. \end{aligned}$$

**G<sub>3</sub> : Inverse**

$$\begin{aligned} \text{Since } A * \bar{A} &= \{x \mid x \text{ belongs to } A \text{ or } \bar{A}\} \\ &= \Phi \quad [\because \text{No element belongs to } A \text{ and } \bar{A} \text{ simultaneously}] \end{aligned}$$

$\therefore \bar{A}$  is the inverse of  $A$ .

**G<sub>4</sub> : Commutativity**

Clearly  $A * B = B * A$

$\therefore (G, *)$  is an Abelian group.

**Example 24 :** Let  $(A, *)$  be a monoid such that for every  $x \in A$ ,  $x * x = e$  where  $e$  is the identity (i.e., every element is its own inverse). Show that  $(A, *)$  is an Abelian group. (M.U. 2000, 01)

OR If every element in a group is its own inverse then the group is Abelian. (M.U. 2013, 15)

**Sol. :** (i) Since  $(A, *)$  is a monoid,  $*$  is associative over  $A$ .  
(ii) Since  $(A, *)$  is a monoid, it has an identity element.  
(iii) Since  $x * x = e$  and  $e$  is the identity element, for every  $x$ , its inverse exists and every element is its inverse.

$\therefore (A, *)$  is a group.

Since by data  $e$  is the identity

But by data

Let us denote

Then from (2),  $b = e$  and then from (1),  $x * b = b * x$  for all  $x \in A$ .

$\therefore (A, *)$  is an Abelian group.

$x * e = e * x = x$

$y * y = e$

$y * y = b$

(1)

$y * y = b$

(2)

**(ii) Congruence Relation**

**Definition :** If  $m$  is any positive integer and if  $a, b$  are any integers then  $a$  is said to be congruent to  $b$  modulo  $m$  if  $m$  divides  $(a - b)$  (i.e. if  $\frac{a-b}{m}$  has zero remainder).

We write this as  $a \equiv b \pmod{m}$ . If the remainder is not zero we write it as  $a \not\equiv b \pmod{m}$ . For example,

- (i)  $81 \equiv 21 \pmod{5}$   $\therefore 5$  divides  $81 - 21 = 60$ .
- (ii)  $58 \equiv 16 \pmod{7}$   $\therefore 7$  divides  $58 - 16 = 42$ .
- (iii)  $34 \not\equiv 12 \pmod{3}$   $\therefore 3$  does not divide  $34 - 12 = 22$ .
- (iv)  $25 \not\equiv 7 \pmod{4}$   $\therefore 4$  does not divide  $25 - 7 = 18$ .

**Theorem :** Congruence modulo  $m$  is an equivalence relation in  $\mathbb{Z}$ .

**Proof :** Let  $m$  be a positive integer.

(i) If  $a$  is any integer  $a - a = 0$ , is divisible by  $m$ .

$\therefore a \equiv a \pmod{m}$  (Reflexivity)

(ii) If  $a \equiv b \pmod{m}$  i.e. if  $(a - b)$  is divisible by  $m$  then  $(b - a) = -(a - b)$  is also divisible by  $m$ .

$\therefore$  If  $a \equiv b \pmod{m}$ , then  $b \equiv a \pmod{m}$  (Symmetry)

(iii) If  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ , then  $(a - b)$  is divisible by  $m$  and  $(b - c)$  is divisible by  $m$ .

$\therefore$  The sum  $(a - b) + (b - c) = a - c$  is also divisible by  $m$ .

$\therefore$  If  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ , then  $a \equiv c \pmod{m}$  (Transitivity)

$\therefore$  Congruence is an equivalence relation.

**Remarks ...**

(i) If  $a$  is congruent to an integer in the set  $S = \{0, 1, 2, \dots, (m-1)\}$  then that integer is unique.

In other words  $a$  cannot be congruent to two integers of the set  $S$ .

(ii) If  $a \equiv b \pmod{m}$  then  $a$  and  $b$  when divided by  $m$  leave the same remainder.

(iii) The set obtained from  $\mathbb{Z}$  modulo  $m$  is denoted by  $\mathbb{Z}_m$ , the operation of addition on  $\mathbb{Z}_m$  is denoted by  $+_m$  and operation of multiplication on  $\mathbb{Z}_m$  is denoted by  $\times_m$ .

**Example 1 :** Find a set of three real numbers that is closed under addition modulo 2 and multiplication modulo 2.  
**Sol. :** Consider the set  $\{-1, 0, 1\}$  and prepare the two tables addition modulo 2 and multiplication modulo 2.

$x_2$	-1	0	1
-1	0	-1	0
0	-1	0	1
1	0	1	0

$x_2$	-1	0	1
-1	-1	0	-1
0	0	0	0
1	-1	0	1

**Example 2 :** Prove that the set  $A = \{0, 1, 2, 3, 4, 5\}$  is a finite Abelian group under addition modulo 6.  
**Sol. :** We first prepare the table of addition modulo 6 denoted by  $\oplus$ .

From the table, it is obvious that  $\oplus$  is a binary operation.

**G1 :** From the table we see that  $\oplus$  is associative.

$$\text{e.g., } 2 \oplus (3 \oplus 5) = 2 \oplus (2) = 4 \quad \text{and} \quad (2 \oplus 3) \oplus 5 = (5) \oplus 5 = 4.$$

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	6 = 0
2	2	3	4	5	6 = 0	7 = 1
3	3	4	5	6 = 0	7 = 1	8 = 2
4	4	5	6 = 0	7 = 1	8 = 2	9 = 3
5	5	6 = 0	7 = 1	8 = 2	9 = 3	10 = 4

**G2 :** The first column or the first row shows that 0 is the identity for  $\oplus$ .

**G3 :** The positions of 0 the additive inverse in every row (and every column) show that every element of  $A$  has the additive inverse. e.g.,  $1 \oplus 5 = 0$ .

Hence, inverse of 1 is 5 and inverse of 5 is 1.

$$\text{Also } \because 3 \oplus 3 = 0 \quad \therefore (3)^{-1} = 3$$

$$\text{Further, } 2 \oplus 4 = 0 \quad \therefore (2)^{-1} = 4 \text{ etc.}$$

$\therefore G$  is a group under addition modulo 6.

**G4 :** Further  $a \oplus b = b \oplus a$ . e.g.,  $4 \oplus 5 = 3$  and  $5 \oplus 4 = 3$

$$\therefore 4 \oplus 5 = 5 \oplus 4. \quad \therefore G$$
 is an Abelian group.

**Example 3 :** Prove that  $A = \{1, 2, 3, 4, 5, 6\}$  is a finite Abelian group under multiplication modulo 7.  
**Sol. :** We first prepare the table of multiplication modulo 7 denoted by  $\otimes$ . From the table it is clear that  $\otimes$  is a binary operation.

**G1 :** From the table, we see that  $\otimes$  is associative.

$$\text{e.g., } 2 \otimes (3 \otimes 5) = 2 \otimes 1 = 2$$

$$\text{and } (2 \otimes 3) \otimes 5 = 6 \otimes 5 = 2$$

**G2 :** The first column (or the first row) show that 1 is the identity for  $\otimes$ .

$\otimes$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

**G3 :** The positions of the multiplicative identity 1 in every row (and every column) show that every element of  $A$  has the multiplicative inverse.

$$\text{e.g., } 2 \otimes 4 = 1 \quad \text{and} \quad 4 \otimes 2 = 1$$

$$\therefore (2)^{-1} = 4 \quad \text{and} \quad (4)^{-1} = 2$$

$\therefore G$  is a group modulo 7.

**G4 :** Further,  $a \otimes b = b \otimes a$

$$\text{e.g., } 4 \otimes 5 = 6 \quad \text{and} \quad 5 \otimes 4 = 6$$

$\therefore G$  is an Abelian Group.

Some Algebraic Structures  
 (M.U. 2006)

$X_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

**Example 4 :** Let  $Z_4$  i.e.,  $G = \{0, 1, 2, 3\}$ . (i) Prepare the composition table with respect to  $X_4$ .  
 (ii) Is it a group?

**Sol. :**  $X_4$  denotes the operation of multiplication modulo 4 and composition table means the table in which this operation is shown.  
 (See the adjoining table.)

From the table, we see that  $G$  is closed under the operation  $X_4$  as all elements in the adjoining table are elements of  $G$ .

**G1 :** From the table, we see that  $\otimes$  is associative.

$$\text{e.g., } 2 \otimes (3 \otimes 1) = 2 \otimes (3) = 2 \otimes 3 = 2$$

$$\text{and } (2 \otimes 3) \otimes 1 = 2 \otimes (1) = 2 \otimes 2 = 2$$

**G2 :** From the second row (or second column) we see that, 1 is the identity element.

$$0 \otimes 1 = 0, \quad 1 \otimes 1 = 1, \quad 2 \otimes 1 = 3, \quad 3 \otimes 1 = 3$$

**G3 :** In the row (or column) of 2, we see that,  $2 \otimes 0 = 0, 2 \otimes 1 = 2, 2 \otimes 2 = 0, 2 \otimes 3 = 2$ . Thus, we do not get an identity element and hence, 2 does not have a inverse.

$\therefore G$  under multiplication modulo 4 is not a group.

### (b) Residue Classes

Since congruence is an equivalence relation, it partitions  $\mathbb{Z}$ , the set of integers into disjoint equivalence classes called the residue classes modulo  $m$ . The residue class of  $a$  is the set of integers which are congruent to  $a$  modulo  $m$ . The residue class of  $a$  is denoted by  $[a]$ . Thus,  $[a] = \{x \mid x \in \mathbb{Z} \text{ and } x \equiv a\}$ .

For example, if  $m = 5$ , we have

$$[0] = \{ \dots, -10, -5, 0, 5, 10, \dots \}$$

$$[1] = \{ \dots, -9, -4, 1, 6, 11, \dots \}$$

$$[2] = \{ \dots, -8, -3, 2, 7, 12, \dots \}$$

$$[3] = \{ \dots, -7, -2, 3, 8, 13, \dots \}$$

$$[4] = \{ \dots, -6, -1, 4, 9, 14, \dots \}$$

### (c) Congruence Relation On Semi-group

**Definition :** An equivalence relation  $R$  on the semi-group  $(S, *)$  is called a congruence relation on the semi-group if  $a R a'$  and  $b R b'$ , then  $(a * b) R (a' * b')$ .

**Example :** Consider the semi-group  $(\mathbb{Z}, +)$  and the relation  $R$  defined by  $a R b$  if and only if  $a \equiv b \pmod{3}$ .

Prove that  $R$  is a congruence relation on the semi-group  $S$ .

Sol. : Considering the above definition we have to prove that if  $a, a', b, b' \in S$  and if  $a R b$  and  $a' R b'$ , then  $(a + a') R (b + b')$  i.e. we have to prove that if  $a = a' \pmod{3}$  and  $b = b' \pmod{3}$  then  $a + b = a' + b' \pmod{3}$ . Now, since  $a = a' \pmod{3}$ ,  $(a - a') = 3m$  say and since  $b = b' \pmod{3}$ ,  $(b - b') = 3n$ , say, where  $m$  and  $n$  are integers.

$$\begin{aligned} & a - a' + b - b' = 3m + 3n \\ & (a + b) - (a' + b') = 3(m + n) \\ & (a + b) = (a' + b') \pmod{3} \end{aligned}$$

Hence, the result.

**(d) Cyclic Group**

Definition : A group  $(G, *)$  is said to be a cyclic group if there exists an element  $a \in G$  such that every element of  $G$  can be written as some power of  $a$  viz.  $a^k$  for some integer  $k$  where by  $a^k$  we mean  $a \times a \times a \dots \times a$  ( $k$  times).

Then  $G$  is said to be generated by  $a$  or  $a$  generates  $G$ .

A cyclic group is always Abelian because commutativity is observed.

$$\therefore \text{If } a^r, a^s \in G, \text{ then } a^r \times a^s = a^s \times a^r.$$

**Example 1 :** The cube roots of unity form a cyclic group under multiplication of complex numbers.

Sol. : In Example 2, page 16-13, we have proved that the cube roots of unity is a group under multiplication.

Now, we shall prove that it is cyclic i.e., every element of the group  $1, \omega, \omega^2$  can be expressed as integral power of some element  $a \in G$ .

$$\text{We note that } \omega^0 = 1, \omega^1 = \omega, \omega^2 = \omega^2.$$

Thus, the element  $1, \omega, \omega^2$  are expressed as  $0^{\text{th}}, 1^{\text{st}}$  and  $2^{\text{nd}}$  power of  $\omega$ . Hence, the group is cyclic with  $\omega$  as a generator.

$$\text{Also, } (\omega^2)^0 = 1, (\omega^2)^1 = \omega^2, (\omega^2)^2 = \omega^4 = \omega^3 \cdot \omega = \omega.$$

$$\text{Thus, } 1, \omega, \omega^2 \text{ are expressed as } 0^{\text{th}}, 1^{\text{st}} \text{ and } 2^{\text{nd}} \text{ power of } \omega^2.$$

Hence, the group is cyclic with  $\omega^2$  as a generator.

**Example 2 :** Prove that the group  $G = \{0, 1, 2, 3, 4, 5\}$  is a finite, abelian, cyclic group under addition modulo 6.

Sol. : We have proved in Example 2, page 16-27 that  $G$  is an Abelian group.

Now, we shall prove that it is a cyclic group i.e., every element of the group  $G$  can be expressed as integral power of some element  $a \in G$ .

$$\text{We note that } 1^1 = 1, 1^2 = 1+6, 1 = 2, 1^3 = 1+1_6 1^2 = 1+6 2 = 3,$$

$$1^4 = 1+6 1^3 = 1+6 3 = 4, 1^5 = 1+6 1^4 = 1+6 4 = 5,$$

$$1^6 = 1+6 1^5 = 1+6 5 = 0. \quad [\text{See the table on page 16-27}]$$

$$\text{Hence, } G = \{1^6, 1^1, 1^2, 1^3, 1^4, 1^5\}.$$

$\therefore G$  is a cyclic group with 1 as a generator.

(It can be shown that 5 is another generator.)

**Subgroup** : Let  $H$  be a subset of group  $G$ , such that

- (i) the identity element  $e$  of  $G$  belongs to  $H$ ,
- (ii) if  $a, b$  belong to  $H$  then  $a + b$  also belongs to  $H$ ,

(iii) If  $a \in H$  then  $a^{-1} \in H$ . Then  $H$  is called a subgroup of  $G$ .

In short a subgroup is a subset of  $G$  having all the properties of a group.

**Illustrations :** (i) Let  $G$  be the group of all non-zero complex numbers  $a + ib$  where  $a, b$  are real under multiplication.

Let  $H = \{a + ib \mid a^2 + b^2 = 1\}$  then  $H$  is a subgroup of  $G$ .

(ii) Let  $G$  be the group of  $2 \times 2$  matrices  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  such that  $ad - bc \neq 0$  under matrix multiplication.

Let  $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad \neq 0 \right\}$ , then  $H$  is a subgroup of  $G$ .

**Example 1 :** Consider the group  $Z$  of integers under addition.

Let  $H = \{\dots, -3m, -2m, -m, 0, m, 2m, 3m, \dots\}$  where  $m$  is a positive integer.

Show that  $H$  is a subgroup of  $Z$ .

Sol. : (i) The identity of element of  $G$  is 0 and 0 belongs to  $H$ .

(ii) If  $km$  and  $lm$  are any two elements of  $H$ , then

$$(km + lm) = (k + l)m \text{ is also an element of } H.$$

(iii) If  $km$  is an element of  $H$ , then its negative (inverse)  $-km$  is also an element of  $H$ .

$H$  is a subgroup.

**Example 2 :** Find the subgroups of  $(Z_5, \oplus)$  where  $\oplus$  is the operation addition modulo 5.

Sol. : The operation addition modulo 5 is given by the adjoining table.

From the first row and first column we see that 0 is the identity element.

$\oplus$	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

Hence, we consider two subgroups of  $(Z_5, \oplus)$  viz.  $G_1 = \{0, 1, 4\}$  and  $G_2 = \{0, 2, 3\}$ .

Now, by definition of subgroup  $H$  is a subgroup if

- (i) the identity element  $e$  belongs to  $H$ ,

- (ii) if  $a, b$  belongs to  $H$  then  $a \oplus b$  belongs to  $H$ ,

- (iii) if  $a$  belongs to  $H$  then  $a^{-1}$  belongs to  $H$ .

The above properties are satisfied by  $\{0, 1, 4\}$  and  $\{0, 2, 3\}$  under  $\oplus$  and hence they are subgroups.

**Example 3 :** Consider the set  $A = \{1, 2, 3, 4, 5, 6\}$  under the multiplication modulo 7.

- Construct the multiplication table.
- Find the inverses of 2, 3, 5 and 6.
- Prove that  $A$  is a cyclic group.
- Find the subgroups generated by  $\{3, 4\}$  and  $\{2, 3\}$  and state their orders. (M.U. 1999, 2000, 16)

**Sol. :** (i) The multiplication table is given by the adjoining table.

From the first column and the first row we see that 1 is the identity element.

(ii) From the table we see that  $2 \cdot 4 = 1$  and  $4 \cdot 2 = 1$ .

$\therefore$  Inverse of 2 is 4.

Also since  $3 \cdot 5 = 1$  and  $5 \cdot 3 = 1$   $\therefore$  Inverse of 3 is 5.

Since  $5 \cdot 3 = 1$  and  $3 \cdot 5 = 1$   $\therefore$  Inverse of 5 is 3.

Since  $6 \cdot 6 = 1$ , inverse of 6 is 6.

(iii) We observe that

$$\begin{array}{lll} 3^1 = 3, & 3^2 = 9_7 = 2, & 3^3 = 27_7 = 6, \\ 3^4 = 81_7 = 4, & 3^5 = 243_7 = 5, & 3^6 = 729_7 = 1. \end{array}$$

Thus, each element of  $A$  can be written as  $3^k$ .

Hence,  $(A, \cdot)$  is a cyclic group and 3 is its generator.

(iv) The subgroup generated by  $\{3, 4\}$  is denoted by  $\langle \{3, 4\} \rangle$ .

Clearly the elements  $\{3, 4\}$  belong to the subgroup  $\langle \{3, 4\} \rangle$ .

The inverse of 3 is 5 and inverse of 4 is 2 and they belong to the subgroup  $\langle \{3, 4\} \rangle$ .

The identity element 1 belongs to the subgroup.

Thus, the elements 1, 2, 3, 4, 5 belong to the subgroup  $\langle \{3, 4\} \rangle$ .

Let us check whether the remaining element 6 also belongs to the subgroup.

Now, since  $4 \in \langle \{3, 4\} \rangle$  and  $5 \in \langle \{3, 4\} \rangle$

$4 \cdot 5$  must belong to the subgroup.

But  $4 \cdot 5_7 = 6$ . Hence,  $6 \in \langle \{3, 4\} \rangle$

$\therefore$  The subgroup of  $\{3, 4\}$  is  $\{1, 2, 3, 4, 5, 6\}$  the set  $A$ . Its order i.e. the number of elements is 6.

Similarly, you can prove that the subgroup of  $\{2, 3\}$  is the set  $A$  itself.

**Example 4 :** Let  $G$  be a reduced system modulo 15 i.e.,  $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$  (i.e., the set of integers between 1 and 15 which are relatively prime to 15 i.e. the integers which are not the factors of 15 or the multiples of the two factors 3, 5 from 1 to 15).

Then,  $G$  is a group under multiplication modulo 15.

- Construct the multiplication table.
- Find  $2^{-1}, 7^{-1}, 11^{-1}$ .
- Is  $G$  cyclic?
- Find the order and the sub-groups generated by 2, 7, 11.

**Sol. :** (a) To prepare the multiplication table we find the remainder when the product of any two elements  $ab$  is divided 15. We thus get the following table,

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

From the first row (or the column), we find that 1 is the identity element.

(b) Since 1 is the multiplicative identity  $b$  is the inverse of  $a$  if  $a \otimes b = 1$ .

From the table, we find that  $2^{-1} = 8, 7^{-1} = 13, 11^{-1} = 11$ .

(c) Since  $2^2 = 4, 2^3 = 8, 2^4 = 1$ , the sub-group generated by 2 is  $\{1, 2, 4, 8\}$ .

The number of elements in this group i.e. the order of this group  $|2| = 4$ .

Since  $7^2 = 7 \cdot 7 = 4, 7^3 = (7 \cdot 7) \cdot 7 = 4 \cdot 7 = 13, 7^4 = (7 \cdot 7 \cdot 7) \cdot 7 = 13 \cdot 7 = 1$ , the sub-

group generated by 7 is  $\{1, 4, 7, 13\}$ . The number of elements in the sub-group i.e.  $|7| = 4$ .

Since  $11^2 = 1$ , the sub-group generated by 11 is  $\{1, 11\}$  and  $|11| = 2$ .

(d) Since no element generates  $G$ ,  $G$  is not cyclic.

**Example 5 :** Consider  $G = \{1, 5, 7, 11, 13, 17\}$  a reduced system modulo 18 (i.e. the set of integers between 1 and 18 which are relatively prime to 18). Then  $G$  is a group under multiplication.

(i) Construct the multiplication table.

(ii) Find  $5^{-1}, 7^{-1}, 17^{-1}$ .

(iii) Find the order and the sub-groups generated by 5, 7, 17.

(iv) Is  $G$  cyclic?

**Sol. :** (i) The multiplication table is as shown in adjoining table.

1 is the identity.

(ii)  $5^{-1} = 11, 7^{-1} = 13, 17^{-1} = 17$ .

(iii) Now  $5^2 = 5 \otimes 5 = 7, 5^3 = 5 \otimes 5 \otimes 5 = 7 \otimes 5 = 17, 5^4 = 17 \otimes 5 = 13, 5^5 = 13 \otimes 5 = 11, 5^6 = 11 \otimes 5 = 1$ .

$\therefore$  Sub-group of 5 is  $\{1, 5, 7, 11, 13, 17\} = G$  and  $|5| = 6$ .

i.e., the number of elements in sub-group of 5 is 6. Hence, the order is 6.

Since  $7^2 = 7 \otimes 7 = 13, 7^3 = 13 \otimes 7 = 1$ .

Sub-group of 7 is  $\{1, 7, 13\}$  and  $|7| = 3$ .

Since  $17^2 = 17 \otimes 17 = 1$ , sub-group of 17 is  $\{1\}$  and  $|17| = 1$ .

(iv) The group  $G$  is cyclic. Sub-group of 5 is  $G$ .

*	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

(M.U. 2002, 05, 07, 10, 13)  
A subgroup of an Abelian group is normal.

**Example 1 :** Prove that "congruence modulo  $H$ " is an equivalence relation.

Sol. : By definition of "Congruence modulo  $H$ "  $a R b$  means  $a + b^{-1} \in H$ .

(i)  $R$  is reflexive

$$\therefore a + a^{-1} = a \text{ and } a \in H \quad \therefore R \text{ is reflexive.}$$

(ii)  $R$  is symmetric

$$\therefore a R b \quad \therefore a + b^{-1} \in H$$

Since,  $(a + b^{-1}) \in H$ ,  $(a + b^{-1})^{-1} \in H$

$$\therefore b + a^{-1} \in H \quad \therefore R \text{ is symmetric.}$$

(iii)  $R$  is transitive

If  $a R b$  then  $a + b^{-1} \in H$

If  $b R c$  then  $b + c^{-1} \in H$

$$\therefore (a + b^{-1}) + (b + c^{-1}) \in H$$

$$\therefore a + (b^{-1} + b) + c^{-1} \in H$$

$$\therefore a + c^{-1} \in H$$

$$\therefore a + c^{-1} \in H \quad \therefore a R c \quad \therefore R \text{ is transitive.}$$

Hence,  $R$  is an equivalence relation.

**Example 2 :** Find all cosets of the sub-group  $H = 3 \cdot Z$  of the group  $(Z, +)$ .

Sol. : We have  $Z = \dots, -4, -3, -2, -1, 0, 1, 2, 3, \dots$

$$\text{and } H = 3 \cdot Z = \{-7, -6, -3, 0, 3, 6, \dots\}$$

$$\text{Now, } H+0 = \dots, -6, -3, 0, 3, 6, \dots = H$$

$$H+1 = \dots, -5, -2, 1, 4, 7, \dots = H_1$$

$$H+2 = \dots, -4, -1, 2, 5, 8, \dots = H_2$$

$$H+3 = \dots, -3, 0, 3, 6, 9, \dots$$

$$\text{But } H+3 = H+0.$$

Hence,  $H, H+1, H+2$  are the only three distinct right cosets of  $H$  in  $Z$ .

Further all these cosets partition the set  $Z$  into three disjoint subsets such that

$$H \cup H_1 \cup H_2 = Z$$

Further, since  $G$  is abelian,  $H$  is abelian and  $ah = ha$ . Hence, every right coset is equal to the left coset.

$$\therefore H+1 = 1+H, \quad H+2 = 2+H.$$

**Example 3 :** Find all the cosets of the sub-group  $H = 2 \cdot Z$  of the sub-group  $(Z, +)$  in  $Z$ .

Sol. : Left to you.

**Example 4 :** Let  $G = Z_6$ . Find the left and right cosets of  $H = \{[0], [3]\}$ .

Is  $H$  a normal subgroup of the group  $Z_6$ .

The table of  $Z_6$  (Here + stands for  $\oplus$ )

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

The group  $Z_6$  is abelian because  $a + b = b + a$  for  $a, b \in Z_6$

$$\text{e.g., } 1 + 2 = 3 \text{ and } 2 + 1 = 3.$$

Now, left coset of  $H = \{[0], [3]\}$  with respect to  $a$  in the set  $Z_6$  is

$$aH = \{a + h \mid h \in H\}$$

$$\therefore 0H = \{0 + 0, 0 + 3\} = \{0, 3\},$$

$$1H = \{1 + 0, 1 + 3\} = \{1, 4\},$$

$$2H = \{2 + 0, 2 + 3\} = \{2, 5\},$$

$$3H = \{3 + 0, 3 + 3\} = \{3, 0\},$$

$$4H = \{4 + 0, 4 + 3\} = \{4, 1\},$$

$$5H = \{5 + 0, 5 + 3\} = \{5, 2\}.$$

Now, the right coset of  $H = \{[0]_6, [3]_6\}$  with respect to  $a$  in the set is

$$Ha = \{h + a \mid h \in H\}$$

$$\therefore H0 = \{0 + 0, 3 + 0\} = \{0, 3\},$$

$$H1 = \{0 + 1, 3 + 1\} = \{1, 4\},$$

$$H2 = \{0 + 2, 3 + 2\} = \{2, 5\},$$

$$H3 = \{0 + 3, 3 + 3\} = \{3, 0\},$$

$$H4 = \{0 + 4, 3 + 4\} = \{4, 1\},$$

$$H5 = \{0 + 5, 3 + 5\} = \{5, 2\}.$$

Clearly, we have

$$0H = H0, \quad 1H = H1, \quad 2H = H2, \quad 3H = H3, \quad 4H = H4, \quad 5H = H5.$$

$\therefore H$  is a normal subgroup of  $Z_6$ .

**Example 5 :** Let  $G = Z_8$ . Determine the left cosets of  $H = \{[0], [4]\}$  in  $G$ .

(M.U. 2005)

Sol. :

The table of  $Z_8$  (Here + stands for  $\oplus$ )

$\oplus_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Now, left coset of  $H = \{[0], [4]\}$  with respect to  $a$  in the  $Z_8$  is

$$aH = \{a + h \mid h \in H\}$$

$$\therefore 0H = \{0 + 0, 0 + 4\} = \{0, 4\},$$

$$1H = \{1 + 0, 1 + 4\} = \{1, 5\},$$

$$2H = \{2 + 0, 2 + 4\} = \{2, 6\},$$

$$3H = \{3 + 0, 3 + 4\} = \{3, 7\},$$

$$4H = \{4 + 0, 4 + 4\} = \{4, 0\},$$

$$5H = \{5 + 0, 5 + 4\} = \{5, 1\},$$

$$6H = \{6 + 0, 6 + 4\} = \{6, 2\},$$

$$7H = \{7 + 0, 7 + 4\} = \{7, 3\}.$$

**Example 6 :** Let  $G = \mathbb{Z}_6$ . Determine all right cosets of  $H = \{[0], [4]\}$  in  $G$ .

Sol. : Left to you.

(g) **Product Group**

**Definition :** If  $G_1$  and  $G_2$  are groups and  $G = G_1 \times G_2$  then  $G$  is called a product group under the operation defined by

$$(a_1, b_1) * (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$$

**Example :** Let  $G_1 = G_2 = \mathbb{Z}_2$ . If  $\bar{0}$  denotes the equivalence class  $[0]$ , and  $\bar{1}$  denotes the equivalence class  $[1]$ , then the multiplication table for the product group  $G_1 \times G_2$  is given by

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

(M.U. 2000)

**(h) Quotient**  
We know that an equivalence relation  $R$  defined on a set  $A$  induces a partition of  $A$  denoted by  $A/R$ . In the same way the equivalence relation  $R$ , mod  $m$  induces a partition of the set  $S$  of the semi-group  $(S, *)$  which we denote by  $S/R$ .  $S/R$  is called quotient.

**Example :** If  $A$  is the set of natural numbers and  $R$  is the relation defined by  $aRb$  if  $a=b \pmod{5}$ , then prove that  $(A/R, \oplus)$  is a group where  $A/R$  denotes the quotient group induced on  $A$  by  $R$  and  $\oplus$  the addition on residue classes i.e.  $[a] \oplus [b] = [a+b]$ .

Sol. : The partition induced on  $A$  by the relation  $a=b \pmod{5}$  is given by

$$\begin{aligned} [0] &= \{ \dots, -10, -5, 0, 5, 10, \dots \} = [5] = [10] = \dots \\ [1] &= \{ \dots, -9, -4, 1, 6, 11, \dots \} = [1] = [6] = \dots \\ [2] &= \{ \dots, -8, -3, 2, 7, 12, \dots \} = [2] = [7] = \dots \\ [3] &= \{ \dots, -7, -2, 3, 8, 13, \dots \} = [3] = [8] = \dots \\ [4] &= \{ \dots, -6, -1, 4, 9, 14, \dots \} = [4] = [9] = \dots \end{aligned}$$

Thus, we have  $A/R = \{[0], [1], [2], [3], [4]\}$

and  $[a] \oplus [b] = [a+b]$ .

$$\text{e.g., } [2] \oplus [3] = [2+3] = [5]$$

With this understanding we can prepare the following table for  $\oplus$  on  $A/R$ .

$\oplus$	[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]

From this table it is clear that  $\oplus$  is a binary operation.

**G1: Associativity**

$$[a] \oplus ([b] \oplus [c]) = [a] \oplus [b+c] \\ = [a+(b+c)] = [a+b+c] \quad [\text{By associativity in } A]$$

Similarly,  $([a] \oplus [b]) \oplus [c] = a+b+c$ .

This proves associativity.

**G2:** From the first row (column) we see that  $[0]$  is the identity for  $\oplus$ .

**G3:** Since in each row and column we find the identity element, every element has its inverse.

$$[0]^{-1} = [0], \quad [1]^{-1} = [4], \quad [2]^{-1} = [3]$$

$$\text{because } [0] \oplus [0] = [0], \quad [1] \oplus [4] = [0], \quad [2] \oplus [3] = [0].$$

Hence,  $(A/R, \oplus)$  is a group.

**Definition :** If  $R$  is a congruence relation defined on a semi-group  $(S, *)$  or on a group  $(G, \cdot)$  and  $(S/R, \oplus)$  or  $(G/R, \oplus)$  is the corresponding quotient semi-group or group defined as above, then the function  $f_R: S \rightarrow S/R$  or  $f_R: G \rightarrow G/R$  defined by  $f_R(a) = [a]$  is an homomorphism called natural homomorphism.

**Example 1 :** Find the natural homomorphism  $f_R: G \rightarrow G/R$  for the set  $A$  of natural numbers and the relation  $R$  defined by  $aRb$  if  $a = b \pmod{5}$ .

Sol. : From the table given the previous page, it is clear that the natural homomorphism is given by  $0 \rightarrow [0], 1 \rightarrow [1], 2 \rightarrow [2], 3 \rightarrow [3], 4 \rightarrow [4]$ .

**Example 2 :** Consider the following semigroup defined on  $S = \{a, b, c, d\}$  by the operation  $*$  given by the adjoining table.

Show that  $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a), (c, d), (d, c)\}$  is an equivalence relation.

Find the quotient semi-group  $(S/R, \oplus)$  induced by  $R$ .

Find the operation table for  $(S/R, \oplus)$ . Find the natural homomorphism  $f_R: S \rightarrow S/R$ .

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Sol. : It is easy to prove that  $R$  is an equivalence relation and is left to you as an exercise.

The partition  $S/R$  induced by  $R$  is  $\begin{array}{|c|c|} \hline a & c \\ \hline b & d \\ \hline \end{array}$  because every element in the block is related to the elements in the same block.

We denote this as congruence classes.  $[a] = \{a, b\}, [c] = \{c, d\}$

Now, by definition  $[a] \oplus [b] = [a+b]$

From the given table, we find that

$$[a] \oplus [a] = [a+a] = [a]$$

$$[c] \oplus [a] = [c+a] = [c]$$

$$[a] \oplus [c] = [a+c] = [c]$$

$$[c] \oplus [c] = [c+c] = [c]$$

Hence, we get the table.

*	[a]	[c]
[a]	[a]	[c]
[c]	[c]	[a]

The natural homomorphism (from partition table).

$$(a) \rightarrow [a], (b) \rightarrow [a], (c) \rightarrow [c], (d) \rightarrow [c]$$

**Example 3 :** Consider the monoid  $S = \{a, b, c, d\}$  with the operation  $*$  defined by the adjoining table.

Consider the congruence relation

$$R = \{(d, d), (d, a), (a, d), (a, a), (b, b), (b, c), (c, b), (c, c)\}$$

- (i) Write operation table of the quotient monoid  $S/R$ .  
(ii) Find the natural homomorphism  $f_R : S \rightarrow S/R$ .

**Sol. :** You can easily prove that  $R$  is an equivalence relation.

The partition  $S/R$  is given by  $[d] = \{a, d\}, [b] = \{b, c\}$ . Further  $d$  is the identity element of  $*$ . From the given table, we find that,

$$\begin{aligned} [a] @ [a] &= [a * a] = [d] = [a] \\ [a] @ [b] &= [a * b] = [b] \\ [b] @ [a] &= [b * a] = [c] = [b] \\ [b] @ [b] &= [b * b] = [b] \end{aligned}$$

Hence, we get the table.

*	[a]	[b]
[a]	[a]	[b]
[b]	[b]	[b]

The natural homomorphism is (from partition table)

$$(a) \rightarrow [a], (d) \rightarrow [a], (b) \rightarrow [b], (c) \rightarrow [b].$$

## 8. Generators and Evaluation of Powers

Let  $(A, *)$  be an algebraic system in which  $A$  is a set of angles in degrees and binary operation  $*$  gives the angle that the combination of 2 angles yields a new angle. We want to know all the possible combinations of angles.

Consider the group  $\{0^\circ, 15^\circ, 45^\circ, 60^\circ, 75^\circ, 90^\circ, 105^\circ, 120^\circ\}, *$  that describes the rotation of straight line in the plane. If we can rotate straight line only by  $60^\circ$  each time. Successive rotations by  $60^\circ$  will give the angles of rotation  $\{0, 60^\circ, 120^\circ\}$ . If we can rotate the straight line only  $15^\circ$  each time, successive rotations by  $15^\circ$  will yield all the rotations of straight line in  $\{0^\circ, 15^\circ, 45^\circ, 60^\circ, 75^\circ, 90^\circ, 105^\circ, 120^\circ\}$ .

A subset of a group is called generating set, if it can be expressed using the elements of a subset by means of the group multiplication and inversion and there is a surjective map from a free group on that many generators to given generators of the free group to the elements of this free group.

The elements of the generating set are termed as generators.

In general, let  $(G, *)$  be an algebraic system where  $*$  is a closed operation and  $A = \{a_1, a_2, \dots\}$  be a subset of  $G$ . Let  $A_1$  be the subset of  $A$  which contains  $A$  as well as elements  $a_i * a_j$  for  $a_i, a_j \in A$ .  $A_1$  is called the set generated by  $A$ , similarly, let  $A_2$  denote set generated by  $A_1, \dots$  and  $A_{i+1}$  denotes the set generated by  $A_i$ . Let  $B$  denote the union of  $A, A_1, A_2, \dots, A_i$ . The algebraic system  $(B, *)$  is system generated by  $A$  and an element is said to be generated by  $A$ , if it is in  $B$ . Thus, for a group  $(G, *)$ , if  $B$  is finite, then  $(B, *)$  is subgroup. If  $B = G$ ,  $B$  is called a generating set or a set of generators of algebraic system  $(G, *)$ . In the example on rotation of straight line ( $15^\circ$ ) is a generating set.

*	a	b	c	d
a	d	b	c	a
b	c	b	c	b
c	b	c	c	c
d	a	b	c	d

a	b
d	c

Alternatively, A subset  $B$  of group  $A$  is called a generating set if it satisfies following conditions.

- For any element  $b \in A$ , we can write  $b = a_1, a_2, \dots, a_n$  for each  $a_i$  either  $a_i \in B$  or  $a_i^{-1} \in B$ .  $B$  is a symmetric subset i.e.,  $a_i \in B$  implies  $a_i^{-1} \in B$ .
- If  $C$  is a proper subgroup of  $A$ , then  $C$  can't contain  $B$ .
- Consider map from free group on as many generators as elements of  $B$  to the group  $A$ , which maps the freely generating set to the elements of  $B$  to the elements of  $A$ , this gives surjective homomorphism from free group to  $G$ .

For example, the set of all elements of a group is a generating set for the group.

If  $S$  is a subset of a group  $G$  s.t. every element of  $G$  is a power of some elements of  $S$ , the  $S$  is a generating set. If  $S$  is empty set, then  $\{S\}$  is the trivial group  $\{e\}$ . Since we consider empty product to be the identity. The set of all non-identity elements of a group is a generating set for the group e.g., the  $5^{\text{th}}$  roots of unity in the complex plane form a group under multiplication. Each non-identity element generates the group.

**Definition :** An element  $a$  of a group  $G$  generates  $G$  and is a generator for  $G$  if  $\langle a \rangle = G$ . A group  $G$  is cyclic if there is some element  $a$  in  $G$  that generates  $G$ . A cyclic group is a group that is generated by a single element.

For example, the group  $\mathbb{Z}$  under addition is a cyclic group, both  $1$  and  $-1$  are generators for the group.

Finding generators of a cyclic group depends upon order of group. If the order of group is  $8$ , then the total number of generators of group  $G$  are equal to positive integers less than  $8$  and coprime to  $8$  i.e.,  $1, 3, 5, 7$  less than  $8$  and coprime to  $8$ . Therefore, if  $a$  is generator of  $G$ , then  $a^3, a^5$  are also generators of  $G$ . Hence, there are  $4$  generators of  $G$ .

## 9. Cosets and Lagrange's Theorem

### (a) Coset

**Definition :** Let  $(G, *)$  be group and  $H$  be a subgroup of  $G$ . If  $a, b$  are two elements of  $G$  and  $a * b^{-1} \in H$ , then we say that "a is congruent to  $b$  modulo  $H$ ". It is written as " $a \equiv b \pmod{H}$ ".

It can be easily verified that this congruence relation is an equivalence relation (See Ex. 1 page 16-33). Since this congruence relation is an equivalence relation on  $G$  it partitions  $G$  into equivalent classes called cosets.

**Definition :** Let  $(G, *)$  be group and  $H$  be a subgroup of  $G$ .

If  $a$  is an element of  $G$  then the set  $Ha = \{h * a \mid h \in H\}$  is called the right coset of  $H$ .

If  $a$  is an element of  $G$ , then the set  $aH = \{a * h \mid h \in H\}$  is called the left coset of  $H$ .

$a$  is called the representative element of the coset  $aH$  or  $Ha$ .

For example, consider binary operation  $+$ , group  $(\mathbb{Z}_6, +)$  elements of this group are

$$\{0, 1, 2, 3, 4, 5\}$$

Let  $H = \{0, 2, 4\}$  is a subgroup of  $\mathbb{Z}_6$ .

$$\text{The left coset of } H \text{ w.r.t. } 0, \text{ i.e., } 0 + H = \{0 + 0, 0 + 2, 0 + 4\} = \{0, 2, 4\}$$

$$\text{The left coset of } H \text{ w.r.t. } 1, \text{ i.e., } 1 + H = \{1 + 0, 1 + 2, 1 + 4\} = \{1, 3, 5\}$$

$$\text{The left coset of } H \text{ w.r.t. } 2, \text{ i.e., } 2 + H = \{2 + 0, 2 + 2, 2 + 4\} = \{2, 4, 0\}$$

Note that,  $0$  is the identity element.

- From (i) and (ii), it follows that  $a = a'$ .  
 $\therefore$  The identity element is unique.
- (ii) If possible let  $b$  and  $b'$  be two distinct inverses of  $a \in G$  in  $G$ .  
Now,  $b = b * a$  (By definition of identity)  
 $= b * (a * b')$  (Since  $a * b' = e$ )  
 $= (b * a) * b'$  (Since  $*$  is associative)  
 $= e * b'$  (Since  $b * a = e$ )  
 $\therefore b = b'$  (Since  $e$  is identity)

This contradicts our hypothesis.  
 $\therefore$  Inverse is unique.

- (iii) Let  $a^{-1} = c$ .  $\therefore c * a = a^{-1} * a = e$ .  
Also  $a * c = a * a^{-1} = e$ .  $\therefore c^{-1} = a$ .  $\therefore (a^{-1})^{-1} = a$ .
- (iv) Let  $c = a * b$ ,  $d = b^{-1} * a^{-1}$ .  
 $\therefore c * d = (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$   
 $= a * a * a^{-1} = a * a^{-1} = e$ .  
Similarly,  $d * c = a$ .  $\therefore c^{-1} = d$   
 $\therefore (a * b)^{-1} = b^{-1} * a^{-1}$ .

#### Remark ...

Since identity is unique in a group, we shall call it *the* identity. Similarly, for the same reason we shall call *the* inverse of an element.

**Theorem 2 : (Cancellation Laws) :** In a group  $(G, *)$  if  $a, b, c \in G$ , then

- (i)  $a * b = a * c$  implies  $b = c$ . [Left cancellation law] (M.U. 2001)
- (ii)  $b * a = c * a$  implies  $b = c$ . [Right cancellation law] (M.U. 1997, 99, 2000)

**Proof :** (i) If  $a * b = a * c$  then by multiplying both sides on the left by  $a^{-1}$ , we get

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

$$\therefore (a^{-1} * a) * b = (a^{-1} * a) * c$$

$$\therefore e * b = e * c \quad \therefore b = c.$$

(ii) Similarly,  $(b * a) * a^{-1} = (c * a) * a^{-1}$  leads us as above to  $b = c$ .

**Theorem 3 : (Solution of equations) :** For any two elements  $a, b$  in a group  $(G, *)$ ,

- (i) the equation  $a * x = b$  has a unique solution.

- (ii) the equation  $y * a = b$  has a unique solution. (M.U. 1998, 2005)

**Proof : (i) Existence of solution :** Since  $a^{-1}$  exists in a group, we multiply the given equation on the left by  $a^{-1}$ .

$$\begin{aligned} & \therefore (a^{-1}) * (a * x) = a^{-1} * b \\ & \therefore a^{-1} * b = (a^{-1} * a) * x = e * x = x \\ & \therefore x = a^{-1} * b \text{ is a solution.} \end{aligned}$$

**(ii) Uniqueness of solution :** If  $x_1$  and  $x_2$  are two distinct solutions of  $a * x = b$ , we have  
 $a * x_1 = b$  and  $a * x_2 = b \quad \therefore a * x_1 = a * x_2$

- $\therefore$  By cancellation law  $x_1 = x_2$ .  
If  $y_1$  and  $y_2$  are distinct solution of  $y * a = b$ , we have  
 $y_1 * a = b$  and  $y_2 * a = b \quad \therefore y_1 * a = y_2 * a$   
 $\therefore$  By cancellation law  $y_1 = y_2$ .

**Example 1 :** Find the solution of  $(3 * x) * 4 = 3 + 4$  in the group  $(G, *)$  given in Example 9 on page 16-16. (M.U. 2002, 03)

Sol.: Consider  $(3 * x) * 4 = 3 + 4$   
By data  $2(3 * x) * 4 = 2(3 * 4) \quad \therefore 6x * 4 = 24$   
 $2(6x * 4) = 24 \quad \therefore 48x = 24 \quad \therefore x = 1/2$ .

**Example 2 :** Find the solution of  $5 * x = 2$

- (i) in the group of real numbers under the binary operation  $a * b = a + b - 1$ ,  
(ii) in the group of rational numbers different from  $-3$  under the binary operation

$$a * b = a + b + \frac{ab}{3}$$

Sol.: (i) Since  $a * b = a + b - 1$ ,  $5 * x = 2$  gives  
 $5 + x - 1 = 2 \quad \therefore x = 2 - 4 = -2$ .

(ii) Since  $a * b = a + b + \frac{ab}{3}$ ,  $5 * x = 2$  gives  
 $5 + x + \frac{5x}{3} = 2 \quad \therefore \frac{8x}{3} = -3 \quad \therefore x = -\frac{9}{8}$ .

**Example 3 :** Prove that if  $a^2 = a$ ,  $a \in G$ , then  $a = e$  where  $e$  is an identity of the group  $G$ . (M.U. 1997)

Sol.: Since  $a^2 = a$ ,  $a^{-1}(a^2) = a^{-1}a$   
 $\therefore (a^{-1}a) * a = e \quad \therefore a = e$ .

**Example 4 :** If in a group every element is its inverse, prove that the group is Abelian. Give an example of such a group. Is the converse true? Give an example if it is not.

Sol.: Let  $a, b \in G$ . Then by data  $a^{-1} = a$ ,  $b^{-1} = b$ .

Since, it is a closed binary operation

$$ab \in G \quad \therefore (ab) = (ab)^{-1}$$

Now,  $ab = (ab)^{-1} = b^{-1} * a^{-1}$  [By (iv) of Theorem 1 of § 11, page 16-40]  
 $\therefore ab = ba$  [By data]

Hence,  $G$  is an Abelian group.

The following is the example of such a group

Let  $G$  be the set of residue classes  $[1], [3], [5], [7]$  modulo 8 under multiplication. We see from the table that every element is its own inverse.

To demonstrate that the converse is not true, we have to give an example of an Abelian group in which  $a^{-1}$  is not  $a$ .

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Now, the set of all rational numbers (without zero) is an Abelian group under usual multiplication. But  $a^{-1}$  is not  $a$ . For example,  $2^{-1}$  is  $1/2$  but it is not 2.

Hence, the converse is not true.

**Similar Example :** Another example of the above type of group i.e. of a group in which every element is its inverse, is: The set  $\{1, -1\}$  under multiplication. The multiplication table is as shown in the right side.

$\times$	1	-1
1	1	-1
-1	-1	1

**EXERCISE - II**

1. Let  $G$  be the set of all non-zero real numbers and let  $a * b = \frac{ab}{2}$ .

Show that  $(G, *)$  is a Abelian group. Find the solution of  $3 * x = 2$  in  $G$ . (M.U. 2009, 14) [Ans.: 4/3]

2. Prove that the set of all  $m \times n$  matrices forms a group under addition.

3. Prove that the set of all  $n \times n$  non-singular matrices forms a non-commutative group.

4. Prove that the set of the following four matrices forms a commutative group under multiplication.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad (\text{M.U. 2003, 04, 05})$$

5. Prove that the set of the following six matrices forms a group under multiplication

$$\begin{bmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{bmatrix}, \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix} \text{ for } \theta = 0, \frac{2\pi}{3}, \frac{4\pi}{3}.$$

6. Prove that the set of all points on the unit circle  $|z| = 1$  is a group under multiplication.

(Hint : If  $z_1 = e^{i\theta_1}$ ,  $z_2 = e^{i\theta_2}$ ,  $z_1 z_2 = e^{i(\theta_1 + \theta_2)} = 1 = e^{i0}$  is an identity and  $e^{-i\theta}$  is the inverse of  $e^{i\theta}$ .)

7. Show that  $G = \{1, 2, 3, 4\}$  is an Abelian group under multiplication modulo 5.

8. Show that  $S = \{1, 2, 3, 4, 5\}$  is not a group under multiplication modulo 6.

9. Prove that the set  $M$  of all  $2 \times 2$  non-singular matrices is a group under multiplication. But  $M$  is not a group under addition.

10. Show that  $(G, *)$  where  $G = \{0, 1, 2, 3, 5\}$  and  $*$  is multiplication modulo 6 (addition modulo 6) is an Abelian group. (M.U. 1997)

11. Prove that the set of all matrices  $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$  where  $a \neq 0, b \neq 0$  are real numbers is a group under matrix multiplication. (M.U. 1997)

12. Show the set  $G = \{0, 1, 2\}$  is a group under addition modulo 3 but is not a group under usual addition.

13. Show that the set  $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$  where the functions are defined by

$$f_1(x) = x, \quad f_2(x) = 1 - x, \quad f_3(x) = \frac{x}{x-1},$$

$$f_4(x) = \frac{1}{x}, \quad f_5(x) = \frac{1}{1-x}, \quad f_6(x) = 1 - \frac{1}{x}.$$

$\Rightarrow$  a group under composition of two functions i.e. under operation of the form  $f \circ g$  where  $f$  and  $g$  are functions.

14. Show that the set  $G = \{0, 1, 2, \dots, (p-1)\}$  of positive integers is a group under addition modulo  $p$  (where  $p$  is a prime) but not under usual addition. (M.U. 2009)

15. Show that the set  $G = \{0, 1, 2, 3\}$  is a group under addition modulo 4. (M.U. 2008)

16. Prove that the set  $Z = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$  is an Abelian group under usual addition. (M.U. 2008)

17. Prove that the set of complex numbers  $Z = a + ib$ ,  $a, b \in R$  is an Abelian group under addition of complex numbers.

18. Prove that the set of fourth roots of unity i.e.  $G = \{1, -1, i, -i\}$  is an Abelian group under multiplication.

19. Prove that the set of all complex numbers  $\sin \theta + i \cos \theta$ ,  $\theta \in R$  under multiplication of complex numbers is a group.

20. Prove that the set of all  $n^{\text{th}}$  roots of unity under multiplication is a group. (M.U. 2002)

(Hint : The set is  $\{e^{2\pi i r/n}, r = 0, 1, 2, \dots, (n-1)\}$ . If  $z_1 = e^{2\pi k_1/n}$ ,  $z_2 = e^{2\pi k_2/n}$  where  $k_1, k_2$  are integers such that  $0 \leq k_1, k_2 \leq (n-1)$  then  $z_1 z_2 = e^{2\pi(k_1+k_2)/n} \quad 0 \leq (k_1+k_2) \leq (n-1)$ .

If  $k_1 + k_2 \geq n$ , then we can find  $q$  and  $r$  belonging to  $z$  such that  $k_1 + k_2 = nq + r$  where  $0 \leq r \leq n-1$ . Hence,  $z_1 z_2 = e^{2\pi(nk_1+k_2)/n} = e^{2\pi qr} \cdot e^{2\pi rk_1/n} = e^{2\pi rk_1/n}$ )

21. Prove that the set  $\{3^n \mid n \in Z\}$  is a group under multiplication.

22. Prove that the set  $\{a + \sqrt{5}b \mid a, b \in Z\}$  is a group under addition.

23. Prove that  $(Z, *)$  where  $*$  is defined by  $a * b = a + b + 3$  is a group.

24. Prove that  $((Q - 1), *)$  where  $*$  is defined by  $a * b = a + b + ab$  is a group. (M.U. 1996, 2001)

25. Prove that  $((Q - 3), *)$  where  $*$  is defined by  $a * b = a + b + \frac{ab}{3}$  is a group. (M.U. 2004)

26. Prove that  $(Q^+, +)$  where  $a + b = ab/2$  is a group. (M.U. 2004)

27. Verify whether  $(Z, *)$  and  $(Q, *)$  where  $a * b = a + b - ab$  are groups or monoids. (M.U. 2005) [Ans. : Group]

28. Prove that  $(C, *)$  where  $*$  is defined by  $a * b = a + b + \cos h \alpha$  where  $\alpha$  is a fixed complex number is a group.

29. Prove that the set  $G$  of all integers under the binary operation  $*$  defined by

$a * b = a + b - 5$  is a group.

Solve the equation  $2 * x = 0$  in  $G$ . (Hint :  $a = 5$ ,  $a^{-1} = 10 - a$ ,  $x = 3$ .)

30. Prove that the set of all real numbers  $G$  is a group under binary operation  $*$  defined by

$a * b = a + b - 1$ . (Ans. :  $a = 1$ ,  $a^{-1} = 2 - a$ ,  $x = 4$ )

Solve the equation  $3 * x = 6$  in  $G$ .

31. Show that the  $G = \{a + \sqrt{2} \cdot b \mid a, b \in Q\}$  is a group under multiplication. (Ans. :  $a = 1$ ,  $(a + \sqrt{2} \cdot b)^{-1} = \frac{a}{a^2 - 2b^2} - \frac{\sqrt{2} \cdot b}{a^2 - 2b^2}$ )

32. Let  $(G_1, \star_1)$  and  $(G_2, \star_2)$  be two groups. Prove that  $(S, \otimes)$  is a group where  $S = G_1 \times G_2$  and  $(a_1, a_2) \otimes (b_1, b_2) = (a_1 \star_1 b_1, a_2 \star_2 b_2)$ .
33. Prove that  $G = \{x \mid x^4 = 1\}$  is a group under multiplication. (M.U. 2001)
34. Let  $Z_n$  denote the set of integers  $\{0, 1, 2, \dots, (n-1)\}$ . Let  $\otimes$  be the binary operation on  $Z_n$  such that  $a \otimes b$  is the remainder of  $ab$  divided by  $n$ .
- construct the table for the operation  $\otimes$  for  $n = 4$ .
  - Is  $Z_n$  a group for any  $n$ ?
- [Ans. : (ii)  $G = \{1, 2, 3, 4\}$  is an Abelian group under multiplication modulo 5. But  $G = \{1, 2, 3, 4, 5\}$  is not a group under multiplication modulo 6. See Ex. 7, 8, page 16-43 and Ex. 14 page 16-44.]
35. Let  $S_3$  be the set of bijective functions that can be defined on the set  $A = \{1, 2, 3\}$ . And  $\circ$  be the operation of composition of functions of the form  $f \circ g$ . Prove that  $(S_3, \circ)$  is a group. Is it Abelian? (See Ex. 21, page 16-23) (M.U. 2006) [Ans. : No]

## 12. Isomorphism and Homomorphism

### (a) Isomorphism of groups

(M.U. 1998, 99)

**Definition :** If  $(G_1, \star_1)$  and  $(G_2, \star_2)$  are groups, then  $f : G_1 \rightarrow G_2$  is an isomorphism from  $G_1$  to  $G_2$  if (i)  $f$  is a bijection (i.e. one-to-one and onto) and (ii)  $f(a \star_1 b) = f(a) \star_2 f(b)$ .

If such a function exists, then  $G_1$  is said to be isomorphic to  $G_2$ .

### (b) Homomorphism of groups

**Definition :** If  $(G_1, \star_1)$  and  $(G_2, \star_2)$  are groups then  $f : G_1 \rightarrow G_2$  is a homomorphism from  $G_1$  to  $G_2$  if for any  $a, b \in G_1$ ,  $f(a \star_1 b) = f(a) \star_2 f(b)$ .

**Example 1 :** Let  $G$  be the group of integers under addition and  $G'$  be the group of even integers under addition. Show that the function  $f : G \rightarrow G'$  defined by  $f(a) = 2a$  is an isomorphism. (M.U. 2003, 06, 10, 12)

**Sol. :** Suppose  $f(a_1) = f(a_2) \quad \therefore 2a_1 = 2a_2 \quad \therefore a_1 = a_2$ .

Hence,  $f$  is one-to-one.

Suppose  $b$  is an even integer i.e.  $b \in G'$ .

Then  $2a = b \quad \therefore a = (b/2) \in G$  and  $f(a) = f(b/2) = 2(b/2) = b$ .

$\therefore f$  is onto.

Here,  $\star_1$  and  $\star_2$  both are addition operations.

$$\begin{aligned} f(a \star_1 b) &= f(a + b) = 2(a + b) = 2a + 2b \\ &= f(a) \star_2 f(b) \end{aligned}$$

Hence,  $f$  is a homomorphism.

**Example 2 :** Let  $G$  be the group of real numbers under addition and  $G'$  be the group of positive real numbers under multiplication. Let  $f : G \rightarrow G'$  be defined by  $f(x) = e^x$ . (M.U. 1999, 2003)

Show that  $f$  is an isomorphism.

**Sol. :** Suppose  $f(a_1) = f(a_2) \quad \therefore e^{a_1} = e^{a_2} \quad \therefore a_1 = a_2$ .

Hence,  $f$  is one-to-one.

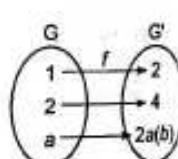


Fig. 16.9

Suppose  $b$  is a positive real number i.e.  $b \in G'$ .

$$\begin{aligned} \text{Then } b &= e^a \quad \therefore a = \log b, \\ \text{and } f(a) &= f(\log b) = e^{\log b} = b, \quad \therefore f \text{ is onto}, \\ f(a \star_1 b) &= f(a + b) = e^{a+b} \\ &= e^a \cdot e^b = f(a) \star_2 f(b) \end{aligned}$$

$f$  is an isomorphism.

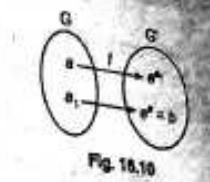


Fig. 16.10

**Example 3 :** Let  $R^+$  be the set of all positive real numbers. Show that the function  $f : R^+ \rightarrow R$  defined by  $f(x) = \ln x$  is an isomorphism of the semi-group  $(R^+, \times)$  to the semi-group  $(R^+, +)$  where  $\times$  and  $+$  are ordinary multiplication and addition respectively. (M.U. 2004, 05)

**Sol. :** (i) Since  $f(x) = \ln x$  if  $f(a) = f(b)$  i.e.,  $\ln a = \ln b$ , then  $a = b$ .

$\therefore f$  is one-to-one.

(ii) If  $c \in R$ , then  $e^c \in R$  and  $f(e^c) = \ln e^c = c \ln e = c \in R^+$

$\therefore f$  is onto.

(iii) Now,  $f(a \times b) = \ln(a \times b) = \ln a + \ln b = f(a) + f(b)$

$\therefore f$  is an isomorphism.

**Example 4 :** Show that the additive group  $Z_4$  is isomorphic to multiplicative group of non-zero elements of  $Z_5$ . (M.U. 2006)

**Sol. :** We have the following tables for the additive group  $G$  of  $Z_4$  and multiplicative group of  $G'$  of (non-zero)  $Z_5$ ,

+	0	1	2	3	$\times  $	1	2	3	4
0	0	1	2	3	1	1	2	3	4
1	1	2	3	0	2	2	4	1	3
2	2	3	0	1	3	3	1	4	2
3	3	0	1	2	4	4	3	2	1

x	1	3	4	2
1	1	3	4	2
3	3	4	2	1
4	4	2	1	3
2	2	1	3	4

Now, we write the table of  $\times$  taking the second column last and second row last.

Clearly, now we can see that  $G \rightarrow G'$  where the mapping is  $0 \rightarrow 1$ ,  $1 \rightarrow 3$ ,  $2 \rightarrow 4$ ,  $3 \rightarrow 2$  is a isomorphism.

**Example 5 :** If  $\omega$  denotes the cube root of unity, show that  $G = \{1, \omega, \omega^2\}$  is isomorphic to  $(Z_3, +)$ .

**Sol. :** We have the following tables for  $\times$  and  $+$ .

$\times  $	1	$\omega$	$\omega^2$	$+$	0	1	2
1	1	$\omega$	$\omega^2$	0	0	1	2
$\omega$	$\omega$	$\omega^2$	1	1	2	0	0
$\omega^2$	$\omega^2$	1	$\omega$	2	2	0	1

Clearly,  $G \rightarrow G'$  where the mapping is  $1 \rightarrow 0$ ,  $\omega \rightarrow 1$  and  $\omega^2 \rightarrow 2$  is an isomorphism.

**Example 6 :** Show that  $(G, \times)$  where  $G = \{1, -1, i, -i\}$  and  $(Z_4, +)$  are isomorphic.

**Sol. :** We first prepare the following tables for  $\times$  and  $+$ .

$\times$	1	-1	0	1
1	1	-1	0	1
-1	-1	1	0	-1
0	0	0	0	0
1	1	-1	0	1

Clearly  $S \rightarrow S'$  where the mapping is  $1 \mapsto 0, -1 \mapsto 2, 0 \mapsto 1$  and  $1 \mapsto 3$  is a homomorphism.

**Example 7:** If a function  $f$  is an isomorphism from a semi-group  $(S, *)$  to another semi-group  $(T, +)$ , show that  $f^{-1}$  is also an isomorphism from  $(T, +)$  to  $(S, *)$ .

**Sol:** Since  $f: S \rightarrow T$  is an isomorphism,  $f$  is one-to-one from  $S$  to  $T$ . (M.U. 2002)

$$\text{i.e., } f(a * b) = f(a) + f(b) \text{ for all } a, b \in S.$$

$f^{-1}$  exists and is also one to one from  $T$  to  $S$ .

Now suppose  $a', b'$  are elements of  $T$ .

Since  $f$  is onto we can always find elements  $a, b$  in  $S$ , such that

$$f(a) = a', f(b) = b'$$

Hence,  $a = f^{-1}(a')$  and  $b = f^{-1}(b')$

$$\text{Now, } f'(a' + b') = f^{-1}[f(a) + f(b)]$$

$$= f^{-1}[f(a + b)] \quad [\text{By (1)}]$$

$$= a + b$$

$$= f^{-1}(a') + f^{-1}(b')$$

∴  $f^{-1}$  is an isomorphism.

**Example 8:** Show that if a function  $f$  is an isomorphism from a group  $(G, *)$  to another group  $(G', +)$  then show that  $f^{-1}$  is also an isomorphism from  $(G', +)$  to  $(G, *)$ .

**Sol:** Left to you.

**Example 9:** If  $f$  is homomorphism from a commutative semigroup  $(S, *)$  onto a semigroup  $(T, +)$  then prove that  $(T, +)$  is also commutative.

**Sol:** Let  $t_1$  and  $t_2$  be any two elements of  $T$ .

Since  $f$  is homomorphic there exist  $s_1$  and  $s_2$  in  $S$ , such that  $t_1 = f(s_1)$  and  $t_2 = f(s_2)$ .

Hence,  $t_1 + t_2 = f(s_1) + f(s_2)$

$$= f(s_1 + s_2)$$

$$= f(s_2 + s_1) \quad [\because S \text{ is a commutative group}]$$

$$= f(t_2) + f(t_1) = t_2 + t_1$$

$\therefore (T, +)$  is also commutative.

### 13. Ring

So far we have studied structures of a set under one operation. We shall now study structures with two operations  $*$  and  $\cdot$  on its elements. This gives rise to two important algebraic structures – rings and fields. Rings have structures similar to natural numbers and fields have structures similar to real numbers with respect to the operations of addition and multiplication.

**(Ring) Definition:** A ring is an ordered triple  $(R, +, \cdot)$  where  $R$  is a non-empty set and  $+$  and  $\cdot$  are two binary operations on  $R$  satisfying the following axioms:

R1 :  $(R, +)$  is a commutative group.

R2 :  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  for all  $a, b, c \in R$  (i.e. associative).

R3 :  $a \cdot (b + c) = a \cdot b + a \cdot c$  for all  $a, b, c \in R$  (distributes over  $+$ ).

R4 : Examples of Rings

1. The set of all integers is a ring (with unity) for  $+$  and  $\cdot$ .

2. The set of all real numbers of the form  $a + \sqrt{b}$  is a ring for  $+$  and  $\cdot$ .

3. The set of all matrices of the form  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  is a ring for  $+$  and  $\cdot$ .

4. The set of complex numbers with usual addition and multiplication is a ring.

**Remark** ...

The binary operation  $+$  and  $\cdot$  referred to above are called addition and multiplication. In the same spirit, the identity of  $(R, +)$  is denoted by 0 and is called zero,  $a'$  is denoted by  $-a$  and is called minus  $a$  and  $a + (-b)$  is denoted by  $a - b$ . Addition is commutative but multiplication in general is not.

**(Commutative Ring) Definition:** A ring  $(R, +, \cdot)$  is called a commutative ring if  $a \cdot b = b \cdot a$  for all  $a, b \in R$ .

(a) **Ring with Unity**

**Definition:** A ring  $(R, +, \cdot)$  is called a ring with unity or identity if there exists an element 1 in  $R$  such that  $a \cdot 1 = 1 \cdot a = a$  for all  $a \in R$ .

(b) **Ring with Zero Divisors**

A ring  $(R, +, \cdot)$  is called a ring with zero divisor if for  $a, b \in R$ , we have  $a \cdot b = 0$  but  $a \neq 0, b \neq 0$ . In this case  $a$  and  $b$  are called proper zero divisors.

For example, we know that, we can find two matrices  $A, B$  such that  $A \cdot B = 0$  but  $A \neq 0, B \neq 0$ .

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

**Definition:** A ring  $(R, +, \cdot)$  is called a ring without zero divisor if for all  $a, b \in R$ , if  $ab = 0$  then either  $a = 0$  or  $b = 0$  or both  $a = 0, b = 0$ .

This means in a ring without zero divisor, the left cancellation law and right cancellation laws hold:

i.e. if  $ab = ac$ , then  $b = c$  and if  $ba = ca$ , then  $b = c$ .

**Examples of Commutative Rings**

**Example 1:** Let  $R$  be the set of integers, positive, negative, and 0;  $+$  is the usual addition and  $\cdot$  is the usual multiplication. Then  $(R, +, \cdot)$  is a commutative ring with unity.

**Example 2:** Let  $R$  be the set of even integers with usual operations of addition and multiplication. Then  $(R, +, \cdot)$  is a commutative ring without unity.

**Example 3 :** Let  $R$  be the set of rational numbers with usual operations of addition and multiplication. Then  $R$  is a commutative ring with unity. (It is also a field). (See § 15)

**Example 4 :** Let  $R = \{0, 1, 2, 3, 4, 5, 6\}$  and  $\oplus$  and  $\otimes$  be two operations multiplication modulo 7 and addition modulo 7. Then,  $(R, \oplus, \otimes)$  is a commutative ring with unity. (It is also a field). (M.U. 2005) (See § 15)

The set  $Z_m = \{0, 1, 2, \dots, (m-1)\}$  under the operations of addition and multiplication modulo  $m$  is a ring. It is called a ring of integers modulo  $m$ . If  $m$  is a prime the  $Z_m$  is a field. (See § 15)

**Example 5 :** Let  $R = \{0, 1, 2, 3, 4, 5\}$  and  $\oplus$  and  $\otimes$  be two operations multiplication modulo 6 and addition modulo 6. Then  $(R, \oplus, \otimes)$  is a ring. (But it is not a field). It is a ring with zero divisors.

**Example 6 :** Prove that  $Z_4$  is a ring under addition and multiplication modulo 4. (M.U. 2004)

**Sol. :** The addition and multiplication table for  $Z_4$  modulo 4 are given below.

	0	1	2	3		0	1	2	3
0	0	1	2	3		0	0	0	0
1	1	2	3	0		1	0	1	2
2	2	3	0	1		2	0	2	0
3	3	0	1	2		3	0	3	2

**R1 :**  $(R, +)$  is a commutative group.

**R2 :**  $(ax)b \cdot c = a(xb \cdot c)$  for all  $a, b, c \in R$ .  $X$  is associative.

**R3 :**  $ax(b+c) = axb + axc$ .

e.g.  $2 \times (3+1) = 2 \cdot 0 = 0$  and  $2 \times 3 + 2 \times 1 = 2 + 2 = 0$   
and  $(b+c)x = b \times x + c \times x$  for all  $a, b, c \in R$ .

$\therefore x$  distributes over  $+$ . Hence,  $(Z_4, +, x)$  is a ring.

**Example 7 :** Prove that  $Z_5$  is a ring under addition and multiplication modulo 5. (M.U. 2005)

**Sol. :** The addition and multiplication tables for  $Z_5$  modulo 5 are given below.

	0	1	2	3	4		0	1	2	3	4
0	0	1	2	3	4		0	0	0	0	0
1	1	2	3	4	0		1	0	1	2	3
2	2	3	4	0	1		2	0	2	4	1
3	3	4	0	1	2		3	0	3	1	4
4	4	0	1	2	3		4	0	4	3	2

Verification that  $(R, +, x)$  is a ring is left to you.

**Example 8 :** Prove that  $R = \{0, 2, 4, 6, 8\}$  is a commutative ring under addition and multiplication modulo 10. (M.U. 2002, 05)

**Sol. :** The addition and multiplication tables are given below.

	0	2	4	6	8		0	2	4	6	8
0	0	2	4	6	8		0	0	0	0	0
2	2	4	6	8	0		2	0	4	8	2
4	4	6	8	0	2		4	0	8	6	4
6	6	8	0	2	4		6	0	2	4	6
8	8	0	2	4	6		8	0	6	2	8

Verification that  $(R, +, x)$  is a ring is left to you.

**Example 9 :** Let  $A = \{a, b, c, d\}$  and let the operations  $+$  and  $\cdot$  be defined by the following

	a	b	c	d		a	b	c	d
a	a	b	c	d		a	a	a	a
b	b	c	d	a		b	a	c	a
c	c	d	a	b		c	a	a	a
d	d	a	b	c		d	a	c	a

(a) Is it a commutative ring? (b) Does it have an identity?

(c) Find the additive inverse of each element of  $A$ .

(M.U. 2007)

**sol. (a) Commutative Ring**

(i) It is easy to see that  $A$  is closed under  $+$  and also under  $\cdot$ .

(ii) Because,  $(a+b)+c = b+a+c = c$

and  $a+(b+c) = a+b+c = c$

$+$  is associative.

(iii) From the first row and the first column we see that  $a$  is the additive identity.

(iv) Since  $a+b=b$  and  $b+a=b$  is true for all elements and

(v) since for every element additive inverse exists  $(R, +)$  is a commutative group.

(vi) From the second table we see that

$(a \cdot b) \cdot c = a \cdot c = a$  and  $a \cdot (b \cdot c) = a \cdot a = a$

$\cdot$  is associative.

(vii) You can establish distributivity. Hence,  $(R, +, \cdot)$  is a ring.

(b) As seen above  $a$  is the additive identity.

(c) From the table we see that the inverse of  $a$  is  $a$ , the inverse of  $b$  is  $d$ , the inverse of  $c$  is  $c$ , the inverse of  $d$  is  $b$ .

**Example 10 :** If  $x, y \in Z$  and the operations  $\oplus, \otimes$  are defined by

$x \oplus y = x + y - 1$  and  $x \otimes y = x + y - xy$

(M.U. 2003, 04, 05)

**Prove that  $(Z, \oplus, \otimes)$  is a ring.**

**sol. :** See Ex. 3 of § 15.

**(c) Basic Properties**

If  $R$  is a ring with identity 0 and unit element 1 then for all elements  $a, b, c \in R$ .

(i)  $a \cdot 0 = 0 \cdot a = 0$

(ii)  $a \cdot (-b) = (-a) \cdot b = - (a \cdot b)$

(iii)  $(-a) \cdot (-b) = a \cdot b$

(iv) unit element is unique.

(v)  $(-1) \cdot a = -a$

(vi)  $(-1) \cdot (-1) = 1$

(M.U. 2006)

**Example 11 :** Show that the set  $R = \{x \mid x = a + b\sqrt{2}, a, b \text{ are integers}\}$  is a ring under usual addition and multiplication.

(M.U. 2003, 06)

**Sol. :** See Ex. 2 of § 15.

Sol. (i) We have

$$\begin{aligned} a \cdot 0 &= a \cdot (0 + 0) \\ &= a \cdot 0 + a \cdot 0 \\ &= a \cdot 0 + a \cdot 0 \\ &= a \cdot 0 + a \cdot 0 \\ &= a \cdot 0 \end{aligned} \quad [\because 0 + 0 = 0]$$

[ $\therefore$  left distributive law]

Similarly, we have

$$\begin{aligned} 0 \cdot a &= (0 + 0) \cdot a \\ &= 0 \cdot a + 0 \cdot a \\ &= 0 \cdot a + 0 \cdot a \\ &= 0 \cdot a + 0 \cdot a \\ &= 0 \cdot a \end{aligned} \quad [\because 0 + 0 = 0]$$

[ $\therefore$  right distributive law]

Hence,  $a \cdot 0 = 0 \cdot a = 0$ 

(ii) Consider

$$\begin{aligned} a \cdot (-b) + a \cdot b &= a \cdot (-b + b) \\ &= a \cdot 0 = 0 \end{aligned} \quad [\because \text{left distributive law}]$$

Hence,  $a \cdot b$  is the inverse of  $a \cdot (-b)$  which is unique.

$$a \cdot (-b) = -(a \cdot b)$$

Similarly, we can prove that,

$$(-a) \cdot b = -(a \cdot b)$$

∴  $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ 

(iii) We have

$$\begin{aligned} (-a) \cdot (-b) &= -[(-a) \cdot b] \\ &= -[-(a \cdot b)] \\ &= a \cdot b \end{aligned} \quad [\because a \cdot (-b) = -(a \cdot b)]$$

[ $\therefore -(-a) = a$ ]

(iv) If possible, suppose there is another unit element  $1'$  with the same properties as  $1$ .

$$1 \cdot 1' = 1' \cdot 1 = 1' \quad [\because 1 \text{ is unit element}]$$

$$\text{But } 1 \cdot 1' = 1 \quad [\because 1' \text{ is unit element}]$$

∴ The unit element is unique.

$$\begin{aligned} (v) \quad (-1) \cdot a &= -[1 \cdot a] \\ &= -a \quad [\because 1 \text{ is unity}] \end{aligned}$$

(vi) Replacing  $a$  and  $b$  by  $1$  in (ii) we get (vi).

(d) Subring

Analogous to the subgroup we have a subring.

Definition : A subset  $R \subseteq S$  is a ring where  $(S, +, \cdot)$  is a ring is called a subring of  $S$ . In other words if  $(S, +, \cdot)$  is a ring then a subset  $R$  of  $S$  is called a subring if  $R$  has all the properties of a ring.

Examples : (i) The ring of even integers is a subring of the ring of integers.

In general for any positive integer  $n$ , the set  $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$  is a subring of  $\mathbb{Z}$ .

(ii) The ring of rationals is a subring of the ring of reals.

## Homomorphism, Automorphism and Isomorphism

We have learnt what we mean by homomorphism, automorphism and isomorphism. We shall relate these concepts with reference to rings.

Homomorphism of ring : Let  $(R, +, \cdot)$  and  $(S, +', \cdot')$  be two rings.A mapping  $\Phi : R \rightarrow S$  is called a ring homomorphism if for  $a, b \in R$ ,

(i)  $\Phi(a + b) = \Phi(a) +' \Phi(b)$

and (ii)  $\Phi(a \cdot b) = \Phi(a) \cdot' \Phi(b)$

Isomorphism of ring : Let  $(R, +, \cdot)$  and  $(S, +', \cdot')$  be two rings.A mapping  $\Phi : R \rightarrow S$  is called a ring isomorphism if for  $a, b \in R$ ,

(i)  $\Phi(a + b) = \Phi(a) +' \Phi(b)$

(ii)  $\Phi(a \cdot b) = \Phi(a) \cdot' \Phi(b)$

and (iii)  $\Phi$  is one-to-one.Automorphism of ring : If  $\Phi$  is an isomorphism from  $R$  on to itself then  $\Phi$  is called an automorphism.Example : If  $\Phi : (R, +, \cdot) \rightarrow (S, +', \cdot')$  is a ring homomorphism then prove that  $\Phi(-a) = -\Phi(a)$  for all  $a \in R$ .

(M.U. 2004)

Sol : Since  $\Phi : R \rightarrow S$  is a homomorphism by definition for  $a, b \in R$ ,

$$\Phi(a + b) = \Phi(a) +' \Phi(b)$$

$$\text{and } \Phi(a \cdot b) = \Phi(a) \cdot' \Phi(b)$$

Now put  $a = -1$  and  $b = a$ ,

$$\therefore \Phi(-1 + a) = \Phi(-1) +' \Phi(a)$$

$$= -1 +' \Phi(a)$$

$$\therefore \Phi(-a) = -\Phi(a).$$

## EXERCISE - III

- Show that the set  $R = \{x \mid x = a + b\sqrt{2}, a, b \text{ integers}\}$  is a ring with ordinary addition and multiplication.
- Show that the set  $R = \{0, 1, 2, 3, 4\}$  is a ring with respect to addition and multiplication modulo 5. (M.U. 2008)
- Show that the set of all  $n \times n$  matrices is a ring with respect to addition and multiplication of matrices.
- If  $R$  is the set of all continuous functions defined on  $[0, 1]$  then prove that  $R$  is a ring with respect to addition and multiplication of functions defined by  $(f+g)(x) = f(x) + g(x)$  and  $(f \cdot g)(x) = f(x) \cdot g(x)$ .
- If  $R$  is a set of all real numbers and  $*_1$  and  $*_2$  are two operations defined on  $R$  such that  $a *_1 b = a + b - 5$  and  $a *_2 b = 5$ , prove that  $(R, *_1, *_2)$  is a commutative ring. What is its 'zero'? Has it zero divisors? [Ans. : 5 is its zero. Yes, it has zero divisors]
- If  $Z$  is a set of integers and  $*_1$  and  $*_2$  are two operations defined on  $Z$  such that  $a *_1 b = a + b - 1$  and  $a *_2 b = a + b - ab$ , prove that  $(Z, *_1, *_2)$  is a commutative ring. What is its 'zero'? Is it a ring with unity? [Ans. : Zero. Yes]

7. If  $R = \{a, b, c, d\}$  and  $+$  and  $\times$  are defined on  $S$  by the following tables, prove that  $(R, +, \times)$  is a ring.

$+$	$a$	$b$	$c$	$d$
$a$	$a$	$b$	$c$	$d$
$b$	$b$	$a$	$d$	$c$
$c$	$c$	$d$	$a$	$b$
$d$	$d$	$c$	$b$	$a$

$\times$	$a$	$b$	$c$	$d$
$a$	$a$	$a$	$a$	$a$
$b$	$a$	$a$	$b$	$a$
$c$	$a$	$b$	$c$	$d$
$d$	$a$	$c$	$b$	$a$

8. Prove that  $(M, +, \cdot)$  where  $M$  is the set of all non-singular square matrices of order  $n$  is a ring under usual addition and multiplication of matrices.

9. Prove that  $(M, +, \cdot)$  where  $M$  is the set of all matrices of the form  $\begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}$  and  $a, b, c, d \in R$  and  $i^2 = -1$  is a ring under usual addition and multiplication of matrices.

10. Prove that  $(R, +, \cdot)$  where  $R = \{0, 1, 2, 3, 4\}$  is a ring under addition modulo 5 and multiplication modulo 5.

11. Let  $Z$  be the set of integers and  $a \oplus b = a + b + 1$ ,  $a \otimes b = a + b + ab$  for all  $a, b \in Z$ . Show that  $(Z, \oplus, \otimes)$  is a ring. Is it a commutative ring? What is the zero of the ring? Is it a ring with unity?

[Ans. : It is commutative ring. Zero of the ring is  $-1$  and  $0$  is its unity.]

12. Show that the set of all matrices of the form  $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$  is a non-commutative ring with respect to addition and multiplication of matrices for every  $a, b \in Q$ . (M.U. 2002)

13. Show that the set of all  $2 \times 2$  matrices of the type  $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ,  $a, b, c, d \in Z$  under usual matrix multiplication and addition is a ring. Is it commutative? What is the zero of the ring? What is the unity of the ring?

[Ans. : (i) Non-commutative, (ii)  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$  is the zero of the ring]

(iii)  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  is the unity of the ring.]

14. Let  $Z$  be the set of integers. Let  $\oplus$  and  $\otimes$  be defined as  $a \oplus b = a + b$  and  $a \otimes b = 0$  for all  $a, b \in Z$ . Is  $(Z, \oplus, \otimes)$  a ring? Is it commutative? Does it have a unity?

[Ans. : (i) Yes, (ii) Yes, (iii) No]

#### 14. Integral Domain

**Definition 1 : (Integral Domain)** : A commutative ring with unity without zero divisors is called an **integral domain**.

An integral domain can also be defined more explicitly as :

**Definition 2 : (Integral Domain)** : A ring  $(R, +, \cdot)$  is called an **integral domain** if the following axioms hold.

J1 : It is a commutative ring.

J2 : It is a ring with unity.

J3 : It is a ring without zero divisors.

#### Example of Integral Domain

1. The set  $(Z, +, \cdot)$  is an integral domain.

2. The set  $(Q, +, \cdot)$  is an integral domain.

3. But the set of even integers including zero with usual addition and multiplication is not an integral domain because it does not have multiplicative identity.

Example 1 : Let  $M = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in R \right\}$  and let  $+$  and  $\cdot$  denote usual matrix addition and multiplication.

Is  $(M, +, \cdot)$  an integral domain?

(M.U. 2001, 03)

#### Sol : Closure

Let  $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ ,  $B = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$ ,  $a, b \in R$ .

Then  $A + B = \begin{bmatrix} a+b & 0 \\ 0 & a+b \end{bmatrix} \in M$

and  $AB = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & ab \end{bmatrix} \in M$

$\therefore M$  is closed under addition and multiplication.

J1 : Consider  $(M, +)$

(i) Matrix addition is associative.

(ii) Since  $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$  for all  $a \in R$ , additive identity exists.

(iii) Since  $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} -a & 0 \\ 0 & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ , additive inverse exists.

(iv) Matrix addition is commutative.

$\therefore (M, +)$  is a commutative group.

(v) For matrices  $A \cdot (B+C) = A \cdot B + A \cdot C$  and  $(B+C) \cdot A = B \cdot A + C \cdot A$ .

Hence,  $\cdot$  distributes over  $+$ .

Hence,  $(M, +, \cdot)$  is a commutative ring.

J2 : Consider  $(M, +, \cdot)$

Since  $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ .

$\therefore$  Multiplicative identity exists.

Hence,  $(M, +, \cdot)$  is a ring with unity.

**I.3:** Consider again  $(M, +, \cdot)$

$$\text{Since } \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & ab \end{bmatrix}, \text{ and } \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} ba & 0 \\ 0 & ba \end{bmatrix}.$$

Hence,  $(M, +, \cdot)$  is a commutative ring with unity but without zero divisors.

$\therefore (M, +, \cdot)$  is an integral domain.

**Example 2:** If addition and multiplication modulo 10 are defined on the set of integers  $R = \{0, 2, 4, 6, 8\}$  then show that the system is an integral domain.

**Sol.:** Refer to Ex. 8 § 13. Yes. The system is an integral domain.

(M.U. 2006, 07)

**Example 3:** In an integral domain  $D$ . Show that if  $ab = ac$  with  $a \neq 0$  then  $b = c$ .

**Sol.:** We have  $ab = ac$ .

Multiply both sides by  $a^{-1}$ ,

$$\begin{aligned} \therefore a^{-1}(ab) &= a^{-1}(ac) \\ \therefore (a^{-1}a)b &= (a^{-1}a)c \quad [\text{associativity}] \\ ab &= ac \quad [\text{inverse}] \\ \therefore b &= c \quad [e \text{ is identity}] \end{aligned}$$

## 15. Field

**Definition 1 (Field):** A commutative ring with unity and multiplicative inverse for each non-zero element is called a field.

A field can be defined in a more explicit way as follows.

**Definition 2 (Field):** A field is an ordered triplet  $(F, +, \cdot)$  where  $F$  is a non-empty set and  $+$  and  $\cdot$  are two binary operations on  $F$  satisfying the following axioms.

**F1:**  $(F, +)$  is a commutative group.

**F2:**  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  for all  $a, b, c \in F$  ( $\cdot$  is commutative.)

**F3:**  $a \cdot (b + c) = a \cdot b + a \cdot c$  for all  $a, b, c \in F$  ( $\cdot$  distributes over  $+$ ).

**F4:**  $(F \setminus 0, \cdot)$  is a commutative group.

Clearly, because of F<sub>4</sub>, a field is a commutative ring with unity in which every non-zero element has multiplicative inverse.

**Example 1:** Show that the set of integers  $Z$  is a ring under addition and multiplication. Is it a field?

**Sol.:** **Closure** - Clearly  $Z$  is closed under  $+$  and  $\cdot$ .

**R1:** Consider  $(Z, +)$

- (i) Since for all integers  $a + (b + c) = (a + b) + c$ , addition is associative.
- (ii) Since  $a + 0 = 0 + a$  for all  $a \in Z$ , additive identity exists.
- (iii) Since we have  $-a$  corresponding to every  $a \in Z$  such that  $a + (-a) = (-a) + a = 0$ ,

every element  $a \in Z$ , additive inverse exists.

(i) Since  $a + b = b + a$  for all  $a, b \in Z$ , addition is commutative.

$\therefore (Z, +)$  is a commutative group.

**R2:**  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  for all  $a, b, c \in Z$ . Hence,  $\cdot$  is associative.

**R3:**  $a \cdot (b + c) = a \cdot b + a \cdot c$  and  $(b + c) \cdot a = b \cdot a + c \cdot a$ .

Hence,  $\cdot$  distributes over  $+$ .

Hence,  $(Z, +, \cdot)$  is a ring.

However, no element of  $Z$  except  $\pm 1$  has multiplicative inverse. For example, there exists no integer  $a$  such that  $2a = 1$ .

$\therefore (Z \setminus 0, \cdot)$  is not a group.  $\therefore (Z, +, \cdot)$  is not a field.

**Example 2:** Show that the set  $F = \{a + b\sqrt{2} \mid a, b \in Q\}$  under addition and multiplication is a field.

(M.U. 2002, 03, 08)

**Sol.:** **Closure** - Let  $x = a + b\sqrt{2}$ ,  $y = c + d\sqrt{2}$  where  $a, b, c, d \in Q$ .

Show,  $x + y = (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$

$$\begin{aligned} \text{and } xy &= (a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd \\ &= (ac + 2bd) + \sqrt{2}(ad + bc) \end{aligned}$$

and since  $(a + c), (b + d), (ac + 2bd), (ad + bc)$  are rational numbers  $(x + y)$  and  $xy \in F$ . Hence,  $F$  is closed under addition  $+$  and multiplication  $\cdot$ .

**F1:** Consider  $(F, +)$ .

(i) Since for all rational numbers addition is associative, we can show that  $x + (y + z) = (x + y) + z$ .  $\therefore$  Addition is associative.

(ii) Since  $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = a + b\sqrt{2}$ ,  $0 + 0\sqrt{2}$  i.e.  $0 \in Q$  is additive identity.

(iii) Since  $(a + b\sqrt{2}) + (-\sqrt{a} - b\sqrt{2}) = 0 + 0\sqrt{2}$ , for every  $a + b\sqrt{2}$ , additive inverse exists.

(iv) Since for rational numbers addition is commutative, we can show that  $x + y = y + x$ .  $\therefore (F, +)$  is a commutative group.

**F2:** It can be shown that  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$  for all  $x, y, z \in F$ .

Hence,  $\cdot$  is associative.

**F3:** It can be shown that  $x \cdot (y + z) = x \cdot y + x \cdot z$

and  $(x + y) \cdot z = x \cdot z + y \cdot z$  for all  $x, y, z \in F$ .

Hence,  $\cdot$  distributes over  $+$ .

**F4:** Consider  $(F \setminus 0, \cdot)$ .

(i)  $\cdot$  is associative as noted in F<sub>2</sub>.

(ii) Since  $(a + b\sqrt{2}) \cdot (1 + 0\sqrt{2}) = a + b\sqrt{2}$ ,  $1 + 0\sqrt{2}$  is the multiplicative identity.

(iii) If  $x \neq 0$  i.e. if  $a \neq 0$ ,  $b \neq 0$ , and  $x = a + b\sqrt{2}$ , then

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b} = c + d\sqrt{2}$$

where  $c = \frac{a}{a^2 - 2b}$ ,  $d = -\frac{b}{a^2 - 2b}$ .

Since  $a + b\sqrt{2} \neq 0$ ,  $a - b\sqrt{2} \neq 0$  hence,  $a^2 - 2b \neq 0$ .

$$\therefore a, d \in Q \quad \therefore \frac{1}{x} \in F.$$

$\therefore$  For every  $x \in (F - 0)$ , there exists multiplicative inverse.

$\therefore (F - 0, \cdot)$  is a commutative group.

Hence,  $(F, +, \cdot)$  is a field.

**Example 3 :** Let  $Z$  be the set of integers and  $a \oplus b = a + b - 1$  and  $a \otimes b = a + b - ab$ .

Show that  $(Z, \oplus, \otimes)$  is a ring? Is it an integral domain? Is it a field?

(M.U. 1998, 99, 2005)

**Sol. :** (i) Clearly  $a \oplus b = a + b - 1$  and  $a \otimes b = a + b - ab$  are binary operations in  $Z$ .

(ii) **R1 :**  $(Z, \oplus)$  is a commutative group as shown below.

**G1 :** For all  $a, b, c \in Z$ ,  $a \oplus b = a + b - 1$

$$\begin{aligned} (a \oplus b) \oplus c &= (a + b - 1) \oplus c \\ &= a + b - 1 + c - 1 \\ &= a + b + c - 2 \end{aligned}$$

Now,  $b \oplus c = b + c - 1$

$$\begin{aligned} \therefore a \oplus (b \oplus c) &= a \oplus (b + c - 1) \\ &= a + b + c - 1 - 1 \\ &= a + b + c - 2 \end{aligned}$$

$$\therefore (a \oplus b) \oplus c = a \oplus (b \oplus c)$$

$\therefore \otimes$  is associative.

**G2 :** There exists additive identity (1).

This is so because,

$$a \oplus 1 = a + 1 - 1 = a \quad \text{and} \quad 1 \oplus a = 1 + a - 1 = a.$$

Thus, 1 is the zero (i.e. additive identity)

**G3 :** For every element  $a \in Z$  there is an element  $b = 2 - a$  which is its inverse.

This is so because

$$a \oplus b = a \oplus (2 - a) = a + 2 - a - 1 = 1$$

$$\text{and} \quad b \oplus a = (2 - a) \oplus a = 2 - a + a - 1 = 1.$$

**G4 : Commutativity of  $\oplus$**

$$a \oplus b = a + b - 1 \quad \text{and} \quad b \oplus a = b + a - 1$$

$\therefore a \oplus b$  is commutative.

$\therefore (Z, \oplus)$  is a commutative group.

**(iii) R2 :  $\otimes$  is associative.** This is so because

$$a \otimes b = a + b - ab$$

$$\therefore (a \otimes b) \otimes c = (a + b - ab) \otimes c$$

$$= a + b - ab + c - ac - bc + abc$$

$$= a + b + c - ab - ac - bc + abc$$

Now,  $b \otimes c = b + c - bc$

$$\therefore a \otimes (b \otimes c) = a \otimes (b + c - bc)$$

(16-58)

$$= a + b + c - bc - ab - ac + abc$$

$$a \otimes (b \otimes c) = (a \otimes b) \otimes c$$

$\therefore \otimes$  is associative.

**R3 : Distributivity**

$$\text{Now, } a \otimes (b \oplus c) = a \otimes (b + c - 1)$$

$$= a + b + c - 1 - ab - ac + a$$

$$= 2a + b + c - ab - ac - 1$$

$$\text{and } a \otimes b = a + b - ab$$

$$a \otimes c = a + c - ac$$

$$(a \otimes b) \oplus (a \otimes c) = (a + b - ab) \oplus (a + c - ac)$$

$$= a + b - ab + a + c - ac - 1$$

$$= 2a + b + c - ab - ac - 1$$

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

$\therefore \otimes$  distributes over  $\oplus$ .

Hence,  $(Z, \oplus, \otimes)$  is a ring.

**Commutativity of  $\otimes$**

$$\text{Now, } a \otimes b = a + b - ab \quad \text{and} \quad b \otimes a = b + a - ba$$

$$a \otimes b = b \otimes a.$$

$\therefore (Z, \oplus, \otimes)$  is a commutative ring.

**v) Unity**

$$\text{Now, } a \otimes 0 = a + 0 - a \cdot 0 = a$$

$$\text{and } 0 \otimes a = 0 + a - 0 \cdot a = a$$

$\therefore 0$  is its unity (i.e. multiplicative identity).

$\therefore (Z, \oplus, \otimes)$  is a commutative ring with unity.

**vi) Zero Divisor**

$$\text{Now, } a \otimes b = a + b - ab$$

and  $a \otimes b$  will be zero if  $a = 0$  and  $b = 0$ .

$\therefore (Z, \oplus, \otimes)$  is a ring without zero divisor.

$\therefore (Z, \oplus, \otimes)$  is an integral domain.

**vii) For  $a, b \in Z$  consider the equation  $a \otimes b = 0$  i.e.  $a + b - ab = 0$ .**

$$\therefore b = -\frac{a}{1-a}.$$

Since  $ab = 0$  for  $b = -\frac{a}{1-a}$  where 0 is its multiplicative identity,  $-\frac{a}{1-a}$  is the multiplicative inverse of  $a$ .

$\therefore (Z, \oplus, \otimes)$  is a field.

**Example 4 :** Prove that  $(Z_5, +, \cdot)$  is a field where  $Z_5$  is a set  $R$  of residue classes of  $\{0, 1, 2, 3, 4\}$  modulo 5. (M.U. 2001, 03, 06, 08)

**Sol. :** We prepare the tables for addition and multiplication of  $\{0, 1, 2, 3, 4\}$  modulo 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

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Closure : It is clear from the table that  $Z_5$  is closed under addition and multiplication modulo 5.

F1 : Consider  $(Z_5, +)$ .

- (i) Since  $a + (b + c) = (a + b) + c$ , for all  $a, b, c \in Z_5$ , addition is associative.
- (ii) Since  $a + 0 = a$  for all  $a \in Z_5$ , 0  $\in Z_5$  is the additive identity.
- (iii) Since  $1 + 4 = 0 = 4 + 1$ ,  $2 + 3 = 0 = 3 + 2$ , additive inverse exist.
- (iv) Since  $a + b = b + a$  for all  $a, b \in Z_5$ , addition is commutative.

$\therefore (Z_5, +)$  is a commutative group.

F2 : It is clear from the table that  $(a \times b) \times c = a \times (b \times c)$  for all  $a, b, c \in Z_5$ .

F3 : It can be seen that

$$a \times (b + c) = a \times b + a \times c \\ \text{and } (b + c) \times a = b \times a + c \times a$$

Hence,  $\times$  distributes over  $+$ .

F4 : Consider  $(Z_5 \setminus \{0\}, \times)$ .

- (i)  $\times$  is associative.
- (ii) From the second row or second column of second table we see that 1 is the multiplicative identity.

(iii) Since  $1 \times 1 = 1$ ,  $2 \times 3 = 1$ ,  $3 \times 2 = 1$ ,  $4 \times 4 = 1$ ,  $1^{-1} = 1$ ,  $2^{-1} = 3$ ,  $3^{-1} = 2$  and  $4^{-1} = 4$ .

For every  $a \in (Z_5 \setminus \{0\})$ , there exists multiplicative inverse.

$\therefore (Z_5 \setminus \{0\}, \times)$  is a commutative group.

Hence,  $(Z_5, +, \times)$  is a field.

Example 5 : Is  $(Z_5, +, \times)$  an integral domain ? Is it a field ?

(M.U. 2003)

Sol. : We first prepare the tables for addition and multiplication modulo 6.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Prove that it is not a field because  $3 \times 4 = 0$  but  $3 \neq 0$  and  $4 \neq 0$ .

Example 6 : Is  $(Z_p, +, \times)$  a field where  $p$  is a prime ?

Sol. : We first note that  $Z_p = \{0, 1, 2, \dots, p-1\}$  where  $p$  is any prime number.

We prepare the tables for addition and multiplication of  $Z_p$ .

+	0	1	2	3	...	$p-1$
0	0	1	2	3	...	$p-1$
1	1	2	3	4	...	$p-2$
2	2	3	4	5	...	$p-3$
3	3	4	5	0	1	$p-4$
4	4	5	0	1	2	$p-5$
$\vdots$						
$p-1$	$p-1$	0	1	2	3	$p-2$

x	0	1	2	3	...	$p-1$
0	0	0	0	0	0	0
1	0	1	2	3	...	0
2	0	2	4	1	3	5
3	0	3	6	2	5	4
4	0	4	1	3	6	2
5	0	5	4	3	2	1

Closure : It is clear that  $Z_p$  is closed under addition and multiplication modulo  $p$ .

F1 : Consider  $(Z_p, +)$ .

As in Ex. 4 page 16-59, we can prove that  $(Z_p, +)$  is a commutative group.

F2 : Consider  $(Z_p \setminus \{0\}, \times)$ .

Again as in Ex. 4 page 16-59, we can prove that  $(Z_p \setminus \{0\}, \times)$  is a commutative group.

Hence,  $(Z_p \setminus \{0\}, +, \times)$  is a field.

Note ...

In the first table the sum of  $p-1$  and  $p-1 = 2p-2$ . When this is divided by  $p$  the quotient in modulo operation is not 2 and the remainder is not -2 because the remainder in modulo operation is a negative. When  $2p-2$  is divided by  $p$  the quotient is 1 and the remainder is  $p-2$ .

Example 7 : Let  $S = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid a \in R \right\}$  and  $+$  and  $\cdot$  be matrix addition and matrix multiplication.

(M.U. 2002, 05)

Is  $S, +, \cdot$  an integral domain ? Is it a field ?

Sol. : Closure

$$\text{Let } A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}, B = \begin{bmatrix} b & b \\ b & b \end{bmatrix}, a, b \in R$$

$$\text{Then } A + B = \begin{bmatrix} a+b & a+b \\ a+b & a+b \end{bmatrix} \in S \text{ and } AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \in S$$

$\therefore S$  is closed under addition and multiplication.

I1 : Consider  $(S, +)$

(i) Matrix addition is associative.

(ii) Since  $\begin{bmatrix} a & a \\ a & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$  additive identity exists.

(iii) Since  $\begin{bmatrix} a & a \\ a & a \end{bmatrix} + \begin{bmatrix} -a & -a \\ -a & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$  additive inverse exists.

(iv) Matrix addition is commutative.

$\therefore (S, +)$  is a commutative group.

(v) For matrices  $A \cdot (B + C) = A \cdot B + A \cdot C$  and  $(B + C) \cdot A = B \cdot A + C \cdot A$

Hence,  $\cdot$  distributes over  $+$ .

$\therefore (S, +, \cdot)$  is a commutative ring.

I 2 : Consider  $(S, +, \cdot)$

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2a & 2a \\ 2a & 2a \end{bmatrix} \quad \therefore A \cdot I \neq A$$

$\therefore$  Multiplicative identity does not exist.

Hence,  $(S, +, \cdot)$  is a ring without unity.

$\therefore$  It is not an integral domain.

Since, there is no multiplicative identity, there is no multiplicative inverse.

Hence, it is not a field.

**Example 8 :** Show that the set of matrices  $M = \begin{bmatrix} a & b \\ -5b & a \end{bmatrix}, a, b \in \mathbb{Z}$  form an integral domain.

Is it a field?

Sol. : Closure

$$\text{Let } A = \begin{bmatrix} a & b \\ -5b & a \end{bmatrix}, B = \begin{bmatrix} c & d \\ -5d & c \end{bmatrix}, a, b, c, d \in \mathbb{Z}.$$

$$\text{Then } A+B = \begin{bmatrix} a+c & b+d \\ -5(b+d) & a+c \end{bmatrix} \in M \quad \text{and} \quad AB = \begin{bmatrix} ac-5bd & ad+bc \\ -5(bc+ad) & ac-5bd \end{bmatrix} \in M.$$

$\therefore M$  is closed under addition and multiplication.

I 1 : Consider  $(M, +)$

(i) Matrix addition is associative.

$$\text{(ii) Since } \begin{bmatrix} a & b \\ -5b & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ -5b & a \end{bmatrix}, a, b \in \mathbb{Z}, \text{ additive identity exists.}$$

$$\text{(iii) Since } \begin{bmatrix} a & b \\ -5b & a \end{bmatrix} + \begin{bmatrix} -a & -b \\ 5b & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \text{ additive inverse exists.}$$

(iv) Matrix addition is commutative.

$\therefore (M, +)$  is a commutative group.

$$\text{(v) For matrices } A \cdot (B+C) = A \cdot B + A \cdot C \quad \text{and} \quad (B+C) \cdot A = B \cdot A + C \cdot A.$$

Hence,  $\cdot$  distributes over  $+$ .

$\therefore (M, +, \cdot)$  is a commutative ring.

I 2 : Consider  $(M, +, \cdot)$

$$\text{Since } \begin{bmatrix} a & b \\ -5b & a \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ -5b & a \end{bmatrix}$$

Multiplicative unity exists.

Hence,  $(M, +, \cdot)$  is a ring with unity.

I 3 : Consider  $(M, +, \cdot)$

$$\begin{bmatrix} a & b \\ -5b & a \end{bmatrix} \begin{bmatrix} c & d \\ -5d & c \end{bmatrix} = \begin{bmatrix} ac-5bd & ad+bc \\ -5(bc+ad) & ac-5bd \end{bmatrix}$$

$$\text{and} \quad \begin{bmatrix} a & d \\ -5d & c \end{bmatrix} \begin{bmatrix} a & b \\ -5b & a \end{bmatrix} = \begin{bmatrix} ac-5d & ad+bc \\ -5(ad+bc) & ac-5bd \end{bmatrix}$$

Hence,  $(M, +, \cdot)$  is a commutative ring with unity but without zero divisors.

I 4 : However, no element of  $M$  has multiplicative inverse.

$\therefore (M - 0, \cdot)$  is not a group.

$\therefore (M - 0, \cdot)$  is not a field.

$\therefore$  Hence,  $(M, +, \cdot)$  is not a field.

**Example 9 :** Let  $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, a \in R \right\}$ . Is  $(S, +, \cdot)$  an integral domain?

(M.U. 2003)

sol. : Yes. Prove it.

**Example 10 :** Prove that every field is an integral domain. Is the converse true?

(M.U. 2001, 02, 94)

sol. : We know that a field is a ring  $(F, +, \cdot)$  in which  $(F - 0, \cdot)$  is a commutative group.

We also know that an integral domain is a commutative ring with unity but without zero divisors.

Thus, to prove that every field is an integral domain, we have to show that a field does not have zero divisors.

Let  $a \neq 0$  be an element of  $F$ . Then,  $a^{-1}$  exists where  $a^{-1}$  is the multiplicative inverse.

Let  $b \in F$  be such that  $ab = 0 \quad \therefore a^{-1}(ab) = 0$

$\therefore (a^{-1}a)b = b \quad \therefore 1b = 0 \quad \therefore b = 0$ .

Thus, we have if  $ab = 0$  and  $a \neq 0$  then  $b = 0$ .

$\therefore F$  has no divisors.

$\therefore$  A field is an integral domain.

But the converse is not true. Every integral domain is not a field. For example,  $\mathbb{Z}$  is an integral domain under usual addition and multiplication. But  $\mathbb{Z}$  is not a field, since  $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$ .

#### Definitions (A Review)

1. Semi-group : A non-empty set  $S$  together with a (i) binary and (ii) associative operation is called a semi-group  $(S, *)$ .

2. Monoid : A semi-group  $(S, *)$  which has identity is called a monoid.

3. Group : A non-empty set  $S$  together with a binary operation  $*$  satisfying the following axioms.

G1 : For all  $a, b, c \in S$

$$a * (b * c) = (a * b) * c \quad (\text{Associativity})$$

G2 : For all  $a \in S$  there exists  $e \in S$  such that  $a * e = e * a = a$  (Identity)

G3 : For all  $a \in S$  there exists  $b \in S$  such that  $a * b = b * a = e$  (Inverse) is called a group  $(S, *)$ .

Note that G2 and G3 make a semi-group into a group. Also note that G3 makes a monoid into a group.

## Some Algebraic Structures

**Definition :** A semi-group with identity and inverse for each element is called a group.

**Definition :** A monoid with inverse for each element is called a group.

**4. Ring :** A ring  $(R, +, \cdot)$  where  $R$  is a non-empty set and  $+$  and  $\cdot$  are two binary operations satisfying the following axioms.

**R 1 :**  $(R, +)$  is a commutative group.

**R 2 :** For all  $a, b, c \in R$ ,  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  (Associativity of  $\cdot$ )

**R 3 :** For all  $a, b, c \in R$ ,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

and  $(b + c) \cdot a = b \cdot a + c \cdot a$  ( $\cdot$  distributes over  $+$ )

Note that R 2 and R 3 make a commutative group into a ring.

**Definition :** A commutative group with another associative binary operation  $\cdot$  which distributes over  $+$  is called a ring.

**5. Integral Domain :** A commutative ring with unity and without zero divisors is called an integral domain.

**6. Field :** A commutative ring with unity, having multiplicative inverse for every non-zero element is called a field.

## EXERCISE - IV

- (A) 1. Prove that the set of even integers is a commutative ring under addition and multiplication. But it is not a field.

2. Prove that  $(3\mathbb{Z}, +, \cdot)$  where  $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$  is a ring but not a field.

3. Prove that  $(m\mathbb{Z}, +, \cdot)$  where  $m$  is a fixed integer is a ring but not a field.

4. Prove that the set of even integers is a ring under addition and multiplication. But it is not a field.

(Hint : Let  $a = 2m$ ,  $b = 2n$ ,  $m, n \in \mathbb{Z}$  etc.)

- (B) Show that  $R = \{0, 2, 4, 6, 8\}$  is a ring under addition and multiplication modulo 10. Is it an integral domain? Is it a field?

[Ans. : Yes, Yes]

- (C) 1. Prove that  $(M, +, \cdot)$  where  $M$  is the set of  $3 \times 3$  matrices is a ring but not a field.

2. Prove that  $(F, +, \cdot)$  where  $F = a + b\sqrt{5}$ ,  $a, b \in \mathbb{Q}$  is a field.

3. Prove that  $(F, +, \cdot)$  where  $F = a + b\sqrt{7}$ ,  $a, b \in \mathbb{Q}$  is a field.

4. Let  $S = \{0, 1, 2\}$ . We define  $\oplus$  as  $a \oplus b =$  the least non-negative remainder obtained on dividing  $a + b$  by 3 and  $a \otimes b =$  the least non-negative remainder obtained on dividing  $ab$  by 3 where  $a, b \in S$ .

- Prove that  $(S, \oplus, \otimes)$  is a field.

(Hint : 0 and 1 are respectively additive and multiplicative identities.  $1 \oplus 2$  implies that 1 and 2 are additive inverses of each other.  $1 \otimes 1, 2 \otimes 2$ , implies that 1 and 2 are multiplicative inverses of themselves.)

5. Show that the matrices of the form  $\begin{bmatrix} a & b \\ 2a & a \end{bmatrix}$  where  $a, b \in \mathbb{Z}$  from a field under matrix addition and multiplication.

(M.U. 1998)

6. Let  $F = \{(a, b) \mid a, b \text{ are reals}\}$ . Let  $\oplus$  and  $\otimes$  be defined as  $(a, b) \oplus (c, d) = (a+c, b+d)$  and  $(a, b) \otimes (c, d) = (ac - bd, bc + ad)$ . Prove that  $F$  is a field.

(M.U. 2004)

## EXERCISE - V

**Theory**  
1. Define a group. What is a commutative group? Give an example of a group which is not commutative.

2. In a group  $(G, \cdot)$ , prove that

(i) identity is unique.

(ii) inverse is unique.

(iii)  $(a^{-1})^{-1} = a$  for all  $a \in G$ .

(iv)  $(a^{-1} * b^{-1}) = b^{-1} * a^{-1}$  for all  $a, b \in G$ .

3. State and prove that in a group, left cancellation and right cancellation laws hold.

4. Define Homomorphism and Isomorphism of groups. Give an example of each.

5. Define : Commutative Ring, Ring' with unity Ring with zero Divisor. If  $R$  is a ring with unity, prove that this unity 1 is the only multiplicative unity.

6. Define the following terms -

(i) Ring, (ii) Commutative Ring, (iii) Ring with unity,

(iv) Ring with zero divisors, giving one example of each.

7. Let  $R$  be a non-empty set with two binary operations addition and multiplication denoted by  $+$  and  $\cdot$ . Explain when the algebraic structure  $(R, +, \cdot)$  becomes a ring.

Show the set  $R$  consisting of a single element 0 with two binary operations defined by  $1+0=0, 0 \cdot 0=0$  is a ring.

8. If  $R$  is a ring with unity, prove that this unity is the only multiplicative unity. (M.U. 2004)

(Hint : Refer to § 13(c), (iv) page 16-50.)

9. Define the terms (i) Ring with unity, (ii) Ring without zero divisor, (iii) Ring with zero divisor.

10. Prove that every field is an integral domain. Is the converse true? Give an example of integral domain.

11. Give examples of binary operations  $*_1, *_2, *_3$  and  $*_4$  on  $\mathbb{Z}$  such that  
(i)  $*_1$  is commutative but not associative. (ii)  $*_2$  is associative but not commutative.  
(iii)  $*_3$  is neither associative nor commutative. (iv)  $*_4$  is both associative and commutative.

[Ans. : (i)  $a * b = \frac{a+b}{2}$  is commutative but not associative. (ii)  $a * b = a \times |b|$  is associative but not commutative. (iii) Usual subtraction or usual division is neither associative, nor commutative. (iv) Usual addition or multiplication is both associative and commutative.]

12. State with justification whether the following statement is true or false. Both addition and multiplication are binary operations on  $A = \{-1, 0, 1\}$ .

[Ans. : Prepare + and  $\times$  tables. + is not binary;  $\times$  is.]

13. Give an example of each of the following.  
(i) A commutative ring with unity.  
(ii) A non-commutative ring with unity.

(M.U. 2002)

**Applied Mathematics - IV**

(16-65)

**Some Algebraic Structures**

[Ans.: (i)  $(Z, +, \cdot)$  is a commutative ring with unity. (ii)  $(M_n, +, \cdot)$ , where  $M_n$  is the set of all  $n \times n$  matrices in non-commutative with unit matrix  $I_n$  as unity.]

14. Give examples of the following with proper justification.

- (i) An Abelian group having 6 elements.
- (ii) Binary operation on  $Z$  which is commutative but not associative.
- (iii) ring having zero divisor.

[Ans.: (i) Let  $G = \{0, 1, 2, 3, 4, 5\}$  and let  $*$  be addition modulo 6. Then  $G \setminus \{0\}$  is an Abelian group. (ii) Let  $*$  be defined on  $Z$  as  $a * b = ab + |a| + |b|$ . Then  $*$  is commutative but not associative. (iii) Let  $(R, +, \times)$  where  $R = \{0, 1, 2, 3, 4, 5\}$  and  $+$  and  $\times$  are operations of addition modulo 6 and multiplication modulo 6. Then  $R$  is a ring with zero divisors because  $3 \times 4 = 12 \equiv 0 \pmod{6}$ ,  $2 \times 3 = 6 \equiv 0 \pmod{6}$ .]

15. State true or false with proper justification.

(i) If  $S = \{[2], [4], [6]\}$  then  $S$  has no identity element under multiplication modulo 10. (Where  $[2], [4], \dots$  denote the set of integers congruent to 2, 4, ..., modulo 10).

- (i) Inverse of an element in a group is unique.
- (ii) Field cannot have finite number of elements.

(M.U. 2002)

[Ans.: (i) Prepare the table for  $A = \{2, 4, 6, 8\}$  multiplication modulo 10. From the third column (under 10) we see that 6 is the identity element. Hence, false. (ii) True. (iii) False.]

16. Do the following sets form integral domains with respect to addition and multiplication?

- (i) The set of even integers ?
- (ii) The set of positive integers.

(M.U. 1997) [Ans.: (i) No, (ii) Yes.]

17. Give an example of

- (i) Non-abelian group, (ii) Abelian group of order 4.

(M.U. 1998)

[Ans.: (i)  $G$  is the set of rational numbers different from 1,  $a * b = a + b - ab$

- (ii)  $G = \{1, 2, 3, 4\}$  is an Abelian group under multiplication modulo 5.]
- ★ ★ ★
18. State true or false :- If  $*$  is a binary operation on real numbers as  $a * b = \frac{a+b}{2}$  then it is associative.
19. Define the following terms with proper illustrations
- (1) Semigroup
  - (2) Monoid
  - (3) Group
  - (4) Commutative Group
  - (5) Cyclic Group
  - (6) Subgroup
  - (7) Coset
  - (8) Normal Subgroup
  - (9) Quotient Group
  - (10) Isomorphism
  - (11) Group Codes
  - (12) Minimum distance of an encoding function
- (M.U. 1999, 2000, 09, 10, 16)
- (M.U. 1999, 2000, 09, 10, 16)
- (M.U. 2000, 01, 09, 10, 16)
- (M.U. 2002)
- (M.U. 1999, 2000)
- (M.U. 2001, 02, 04, 05, 10)
- (M.U. 1998, 2001)
- (M.U. 2000, 02, 05, 07, 10)
- (M.U. 2000)
- (M.U. 1999)
- (M.U. 1999, 2000, 05)
- (M.U. 1998, 99)
- Applied Mathematics - IV**
- (16-66)
- Some Algebraic Structures**
- (13) Ring
  - (14) Commutative Ring
  - (15) Subring
  - (16) Field
  - (17) Integral Domain
  - (18) Ring Homomorphism
  - (19) Ring Isomorphism
  - (20) Ring Automorphism.
- (M.U. 2000, 01, 02)  
 (M.U. 2000)  
 (M.U. 1997)  
 (M.U. 2002, 05)  
 (M.U. 2002, 06)  
 (M.U. 2002, 04)  
 (M.U. 2002, 05, 07)

# CHAPTER 17

## Equivalence Relations And Posets

### 1. Introduction

We are familiar with the concept of relation as used in everyday language. We know various relationships between people, (e.g. "is a son of", "is a friend of" etc.), numbers (e.g. "is square of", "is a cube root of" etc.), sets (e.g. "is a subset of", "is complement of" etc.). These relationships lead us to the formal concept of a binary relation. We shall then discuss a special type of relations, a function. Function is a very old and very important concept in classical as well as modern mathematics.

**Notation :** We shall use the following standard notation throughout this book :

- (a)  $Z$  = the set of all integers positive or negative including zero :  
-4, -3, -2, -1, 0, 1, 2, 3, 4, ....
- (b)  $Z^+$  =  $N$  = the set of all positive integers : 1, 2, 3, 4, ....
- (c)  $Z^{-T}$  = the set of all negative integer : -1, -2, -3, -4, ....
- (d)  $W$  = the set of positive integers including zero : 0, 1, 2, 3, 4, ....
- (e)  $Q$  = the set of all rational numbers.
- (f)  $R$  = the set of all real numbers.

In the chapter on set theory we have studied Cartesian product and partition. We shall briefly review these concepts for the sake of revision and proceed to study relations and functions.

### 2. Cartesian Product

(M.U. 2011)

**Definition :** An ordered pair  $(a, b)$  is a listing of two objects  $a$  and  $b$  in the given order, with  $a$  appearing first and  $b$  appearing second.

Thus,  $(2, 3)$ ,  $(x, y)$  are ordered pairs. Since in the ordered pair, order in which the elements are listed is important, the ordered pair  $(2, 3)$  is not equal to the ordered pair  $(3, 2)$ . We know that the point  $(2, 3)$  is different from the point  $(3, 2)$ . In the same manner  $(x, y) \neq (y, x)$ .

**Definition :** The ordered pairs  $(a_1, b_1)$  and  $(a_2, b_2)$  are **equal** if and only if  $a_1 = a_2$  and  $b_1 = b_2$ .

**Definition :** If  $A$  and  $B$  are two non-empty sets then we define the **product set** or **cartesian product**  $A \times B$  as the set of all ordered pairs  $(a, b)$  such that  $a \in A$  and  $b \in B$ . Thus,  $A \times B = \{(a, b) | a \in A \text{ and } b \in B\}$ .

It is easy to see that if  $A$  has  $n_1$  elements and  $B$  has  $n_2$  elements then  $A \times B$  has  $n_1 n_2$  elements.

The product  $AB$  is named after the French mathematician and philosopher René Descartes.

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

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

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

### 17-2

### Equivalence Relations & Posets

In this case clearly  $A \times B = B \times A$  and so we write it as  $A \times A$ .

The elements of a cartesian product  $A \times B$  can also be shown in a tabular way as follows,

A	B	1	2	3
1		(1, 1)	(1, 2)	(1, 3)
2		(2, 1)	(2, 2)	(2, 3)
3		(3, 1)	(3, 2)	(3, 3)

### 17-2

### Equivalence Relations & Posets

In this case clearly  $A \times B = B \times A$  and so we write it as  $A \times A$ .

The elements of a cartesian product  $A \times B$  can also be shown in a tabular way as follows,

A	A	1	2	3
1		(1, 1)	(1, 2)	(1, 3)
2		(2, 1)	(2, 2)	(2, 3)
3		(3, 1)	(3, 2)	(3, 3)

### Remark

Generally, we need to take the cross product of  $A$  with  $A$  itself.

### 3. Partition of a Set

**Definition :** A collection  $\mathcal{P}$  of subsets of  $A$  is called a **partition** or **quotient set** of a non-empty set  $A$  if

- (i) each subset  $A_i$  is non-empty.
- (ii) each element of  $A$  belongs to one of the sets in  $\mathcal{P}$ .
- (iii) if  $A_1$  and  $A_2$  are two distinct elements of  $\mathcal{P}$  then  $A_1 \cap A_2 = \emptyset$ .

The members of the partition i.e.  $A_1, A_2, \dots$  etc. are called **blocks** or **cells** of the partition.

In other words if  $A$  is a given set and if  $A_1, A_2, \dots, A_n$  are subsets of  $A$  then  $\{A_1, A_2, \dots, A_n\}$  represents a partition of  $A$  if

- (i) each  $A_i$  is non-empty.
- (ii)  $A_1 \cup A_2 \cup A_3 \cup \dots \cup A_k = A$  and
- (iii)  $A_i \cap A_j = \emptyset$  for all  $i \neq j$

every element of  $A$  must belong to one of the subset  $A_i$  and no element must belong to two or more subsets.

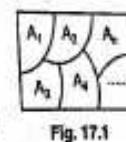


Fig. 17.1

The collection of non-empty, pairwise disjoint subsets of  $A$  whose union is  $A$  is called a **partition** of  $A$ .

The figure given above shows a partition of the set  $A$ .

$$\therefore \mathcal{P} = \{A_1, A_2, A_3, \dots, A_n\}$$

$A_1, A_2, \dots, A_n$  are the **blocks** or the **cells** of the partition.

**Example :** Let  $A = \{1, 2, 3, 4, 5, 6\}$ . Find whether or not each of the following is a partition of  $A$ .

- (i)  $P_1 = \{(1, 3, 5), (2, 4, 5, 6)\}$
- (ii)  $P_2 = \{(1, 3, 5), (2, 1) (6)\}$
- (iii)  $P_3 = \{(1, 3, 6), (2, 4, 5, 7)\}$
- (iv)  $P_4 = \{(1, 2), (3, 4, 5), (6)\}$

**Sol.:** To answer such questions, it is convenient to draw Venn diagrams.

1, 3, 5
2, 4, 5, 6

Fig. (a)

3, 5
2, 1

Fig. (b)

1, 3, 6
2, 4, 5, 7

Fig. (c)

1, 2	6
3, 4, 5	

Fig. (d)

Fig. 17.2

- (i) Since 5 belongs to two cells,  $P_1$  is not a partition. [Fig. 17.2 (a)]  
(ii) Since 4 does not belong to any cell,  $P_2$  is not a partition. [Fig. 17.2 (b)]  
(iii) Since 7 does not belong to  $A$ ,  $\{2, 4, 5, 7\}$  is not a subset of  $A$ . Hence,  $P_3$  is not a partition. [Fig. 17.2 (c)]  
(iv)  $P_4$  is a partition of  $S$ . [Fig. 17.2 (d)]

#### 4. Relation

We know what we mean by a relation. A relation can be stated as a rule or can be given as an ordered pair. A set of all such ordered pairs, in each of which the first member has some definite relationship with the second member describes particular relationship. In what follows we shall be concerned with relations between two objects; such a relation is called a **binary relation**.

We are here concerned with most abstract relations which may not be described verbally or symbolically. If  $A$  and  $B$  are two sets and if there is a relation between elements of  $A$  and elements of  $B$  it is enough for us to know which element of  $A$  is related to which element of  $B$ . If we know the complete list of related pairs of elements, we know the relation. We shall denote a relation by  $R$ . If the elements  $a$  and  $b$  of a set are related, we shall denote it by  $a R b$  and if they are not related, we shall denote it by  $a \not R b$ . If  $A = \{1, 2, 3\}$  and we define  $R$  from  $A$  to  $A$  as  $1 R 2, 1 R 3, 2 R 3$ , this is the "less than" relation. We might express this as a set of ordered pair  $R = \{(1, 2), (1, 3), (2, 3)\}$ . But this is a subset of  $A \times A$  (See Ex., page 17-2). In this way we can define a relation from  $A$  to  $B$  as a subset of the cartesian product  $A \times B$ .

**Definition :** Let  $A$  and  $B$  be two non-empty sets. A relation  $R$  from  $A$  to  $B$  is defined as a subset of  $A \times B$ . If  $R \subseteq A \times B$  and if  $(a, b) \in R$  then we say that  $a$  is related to  $b$  by  $R$  and we denote it as  $a R b$ . If  $a$  is not related to  $b$  we denote it as  $a \not R b$ .

**Example 1 :** Let  $A = \{1, 2, 3\}$ ,  $B = \{a, b\}$ . Then  $R = \{(1, a), (2, b)\}$  is a relation from  $A$  to  $B$ .

**Example 2 :** Let  $A = \{1, 2, 3, 4\}$ . Let the relation  $R$  be "is less than".  $a R b$  if  $a < b$ . Then  $R = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$ .

**Example 3 :** Let  $A$  be a set of real numbers. We define the relation "is equal to" by  $a R b$  if and only if  $a = b$ ,  $a \in A$ ,  $b \in A$ .

**Example 4 :** Let  $R$  be the relation on  $A = \{2, 3, 4, 5, 6\}$  defined by  $a R b$  if and only if  $|a - b|$  is divisible by 3. Write  $R$  as a set of ordered pairs. (M.U. 1997)

**Sol. :** It is easy to see that the relation  $R$  as a set of ordered pairs can be written as,  
 $R = \{(2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (2, 5), (5, 2), (3, 6), (6, 3)\}$ .

#### 5. Diagram of a Relation

Relation can be easily represented and clearly understood if we represent it by a diagram as follows. We denote the two sets  $A$  and  $B$  by some geometric figures such as circles or ellipses as usual. Show the elements of  $A$  and  $B$  of the sets by dots inside these figures. We then draw an arrow from the element of  $A$  to the element of  $B$  to which it is related. This is done for all elements of  $A$  which are related to the elements of  $B$ . This is the required diagram of the relation  $R$ .

**Example :** Draw the diagrams of the relations in Ex. 1, 2 and 4 above (previous page).

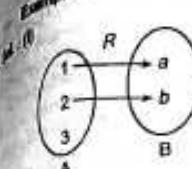


Fig. 17.3 (a)

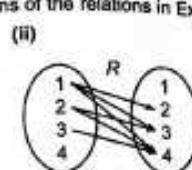


Fig. 17.3 (b)

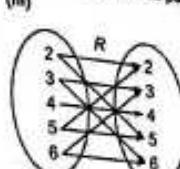


Fig. 17.3 (c)

#### i. Matrix of a Relation

A relation between two finite sets can be represented by a matrix as follows.

**Definition :** If  $A = \{a_1, a_2, \dots, a_m\}$ ,  $B = \{b_1, b_2, \dots, b_n\}$  are finite sets containing  $m$  and  $n$  elements, respectively, and if  $R$  is a relation from  $A$  to  $B$ , we represent  $R$  by the matrix  $M_R = [m_{ij}]$  of order  $m \times n$  which is defined by

$$m_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R \\ 0 & \text{if } (a_i, b_j) \notin R \end{cases}$$

To write the matrix  $M_R$ , we write the elements of  $A$  vertically on the left and the elements of  $B$  horizontally at the top outside the matrix.

The matrix  $M_R$  is called the **adjacency matrix** of the relation  $R$  or simply the matrix of the relation  $R$ . Conversely from a given matrix of a relation we can write the relation as a set.

**Definition :** The matrix whose elements are either 1 or 0 is called a **Boolean Matrix**.

Thus, a Boolean matrix can be looked upon as an adjacency matrix and conversely.

**Example 1 :** Let  $R$  be the relation given in Ex. 1 above. Write the matrix of  $R$ .

**Sol. :** The matrix of  $R$  is,

$$M_R = 2 \begin{bmatrix} a & b \\ 1 & 0 \\ 0 & 1 \\ 3 & 0 \\ 0 & 0 \end{bmatrix}$$

**Example 2 :** Let  $R$  be the relation given in Ex. 2 above. Write the matrix of  $R$ .

**Sol. :** The matrix of  $R$  is

$$M_R = 4 \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & 1 \\ 2 & 0 & 0 & 1 & 1 \\ 3 & 0 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 & 0 \end{bmatrix}$$

**Example 3 :** Let the matrix of a relation between  $A = \{a_1, a_2, a_3\}$  and  $B = \{b_1, b_2, b_3, b_4\}$  be

$$M_R = a_2 \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Write the relation.

Sol. : We know that if  $m_{ij} = 1$  then  $(a_i, b_j) \in R$ . i.e.  $a_i R b_j$  and if  $(a_i, b_j) = 0$  then  $(a_i, b_j) \notin R$ . In other words, if there is 1 in the matrix, we form a pair of elements on the left and on the right in that order.

$$\therefore R = \{(a_1, b_1), (a_1, b_3), (a_2, b_2), (a_2, b_4), (a_3, b_2), (a_3, b_3), (a_3, b_4)\}$$

**Example 4 :** Let the matrix of a relation between  $A = \{1, 2, 3\}$  and  $B = \{a, b, c, d\}$  be

$$M_R = 2 \begin{bmatrix} a & b & c & d \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 3 & 1 & 0 & 1 \end{bmatrix}$$

Write the relation.

$$\text{Sol. : } R = \{(1, a), (1, b), (2, b), (2, d), (3, a), (3, c)\}.$$

**Remark ...**

Note that the number of 'ones' in the matrix  $M_R$  is equal to the number of pairs in the relation  $R$ . In Example 4 there are six 'ones' in the matrix  $M_R$  and this is equal to the number of pairs in  $R$ .

#### Matrix of a relation is not unique

The matrix of a relation is not unique. By changing the order of the elements of  $A$  along the row or along the column or both but maintaining the same relation we get different matrices. For example, in Ex. 2 above, we can have the following matrices.

$$\begin{array}{c} \begin{array}{cccc} 1 & 2 & 4 & 3 \\ 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 \\ 3 & 0 & 0 & 1 \end{array} \quad \begin{array}{cccc} 1 & 2 & 4 & 3 \\ 3 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 1 \end{array} \end{array}$$

## 7. Digraph of a Relation

A relation from  $A$  to  $A$  can also be represented pictorially as follows :-

Draw a small circle for each element of  $A$  and write the element in that circle. These circles called **vertices**. If the element  $a_i$  is related to the element  $a_j$ , i.e. if  $a_i R a_j$ , draw a straight line or an arc with an arrow in the direction from  $a_i$  to  $a_j$ . Such a straight line or an arc with an arrow is called an **edge**. If an element  $a_i$  is related to itself, we draw an arc with an arrow head starting and ending at  $a_i$ . Such an arc is called a **loop**. The resulting pictorial representation is called **directed graph** or **digraph** of  $R$ .

Thus, if a relation  $R$  on  $A$  is represented by a digraph then the edges and loops in the digraph correspond to the pairs in  $R$  and the vertices correspond to the elements of  $A$ .

Conversely if a digraph is given we can write the set of the corresponding relation.

**Example 1 :** Let  $A = \{1, 2, 3, 4\}$  obtain digraph for

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

Sol. : To draw the digraph we first draw one small circle for each of the four elements of  $A$ . Write the elements in these circles and connect the elements by arrows if they are related e.g. 1 is related to 1, so we draw a curve with an arrow head starting from 1 and going to 1; 1 is related to 2 so we draw a straight line with an arrow head starting from 1 and going to 2 and so on.

**Remark ...**

The total number of "arrow heads" or "edges (including loops)" in the digraph is equal to the number of pairs in  $R$ . Considering this remark and the remark given above, we can say that the number of 'ones' in the matrix  $M_R$  = the number of arrow heads in the digraph = the number of pairs in  $R$ .

**Example 2 :** Find the relation determined by the following digraph.

Sol. : By definition  $a_i R a_j$ , if and only if there is an arrow from  $a_i$  to  $a_j$ . Since there is an arrow from 1 to 2, 1 R 2; since there is an arrow from 2 to 2, 2 R 2; there is an arrow from 1 to 3, 1 R 3 and so on. In this way we consider each vertex and get

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

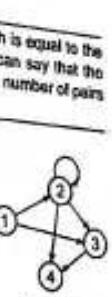


Fig. 17.5

**Example 3 :** Let  $A = \{1, 3, 7\}$  and  $R$  be given by the digraph shown below. Find  $M_R$  and  $R$ .

Sol. :

$$M_R = 3 \begin{bmatrix} 1 & 3 & 7 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 7 & 0 & 1 \end{bmatrix}$$

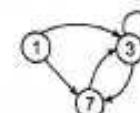


Fig. 17.6

$$R = \{(1, 3), (1, 7), (3, 3), (3, 7), (7, 3)\}.$$

**Example 4 :** Let  $A = \{1, 2, 3, 4\}$  and let  $R$  be the relation 'greater than'. Represent  $R$  as a set, a digraph, a matrix and diagram.

$$\text{Sol. : } R = \{(2, 1), (3, 1), (4, 1), (3, 2), (4, 2), (4, 3)\}$$

$$M_R = 4 \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 1 & 1 & 0 \\ 4 & 1 & 1 & 1 \end{bmatrix}$$

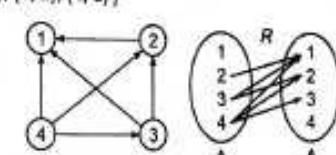


Fig. 17.7

**Remark ...**

There are six 'ones' in  $M_R$ , six arrow heads in the digraph and six pairs in the set  $R$  as stated in the remark at the top.

**Example 5:** Let  $A = \{2, 3, 4, 6, 8\}$ . Let  $R$  be defined on  $A$  by "If  $x$  divides  $y$  then  $x R y$ ". Find  $R$ , its matrix, its digraph and diagram.

Sol.:  $R = \{(2, 2), (2, 4), (2, 6), (2, 8), (3, 3), (3, 6), (4, 4), (4, 8), (6, 6), (8, 8)\}$

$$M_R = \begin{bmatrix} 2 & 3 & 4 & 6 & 8 \\ 2 & 1 & 0 & 1 & 1 \\ 3 & 0 & 1 & 0 & 0 \\ 4 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 0 & 1 \\ 8 & 0 & 0 & 0 & 0 \end{bmatrix}$$

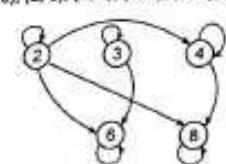


Fig. 17.8 (a)

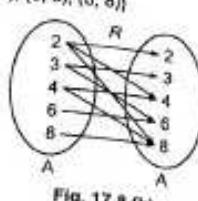


Fig. 17.8 (b)

**Remark** ....

We note for the last time that the number of pairs in  $R$ , the number of '1's in  $M_R$  and the number of arrow heads ( $\rightarrow$ ) in the digraph are all equal.

**8. Types of Relations**

Relations can be classified in the following classes.

- 1. Reflexive Relations
- 2. Symmetric, Asymmetric and Antisymmetric Relations
- 3. Transitive Relations
- 4. Equivalence Relations

**9. Properties of Relations**

If we consider a relation  $R$  on  $A$ , the relation satisfies certain properties. We consider these properties below.

**(a) Reflexive and Irreflexive Relations**

**Definition:** A relation  $R$  on a set  $A$  is called **reflexive** if  $(a, a) \in R$  for all  $a \in A$  i.e. if  $a R a$  for all  $a \in A$  (Note all).

A relation  $R$  on a set  $A$  is called **irreflexive** if  $(a, a) \notin R$  for all  $a \in A$  i.e.  $a \not R a$  for all  $a \in A$  (Note all).

In other words,  $R$  is reflexive if each element of  $A$  is related to itself and it is irreflexive if no element is related to itself.

(i) Since in a reflexive relation every element is related to itself in the matrix  $M_R$  of a reflexive relation we should have **all diagonal elements unity**. Non-diagonal elements may be zero or unity.

(ii) By the same reasoning in the matrix of an irreflexive relation we should have **all diagonal elements zero**.

(iii) In a matrix of a relation which is neither reflexive nor irreflexive, we have in the diagonal some at least one 1 and some at least one zero.

In the digraph of a reflexive relation we should have **a loop around each vertex**. These vertices may be or many not connected to one another and in the digraph of an irreflexive relation we should have **no loop around any vertex**. In the digraph of a relation which is neither reflexive nor irreflexive we show should have **some at least one vertex with a loop around it and some at least one vertex without a loop around it**.

$$\begin{bmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{bmatrix}$$

Some Diagonal Elements are unity some are zero.

Example 1 : Let  $A$  be any (non-empty) set and  $R = \Phi$  (null set).

This relation is not reflexive because there is no element  $a$  in  $A$  such that  $(a, a) \in \Phi$  as  $\Phi$  does not have any element.

But this relation is not irreflexive also because we cannot show any element which is not related to itself as  $\Phi$  does not have any element.

Since  $\Phi$  is empty, the matrix of the relation is also empty.

Example 2 : Let  $A = \{a, b, c\}$ . The relation  $R_1 = \{(a, a), (b, b), (c, c), (a, c), (b, c)\}$  is reflexive,  $R_2 = \{(a, b), (b, c), (a, c)\}$  is irreflexive and  $R_3 = \{(a, a), (a, b), (a, c)\}$  is neither reflexive nor irreflexive. Their matrices and digraphs are

$$M_{R_1} = \begin{bmatrix} a & b & c \\ a & 1 & 0 & 1 \\ b & 0 & 1 & 1 \\ c & 0 & 0 & 1 \end{bmatrix} \quad M_{R_2} = \begin{bmatrix} a & b & c \\ a & 0 & 1 & 1 \\ b & 0 & 0 & 1 \\ c & 0 & 0 & 0 \end{bmatrix} \quad M_{R_3} = \begin{bmatrix} a & b & c \\ a & 1 & 1 & 1 \\ b & 0 & 0 & 0 \\ c & 0 & 0 & 0 \end{bmatrix}$$

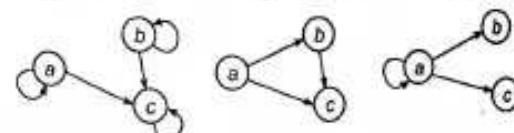
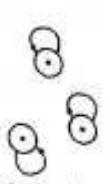
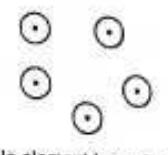


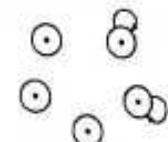
Fig. 17.9



All elements have loops.



No element has a loop.



Some elements have loops and some don't have.

Note carefully that a relation cannot be reflexive and irreflexive simultaneously. But it can be neither reflexive nor irreflexive simultaneously as in the above example.

#### 10. Symmetric, Asymmetric and Anti-symmetric Relations

We know that the relation of "equality" is such that if " $a = b$  then  $b = a$ ". This is called a symmetric relation. Further, if " $a < b$ , then  $b < a$ ". This is called an asymmetric relation. If " $a \leq b$ , then  $b \leq a$ , then  $a = b$ ". This is called an anti-symmetric relation. In the light of these examples, we shall now define the terms :-

##### Symmetric, Asymmetric and Antisymmetric Relations

**Definition 1 :** A relation  $R$  on a set  $A$  is called symmetric if whenever  $a R b$  we have  $b R a$ .

In other words, if  $a R b$  then for symmetry we should have  $b R a$ .

It follows that a relation  $R$  on  $A$  is not symmetric if we can find some  $a, b \in A$  such that  $a R b$  but  $b \not R a$ .

**Example 1 :** Let  $A$  be set of all males and  $R$  be relation of "being a brother". The relation is symmetric because if  $a$  is a brother of  $b$  then  $b$  is also a brother of  $a$  i.e.  $a R b$  then  $b R a$ .

Because of the above definition the matrix of a symmetric relation  $M_R$  satisfies the property that if  $m_{ij} = 1$  then  $m_{ji} = 1$  and if  $m_{ij} = 0$  then  $m_{ji} = 0$ .

This means the matrix of a symmetric relation is symmetric. i.e. the matrix  $M_R$  is a square matrix and non-diagonal elements 0 and 1 are symmetrically placed. Hence, the transpose  $M_R$  of a symmetric matrix is  $M_R$  itself and  $M_R$  must be a square matrix.

In the digraph of a symmetric relation if there is an edge from  $i$ -th vertex to the  $j$ -th vertex, there is also an edge from the  $j$ -th vertex to the  $i$ -th vertex. In other words in the digraph of a symmetric relation the edges appear in "both directions" i.e. in a symmetric relation there are no (arrowheads) lines connecting one vertex to another or there is no line at all. There is "both traffic" or the lane is "closed both ways".

**Example 2 :** Let  $A = \{1, 2, 3, 4\}$  and  $R = \{(1, 2), (2, 1), (2, 2), (3, 1), (1, 3), (3, 4), (4, 3), (4, 2)\}$

The relation is symmetric because whenever  $a R b$  we have  $b R a$ . Its matrix and digraph are shown below.

1	2	3	4
0	1	1	0
1	0	0	0
3	1	0	0
4	0	1	1

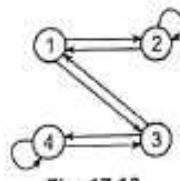


Fig. 17.10

**Note ...**

Note that the matrix  $M_R$  is a square matrix and a symmetric matrix. The diagonal elements may be 1 or zero. In the digraph a vertex is connected to another vertex by two lines or not connected at all.

**Example 3 :** If  $A$  is a set of people and  $R$  is a relation defined on  $A$  as  $R = \{(x, y) | (x, y) \in A \times A \text{ and } x \text{ is a sister of } y\}$

Verify if  $R$  is symmetric.

**Sol. :** If  $x$  and  $y$  are both female and if  $x$  is a sister of  $y$  then obviously  $y$  is a sister of  $x$ . But if  $x$  is female and  $y$  is male and if  $x$  is a sister of  $y$  then  $y$  is not a sister of  $x$ .  $y$  is a brother of  $x$ .

The relation is not symmetric.

**Example 4 :** Let  $A = \{1, 4, 5\}$  and  $R$  be relation on  $A$  defined by a  $R$  if  $a + b \leq 5$ . Write  $R$ ,  $M_R$  and check for reflexivity and symmetry.

**Sol. :** (i) Since  $1 + 1 \leq 5$ ,  $1 + 4 \leq 5$ ,  $1 + 5 \leq 5$ ,  $1 R 1$

But  $4 + 5 \not\leq 5 \therefore 4 \not R 5$ .

Also  $4 + 4 \not\leq 5 \therefore 4 \not R 4$ ,  $5 + 5 \not\leq 5 \therefore 5 \not R 5$ .

Hence, we get  $R = \{(1, 1), (1, 4), (1, 5), (4, 1), (5, 1)\}$

$$\text{And } M_R = 4 \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

The relation is symmetric but not reflexive.

**Definition 2 :** A relation  $R$  on  $A$  is called asymmetric if whenever  $a R b$  then  $b \not R a$ . It follows that a relation on  $A$  is not asymmetric if for some  $a, b \in A$ , we have both  $a R b$  and  $b R a$ .

The matrix  $M_R$  of an asymmetric relation is such that if  $m_{ij} = 1$  then  $m_{ji} = 0$  for all  $i$  and  $j$ . Hence, we must have  $m_{ii} = 0$  for all  $i$ . In other words, all diagonal elements of  $M_R$  of an asymmetric matrix are zero and non-diagonal elements are not symmetrically placed.

In the digraph of an asymmetric relation since, we have  $a R b$  but  $b \not R a$ , we have all edges in "one direction" only. Also there is no loop around any element.

**Example 5 :** Let  $A = \{1, 2, 3, 4\}$  and let  $R = \{(1, 2), (2, 3), (3, 4), (4, 2)\}$

The relation is asymmetric because we have  $a R b$  but  $b \not R a$  for all  $a, b$ .

$$\text{And } M_R = 4 \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 1 \\ 4 & 0 & 1 & 0 & 0 \end{bmatrix}$$

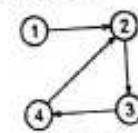


Fig. 17.11

**Note ...**

Note that the above matrix  $M_R$  is not a symmetric matrix with all diagonal elements zero. In the digraph there are no "double lines" and no loop around any vertex.

**Definition 3 :** A relation  $R$  on a set  $A$  is called antisymmetric if whenever  $a R b$  and  $b R a$ , then  $a = b$ . The contrapositive statement of this definition is that a relation  $R$  is antisymmetric if  $a \neq b$  then  $a \not R b$  or  $b \not R a$ .

It follows that a relation is not antisymmetric if  $a \neq b$  and we have both  $a R b$  and  $b R a$ .

The matrix of the antisymmetric relation is such that if  $i \neq j$  then  $m_{ij} = 0$  or  $m_{ji} = 0$  or both zero. If  $i = j$ ,  $m_{ii}$  may be 1 or zero. There is no condition imposed on  $m_{ii}$ .

In the digraph of an antisymmetric relation whenever  $i \neq j$  there can be only "one way" edges. If  $i = j$  no condition is imposed. There may or may not be a loop around a vertex.

**Remark ...**

The relation of " $=$ " is symmetric, of " $<$ " is asymmetric and of " $\leq$ " is anti-symmetric.

**Example 1 :** If  $S$  is any set and  $P^S$  is its power set (set of all subsets of  $S$ ) the relation  $\subseteq$  (is a subset of) is an antisymmetric relation.

**Sol. :** If  $A \subseteq B$  and  $B \subseteq A$ , then we know that  $A = B$ .  
 $\therefore \subseteq$  is an antisymmetric relation on  $P^S$ .

**Example 2 :** If  $Z^+$  is the set of all positive integers, then the relation  $\leq$  (less than or equal to) is an antisymmetric relation.

**Sol. :** If  $a, b$  are two positive integers and if  $a \leq b$  and  $b \leq a$  then we know that  $a = b$ .  
 $\therefore \leq$  is an antisymmetric relation of  $Z^+$ .

**Example 3 :** If  $Z^+$  is the set of all positive integers then  $\geq$  (greater than or equal to) is an antisymmetric relation.

**Sol. :** Let it to you.

**Example 4 :** If  $Z^+$  is the set of all positive integers then 'a divides b' and 'b divides a' where  $a, b \in Z^+$  is an antisymmetric relation.

**Sol. :** If  $a, b$  are two positive integers and if  $a$  divides  $b$  and  $b$  also divides  $a$ , then clearly  $a = b$ .  
 $\therefore$  "a divides b" and "b divides a" is an antisymmetric relation in  $Z^+$ .

**Example 5 :** Let  $R = \{(1, 2), (1, 3), (2, 1), (4, 1), (4, 3), (4, 4)\}$

The relation is antisymmetric because we have whenever  $a R b$  and  $b R a$  then  $a = b$  and when  $a \neq b$ , we have  $a \not R b$  or  $b \not R a$ .

$$M_R = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 4 & 1 & 0 & 1 \end{bmatrix}$$

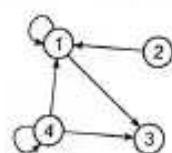


Fig. 17.12

**Note ...**

Note the matrix  $M_R$  is not a symmetric matrix with some diagonal elements zero. In the digraph there are no double lines.

The matrices of symmetric, asymmetric and antisymmetric relations are square matrices. In the symmetric relation, the matrix is symmetric with no restriction on diagonal elements. In the asymmetric relation, the matrix is asymmetric with all diagonal elements zero. In the antisymmetric relation, the matrix is asymmetric with no restriction on the diagonal elements. In the digraph of a symmetric relation two vertices are connected by two lines, there may or may not be a loop around a vertex. In the digraph of an asymmetric relation, all lines are single lines and there is no loop

around any vertex. In the digraph of antisymmetric relation all lines are single lines and there are two around some vertices.

**Remark ...**

To prove that a relation does not have a particular property it is enough to have one pair  $(a, b)$  in which the property does not hold i.e.  $a \not R b$ .

**Example 6 :** Let  $A = \{1, 2, 3, 4\}$  and  $R = \{(1, 2), (1, 3), (3, 3), (3, 4)\}$

State the nature of the relation. Give its matrix and digraph.

**Sol. :** The relation is not symmetric because  $(1, 2) \in R$  but  $(2, 1) \notin R$  i.e.  $1 R 2$  but  $2 \not R 1$ .

The relation is not asymmetric because  $(3, 3) \in R$ .

The relation is antisymmetric because whenever  $a R b$ ,  $b R a$  then  $a = b$  e.g.  $(3, 3) \in R$  and whenever  $a \neq b$  then either  $a \not R b$  or  $b \not R a$ .

$$M_R = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 \\ 3 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 \end{bmatrix}$$

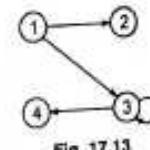


Fig. 17.13

**Example 7 :** Let  $A = \{1, 2, 3, 4\}$  and  $R = \{(1, 3), (1, 4), (2, 4), (4, 1)\}$ .

State the nature of the relation. Give its matrix and digraph.

**Sol. :** The relation is not symmetric because  $(1, 3) \in R$  but  $(3, 1) \notin R$ .

It is not asymmetric because both  $(1, 4) \in R$  and  $(4, 1) \in R$ .

It is not antisymmetric because  $(1, 4) \in R$  and  $(4, 1) \in R$  but  $4 \neq 1$ .

$$M_R = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 4 & 1 & 0 & 0 \end{bmatrix}$$



Fig. 17.14

**Example 8 :** Let  $A = \{1, 2, 3, 4\}$  and  $R = \{(1, 1), (1, 4), (2, 2), (2, 3), (4, 4)\}$ .

State the nature of the relation. Give its matrix and digraph.

**Sol. :** Since  $(1, 4) \in R$  but  $(4, 1) \notin R$ , the relation is not symmetric.

Since  $(1, 1) \in R$  (also  $(4, 4) \in R$ ) the relation is not asymmetric.

It is antisymmetric because when  $a \neq b$ , we have either  $a \not R b$  or  $b \not R a$  e.g.  $(1, 1) \in R$ .

$$M_R = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 \\ 3 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 1 \end{bmatrix}$$

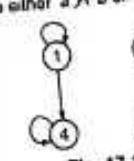


Fig. 17.15

**Example 9 :** Let  $A = \{1, 2, 3, 4\}$  and  $R = \{(1, 2), (1, 3), (2, 3), (3, 4)\}$ .

State the nature of the relation. Give its matrix and digraph.

**Sol. :** Because  $(1, 2) \in R$  but  $(2, 1) \notin R$  the relation is not symmetric.

It is asymmetric because whenever  $a R b$ , we have  $b \not R a$ .

It is antisymmetric because whenever  $a \neq b$  we have  $a \not R b$  or  $b \not R a$ .

$$M_R = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 & 0 \end{bmatrix}$$

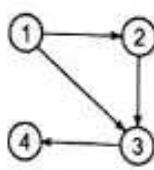


Fig. 17.16

**Example 10 :** Determine whether the following relations are (i) symmetric, (ii) asymmetric, (iii) antisymmetric.

$$(a) \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad (b) \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (\text{M.U. 2012})$$

**Sol. :** (a) We draw the digraph of the relation. [ Fig. 17.17 (a) ]

We see from the digraph whenever  $a R b$ , we have  $b R a$ .  $\therefore R$  is symmetric.  
In the matrix non-diagonal elements are symmetric.

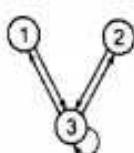


Fig. 17.17 (a)

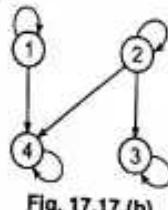


Fig. 17.17 (b)

(b) We draw the digraph of the relation. [ Fig. 17.17 (b) ]

The relation is antisymmetric because there are only one sided arrows.

**Example 11 :** Let  $A$  be a set of real numbers. Let  $R$  be the relation on  $A$  such that  $a R b$  if and only if  $a \leq b + 1$ .

Check  $R$  for (i) reflexivity, (ii) symmetry, (iii) antisymmetry, (iv) asymmetry and (v) transitivity.

**Sol. :** (i) Since  $a \leq a + 1$  for every  $a$ ,  $a R a$  i.e.  $a$  is related to  $a$ .  
Hence, the relation  $R$  is reflexive.

(ii) If  $a$  and  $b$  are any two numbers such that  $a \leq b + 1$ , we need not have  $b \leq a + 1$ .  
e.g.  $4 \leq 10 + 1$  but  $10 \not\leq 4 + 1$ . Hence,  $R$  is not symmetric.

(iii) If  $a \leq b + 1$ ,  $b \leq c + 1$  clearly  $a \leq c + 1$ .  
Hence, if  $a R b$ , and  $b R c$ , then  $a R c$ .

$\therefore R$  is transitive.

[ See next § 11, page 17-14 ]

(i) Since  $2 \leq 3 + 1$  and  $3 \leq 2 + 1$ , we have  $a R b$  and  $b R a$  for  $a = 2, b = 3$ .

$\therefore R$  is not asymmetric.

(ii) Since  $a R b$  and  $b R a$  does not imply  $a = b$ ,  $R$  is not antisymmetric.

(iii) Since  $2 \leq 3 + 1$ ,  $3 \leq 2 + 1$ , but  $2 \neq 3$ .

Note ...

We note here that 'reflexivity' must be satisfied for all elements. Similarly, 'irreflexivity' must be satisfied for all elements. But the property of symmetry, asymmetry and antisymmetry need not be satisfied for all elements. It is enough that the property is satisfied even by one element. For symmetry whenever  $a R b$ , then we must have  $b R a$  not necessarily for all  $a$  and  $b$ . For asymmetry, we have whenever  $a R b$ , then we must have  $b \not R a$ , not necessarily for all  $a$  and  $b$ . For antisymmetry, we must have if  $a R b$  and  $b R a$ , then  $a = b$  not necessarily for all  $a, b$ . Because of this nature, we can have a relation which is symmetric, and also asymmetric simultaneously. Consider the following example.

**Example 12 :** Let  $A = \{1, 2, 3\}$  and consider the relation  $\{(1, 2), (1, 3), (2, 1)\}$ .

**Sol. :** The relation is

(i) Symmetric because  $1 R 2$  and  $2 R 1$ .

(ii) Asymmetric because  $1 R 3$  and  $3 \not R 1$ .

## 11. Transitive Relations

**Definition :** A relation  $R$  on set  $A$  is called transitive if whenever  $a R b$  and  $b R c$  then  $a R c$ . A relation is not transitive if we can find  $a, b, c$  such that  $a R b$ , and  $b R c$  and still  $a \not R c$ . A relation  $R$  is transitive if and only if its matrix  $M_R$  is such that if  $[m_{ij}] = 1$  and  $[m_{jk}] = 1$  then  $[m_{ik}] = 1$ .

In the digraph of a transitive relation the edges form at least one triangle. (See the triangle in the Fig. of Ex. 4 on the next page).

The three types of relations viz. reflexive, symmetric and transitive are shown in the following Fig. 17.18.

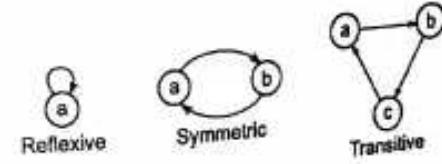


Fig. 17.18

**Example 1 :** Let  $A$  be the set of all integers and let  $R$  be the "less than" relation. (M.U. 2008, 09)

We know that if  $a < b$  and  $b < c$  then  $a < c$  i.e. if  $a R b$  and  $b R c$  then  $a R c$ .  
Hence,  $R$  is transitive.

**Example 2 :** Let  $A = \mathbb{Z}$ , the set of all positive integers and let  
 $R = \{(a, b) \in A \times A \mid a \text{ divides } b\}$

We know that if  $a$  divides  $b$  and  $b$  divides  $c$  then  $a$  divides  $c$  i.e. if  $a R b$  and  $b R c$  then  $a R c$ . Hence,  $R$  is transitive on  $A$ .

**Example 3:** Let  $A = \{1, 2, 3, 4\}$  and let  $R = \{(1, 2), (2, 3), (4, 2)\}$ . We do not have  $a, b, c$  such that  $a R b$ ,  $b R c$  and  $a R c$ . (The pair  $(1, 3)$  is absent.)

Hence,  $R$  is not transitive.

**Example 4:** Which of the following relations are transitive?

- (a)  $R_1 = \{(1, 2), (2, 3), (1, 3)\}$
- (b)  $R_2 = \{(1, 2)\}$
- (c)  $R_3 = \{(1, 2), (2, 1), (1, 1), (3, 2), (3, 3), (2, 3)\}$

Also write adjacency matrix for  $R_1$  and draw its digraph.

Sol.: (a) In  $R_1$  we have  $(1, 2), (2, 3), (1, 3)$ .

Hence,  $R_1$  is transitive. Its adjacency matrix and digraph are :

$$\begin{matrix} & 1 & 2 & 3 \\ 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 \end{matrix}$$

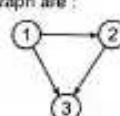


Fig. 17.19

(b)  $R_2$  is transitive by default.

(c) In  $R_3$ , we have  $(1, 2) \in R$  and  $(2, 3) \in R$  but  $(1, 3) \notin R$ . Hence,  $R_3$  is not transitive.

**Example 5:** In the set of natural numbers, prove that the relation  $x R y$  if and only if  $x^2 - 4xy + 3y^2 = 0$ , is reflexive, but neither symmetric nor transitive.

Sol.: (i)  $x R x$  because  $x^2 - 4x \cdot x + 3x^2 = 0$ .

∴  $R$  is reflexive.

(ii) If  $x R y$  then  $x^2 - 4xy + 3y^2 = 0$

∴  $(x-y)(x-3y) = 0$  ∴  $x = 3y$  as  $x$  and  $y$  are distinct.

For  $y R x$ , we must have  $y^2 - 4xy + 3x^2 = 0$

∴  $(y-x)(y-3x) = 0$  ∴  $y = x$  which is impossible; if  $x = 3y$ .

∴  $R$  is not symmetric.

(iii) If  $x, y, z$  are distinct then  $x R y$  means  $x = 3y$  (as seen above) and  $y R z$  means  $y = 3z$ .

∴  $x = 9z$ .

But for  $x R z$  we must have  $x = 3z$  which is impossible, if  $x = 9z$ .

∴  $R$  is not transitive.

∴  $R$  is reflexive but neither symmetric, nor transitive.

**Example 6:** Let  $A = \{1, 2, 3, 4\}$  and  $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 3), (3, 4), (4, 4)\}$ . Determine whether the relation is reflexive, symmetric, and transitive.

Sol.: (i) Since  $(1, 1), (2, 2), (3, 3), (4, 4) \in R$ ,  $R$  is reflexive.

(ii) Since when  $(1, 2) \in R$ , we have  $(2, 1) \in R$ , when  $(3, 4) \in R$ , we have  $(4, 3) \in R$ ,  $R$  is symmetric.

(iii) Since we have  $(1, 2), (2, 1)$ , then  $(1, 1); (3, 4), (4, 3)$ , then  $(3, 3)$ ,  $R$  is transitive.

**Example 7:** Let  $A = \{1, 2, 3, 4\}$  and  $R = \{(1, 1), (1, 2), (1, 3), (3, 1), (3, 3), (4, 4)\}$ . Determine whether the relation is reflexive, symmetric and transitive.

(M.U. 2011)

∴ (i) Since  $(1, 1), (3, 3)$ , and  $(4, 4)$  but  $(2, 2) \notin R, 2 \notin R$ , and the relation is not reflexive. We do not have  $a R a$  for all  $a$ .

(ii) Since  $(1, 2) \in R$  but  $(2, 1) \notin R$ ,  $R$  is not symmetric.

(iii) Since  $(3, 1) \in R$  and  $(1, 2) \in R$  but  $(3, 2) \notin R$ ,  $R$  is not transitive.

**Example 8:** Show by an example or otherwise that if a relation  $R$  on a set  $A$  is transitive and reflexive, then it is asymmetric.

(M.U. 2001, 08, 10, 14)

sol.: Let  $A = \{a, b, c\}$  and  $R = \{(a, b), (b, c), (a, c), (b, a), (c, b), (c, a)\}$  i.e., assume  $R$  to be reflexive, irreflexive and symmetric.

Now, since  $b R c$  and  $c R b$  by transitivity, we get  $b R b$ .

But this is against our assumption because our relation  $R$  is irreflexive.

Hence, our assumption is wrong.

Hence, if a relation is transitive and irreflexive, then it is not symmetric.

**Example 9:** Give examples of relations  $R$  on  $A = \{1, 2, 3\}$  having the following properties.

- (i)  $R$  is transitive but not symmetric.
- (ii)  $R$  is symmetric but not transitive.
- (iii)  $R$  is both symmetric and antisymmetric.
- (iv)  $R$  is neither symmetric nor antisymmetric.

sol.: (i)  $R = \{(1, 2), (2, 3), (1, 3)\}$

Since  $1 R 2, 2 R 3$  and  $1 R 3$ ,  $R$  is transitive but  $(2, 1), (3, 2), (3, 1)$  do not belong to  $R$ .

Therefore,  $R$  is not symmetric.

(ii)  $R = \{(1, 2), (2, 1), (1, 3), (3, 1)\}$

Since  $1 R 2$  and  $2 R 1$  but  $1 \notin 1, 1 R 3$  and  $3 R 1$  but  $1 \notin 1$ , the relation is symmetric but not transitive.

(iii)  $R = \{(2, 3), (3, 2), (2, 2)\}$

Since  $2 R 3$  and  $3 R 2$ ,  $R$  is symmetric. Since  $2 R 3, 3 R 2$ , and  $2 R 2$ ,  $R$  is antisymmetric.

(iv)  $R = \{(1, 2), (2, 3), (3, 2)\}$

Since  $1 R 2$  but  $2 \notin 1$ , it is not symmetric.

Since  $2 R 3$  and  $3 R 2$  but  $2 \notin 3$ , it is not antisymmetric.

**Example 10:** Given  $A = \{1, 2, 3, 4\}$ , determine whether the following relations are symmetric, reflexive, transitive and antisymmetric.

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

(M.U. 2003)

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

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

sol.: (i) Consider  $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$

Since  $1 R 1, 2 R 2, 3 R 3, 4 R 4$ ,  $R$  is reflexive.

Since  $1 R 2$  and  $2 R 1$ ,  $R$  is symmetric.

Since  $1 R 2, 2 R 1$  and  $1 R 1$ ,  $R$  is antisymmetric.

- (i) Consider  $R = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$ ,  $R$  is only reflexive.  
(ii) Consider  $R = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)\}$   
Since  $a \neq a$  for all  $a$ ,  $R$  is not reflexive.  
Since  $2 R 3$  but  $3 \neq 2$ ,  $R$  is not symmetric.  
Since  $1 R 3$  and  $3 R 1$  but  $1 \neq 1$ ,  $R$  is not antisymmetric.

**Example 11 :** Let  $A = \{a, b, c, d\}$ . Define on  $A$  a relation that is  
(i) reflexive, symmetric and transitive.  
(ii) symmetric and transitive.

Sol. : (i) Reflexive, symmetric and transitive (M.U. 2007)  
 $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a), (a, c), (c, a), (a, d), (d, a), (b, c), (c, b), (b, d), (d, b), (c, d), (d, c)\}$

- (ii) Symmetric and transitive  
 $R = \{(a, b), (b, c), (a, c), (c, d), (a, d)\}$

**Example 12 :** Does there exist a relation that is both symmetric and antisymmetric?

Sol. : Consider  $A = \{a, b\}$  and  $R = \{(a, b), (b, a), (a, a)\}$  (M.U. 1999, 2001)  
Since  $a R b$  and  $b R a$ ,  $R$  is symmetric.  
Since  $a R b$ ,  $b R a$  and  $a R a$ ,  $R$  is antisymmetric.

#### An Important Note

It should be carefully noted that for a reflexive relation, reflexivity must be observed by all elements (i.e.  $a R a$  for all  $a$ ); so also for an irreflexive relation, irreflexivity must be observed by all elements (i.e.  $a \neq a$  for all  $a$ ). Hence, a relation is either reflexive or irreflexive or neither but it cannot be both reflexive and irreflexive simultaneously. On the other hand a relation can be symmetric or antisymmetric or asymmetric or transitive if there is even only one pair (or a triplet) satisfying the conditions. Also a relation is not symmetric or antisymmetric, or a symmetric or transitive if there is one pair (or a triplet) which does not satisfy the conditions.

## 12. Equivalence Relations

**Definition :** A relation  $R$  on a set  $A$  is called equivalence relation if it is reflexive, symmetric and transitive.

**Example 1 :** Let  $A$  be the set of all triangles and  $R$  be the relation "... is congruent to ...". Prove that  $R$  is an equivalence relation.

Sol. : If  $a, b, c$  are three triangles in  $A$  then it is easy to see that

- (i)  $a R a$  (a triangle  $a$  is congruent to itself)  $\therefore R$  reflexive.  
(ii) If  $a R b$  then  $b R a$  (if a triangle  $a$  is congruent to  $b$ , then the triangle  $b$  is congruent to  $a$ )  $\therefore R$  is symmetric.

- (iii) If  $a R b$  and  $b R c$  then  $a R c$  (if a triangle  $a$  is congruent to  $b$  and  $b$  is congruent to  $c$  then  $a$  is congruent to  $c$ )  $\therefore R$  is transitive.

Hence the relation  $R$  "... is congruent to ..." is an equivalence relation.

**Example 2 :** Let  $A = \{1, 2, 3, 4\}$  and  $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (2, 1), (1, 2), (2, 3), (3, 2), (3, 1), (1, 3)\}$

Prove that  $R$  is an equivalence relation. Also find its matrix and draw its digraph.

- Sol. (i) : Since  $1 R 1, 2 R 2, 3 R 3, 4 R 4$ ,  $a R a$  for all  $a \in A$ .  
 $\therefore R$  is reflexive.  
(ii) Since when  $2 R 3$  we have  $3 R 2, 3 R 4$  and  $4 R 3$ .  
 $\therefore$  If  $a R b$  then  $b R a$ .  $\therefore R$  is symmetric.  
(iii) Since  $2 R 3$  and  $3 R 1$ , we have  $2 R 1$ . Also when  $3 R 1$  and  $1 R 2$ , we have  $3 R 2$ .  
 $\therefore$  If  $a R b$  and  $b R c$  then  $a R c$ .  $\therefore R$  is transitive.  
 $\therefore R$  is an equivalence relations.

1	2	3	4
1	1	1	0
2	1	1	1
3	1	1	1
4	0	0	1

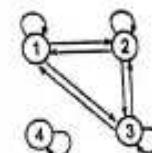


Fig. 17.20

It is easy to see that the relation  $R$  is an equivalence relation.

#### Note ....

The matrix of an equivalence relation  $M_R$  has the following properties.

- (i) All elements in the leading diagonal are unity.  
(ii) The elements 0, 1 are symmetric with respect to the leading diagonal.

The digraph of an equivalence relation has the following properties.  
(i) All vertices have loops around them.  
(ii) Vertices if connected then they are connected both ways. (Two way traffic or not traffic).

- (iii) Edges of at least three vertices form a triangle by double lines.

**Example 3 :** Let  $A = \mathbb{Z}$ , the set of all integers and let the relation be defined as  $a R b$  if  $a \leq b$ . (M.U. 2008, 09)

Prove that  $R$  is not an equivalence relation.

Sol. : It is easy to see that  $R$  is reflexive because  $a \leq a$ .

But if  $a$  and  $b$  are distinct and if  $a \leq b$  it is not true that  $b \leq a$ . Hence,  $R$  is not symmetric (e.g.  $3 \leq 5$  but  $5 \leq 3$ ).

It may be noted that if  $a \leq b$  and  $b \leq c$  then  $a \leq c$  i.e.  $R$  is transitive.  
 $\therefore R$  is not an equivalence relation.

**Example 4 :** Suppose that  $A$  is a non-empty set and  $f$  is a function that has  $A$  as its domain. Let  $R$  be the relation on  $A$  consisting of all ordered pairs  $(x, y)$  where  $f(x) = f(y)$ . (M.U. 2010)

Show that  $R$  is an equivalence relation.

Sol. : (i) Since  $f(x) = f(x)$  for every  $x$ ,  $R$  is reflexive.

- (ii) If  $f(x) = f(y)$ , then  $f(y) = f(x)$ .  
 $\therefore R$  is symmetric.

- (iii) If  $f(x) = f(y)$  and  $f(y) = f(z)$ , then  $f(x) = f(z)$ .  
 $\therefore R$  is transitive.  $\therefore R$  is an equivalence relation.

**Example 5:** Let  $S = \{1, 2, 3, 4\}$  and  $A = S \times S$ . Define the following relation.

$R$  on  $A$ :  $(a, b) R (a', b')$  if and only if  $a + b = a' + b'$

Show that  $R$  is an equivalence relation.

**Sol.:** (i)  $(a, b) R (a, b)$  because  $a + b = a + b$ . (M.U. 2013)

$\therefore R$  is reflexive.

(ii) If  $(a, b) R (a', b')$ , then  $a + b = a' + b'$

Hence,  $a' + b' = a + b \therefore (a', b') R (a, b)$

$\therefore R$  is symmetric.

(iii) Let  $(a, b) R (a', b')$  and  $(a', b') R (a'', b'')$

Then  $a + b = a' + b'$  and  $a' + b' = a'' + b''$

$\therefore a + b = a'' + b'' \therefore (a, b) R (a'', b'')$

$\therefore R$  is transitive.

Hence,  $R$  is an equivalence relation.

**Example 6:** Let  $R$  be the relation on the set of real numbers such that  $a R b$  if and only if  $a - b$  is an integer.

Prove that  $R$  is an equivalence relation.

**Sol.:** (i)  $R$  is reflexive because  $a - a = 0$  is an integer. (M.U. 2006, 07, 12)

$\therefore a R a$  for all  $a$ .

(ii) If  $a R b$  i.e.,  $a - b$  is an integer then  $b R a$ , because  $b - a$  is also an integer.

$\therefore R$  is symmetric.

(iii) If  $a R b$  and  $b R c$  i.e., if  $a - b$  is an integer and  $b - c$  is an integer then  $a - c = (a - b) + (b - c)$  also is an integer.  $\therefore a R c$

$\therefore R$  is transitive.  $\therefore R$  is an equivalence relation.

### 13. Partially Ordered Sets (Posets)

#### (a) Partial Order Relation

**Definition:** A relation  $R$  on a set  $A$  is called a partial order relation if  $R$  is (i) reflexive, (ii) antisymmetric and (iii) transitive. For example, the relations  $\leq$ ,  $\geq$ ,  $\subseteq$  are partial order relations.

#### (b) Partially Ordered Set

**Definition:** The set  $A$  together with the partial order relation  $R$  is called a partially ordered set or in brief poset and is generally denoted by  $(A, R)$  or by  $(A, \leq)$  where  $A$  denotes the set and  $R$  denotes the relation.

(Why such a set is called partially ordered set is explained in Ex. 1, (bottom) page 17-21.)

**Remark:** ...

Partial order relation can be memorised by its acronym RAT (Reflexive, Antisymmetric, Transitive.)

**Example 1:** If  $S$  is any set and  $P$  is its power set (collection of subsets) then the relation  $\subseteq$  (is a subset of) is a partial order relation on  $P$ .

**Sol.:** Let  $A, B, C$  be the elements of  $P$ .

(i) Since  $A \subseteq A$ ,  $R$  is reflexive.

(ii) If  $A \subseteq B$  and  $B \subseteq A$  then  $A = B$ .

(iii)  $R$  is antisymmetric.

(iv) If  $A \subseteq B, B \subseteq C$  then  $A \subseteq C$ .

(v)  $R$  is transitive.

(vi)  $R$  is a partial order relation on  $P$ .



Fig. 17.21

**Example 2:** If  $Z^+$  is the set of positive integers then the relation  $\leq$  (less than or equal to) is a partial order relation on  $Z^+$ .

**Sol.:** Let  $a, b, c$  be any three natural numbers.

(i) Since  $a \leq a$ ,  $R$  is reflexive. e.g.  $3 \leq 3$

(ii) If  $a \leq b$  and  $b \leq a$  then  $a = b$ .

(iii)  $R$  is antisymmetric.

(iv) If  $a \leq b, b \leq c$  then  $a \leq c$ . e.g.  $2 \leq 3, 3 \leq 4 \therefore 2 \leq 4$ .

(v)  $R$  is transitive.  $\therefore R$  is a partial order relation.

**Example 3:** If  $Z^+$  is a set of positive integers then the relation  $\geq$  (greater than or equal to) is a partial order relation on  $Z^+$ .

**Sol.:** Prove it.

**Example 4:** If  $Z^+$  is a set of positive integers then the relation  $R$  of divisibility i.e.  $a R b$  if and only if  $a | b$  ( $a$  divides  $b$ ) is a partial order relation on  $Z^+$ .

**Sol.:** Prove it. Or see Ex. 1 page 17-21.

**Example 5:** Consider a set of integers  $Z$ . Let  $a R b$  if  $a = 2b$ . Examine whether  $R$  is a partial order relation.

**Sol.:** Let  $a, b, c \in Z$ .

Since, we cannot have  $a = 2a$ .  $\therefore R$  is not reflexive.

Also, if  $a = 2b$  and  $b = 2c$ ,  $a = 4c$ .  $\therefore R$  is not transitive.

$\therefore R$  is not a partial order relation.

**Example 6:** Define a relation  $R$  on the set  $Z$  by  $a R b$  if  $a - b$  is a non-negative even integer.

**Sol.:** Verify whether  $R$  is a partial order relation.

**Sol.:** Let  $a, b, c$  be three integers.

(i)  $a - a = 0$  and zero is non-negative even integer.

$\therefore a R a \therefore R$  is reflexive.

(ii) If  $a R b$  and  $b R c$  then  $(a - b)$  is non-negative even integer and  $(b - c)$  is also a non-negative even integer. This is possible only if  $a - b = 0$ .

$\therefore a = b \therefore R$  is anti-symmetric.

- (iii) Let  $a R b$  and  $b R c$ . Then  $a - b = 2n_1$ , say, and  $b - c = 2n_2$  where  $n_1$  and  $n_2$  are non-negative integers.  
 $\therefore (a - b) + (b - c) = 2n_1 + 2n_2$   
 $\therefore a - c = 2(n_1 + n_2)$   
 $\therefore (a - c)$  is an even non-negative integer  
 $\therefore a R c$        $\therefore R$  is transitive.

Since  $R$  is reflexive, antisymmetric and transitive  $R$  is partially ordered.

**Example 7:** Let  $R$  be a relation on the set of positive integers such that  $R = \{(a, b) \mid (a - b)$  is an odd positive integer}. Is  $R$  an equivalence relation, a partial order relation? (M.U. 2000)

Sol.: (i)  $a - a = 0$  and 0 is an odd positive integer.

$\therefore R$  is reflexive.

(ii) Let  $a R b$ , then  $a - b$  is an odd positive integer, say,  $a - b = 2n_1 + 1$ .  
 Then  $b - a = -2n_1 - 1$  which is negative and hence  $b \not R a$ .

$\therefore R$  is not symmetric and  $R$  is not antisymmetric.

- (iii) Let  $a R b$  and  $b R c$ .  
 $\therefore a - b = 2n_1 + 1$  and  $b - c = 2n_2 + 1$   
 $\therefore (a - b) + (b - c) = (2n_1 + 1) + (2n_2 + 1)$   
 $\therefore a - c = 2n_1 + 2n_2 + 2 = 2(n_1 + n_2 + 1)$ , even integer.  
 $\therefore a \not R c$        $\therefore R$  is not transitive.  
 $\therefore R$  is neither an equivalence relation nor a partially ordered relation.

### EXERCISE - I

Give examples of relations  $R_1$ ,  $R_2$  and  $R_3$  on  $A = \{1, 2, 3, 4\}$  with justification such that (i)  $R_1$  is reflexive but not symmetric, (ii)  $R_2$  is transitive, symmetric but not reflexive, (iii)  $R_3$  is a partial order relation.

- [Ans.: (i)  $R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (1, 3)\}$  (M.U. 2001)  
 (ii)  $R_2 = \{(2, 3), (3, 2), (2, 2), (3, 3)\}$   
 (iii)  $R_3 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (1, 4), (1, 3), (2, 4), (3, 4)\}$ ]

### (c) Comparable Elements

**Definition :** If  $A$  is given set and  $R$  is a partial order relation on  $A$  then the elements  $a, b \in A$  are said to be comparable if  $a R b$  or  $b R a$ . This means if  $a \not R b$  or  $b \not R a$  then  $a$  and  $b$  are not comparable.

For example, in a set of  $Z^+$  if  $R$  is a relation "is divisible by 3" then the elements 3 and 6 are comparable but 4 and 11 are not comparable.

**Example 1 :** If  $Z^+$  is a set of positive integers and  $R$  is a relation "a divides b" then prove that  $R$  is partial order relation. Show that  $Z^+$  is partially ordered. Find two elements which are not comparable.

Sol.: Let  $a, b, c \in Z^+$

- (i) Since 'a divides a',  $R$  is reflexive.

(M.U. 2004, 08, 11)

- (i) If  $a R b$  and  $b R a$  i.e. if  $a$  divides  $b$  and  $b$  divides  $a$  then  $b = a$ .  
 $\therefore R$  is antisymmetric.

- (ii) If  $a R b, b R c$  then  $a R c$ .  
 $\therefore R$  is transitive.       $\therefore R$  is a partial order relation on  $Z^+$ .

Now, in this set 3 and 8 are not comparable elements because 3 does not divide 8 and 8 does not divide 3. Similarly, 2 and 11 are not comparable elements. Thus, in a poset, some elements are related i.e. comparable and some elements are not related i.e. not comparable. In this sense the set is ordered but "partially".

### (d) Total Order Relations or Chains

**Definition :** If any two elements in a poset are comparable, then the partial order is called a total order or a linear order. In such a situation the relation is called simple ordering relation or linear ordering relation. The set  $A$  together with a total order relation is called totally ordered set or simply ordered set or a chain.

For example, the set  $\{2, 4, 8, 16\}$  with 'divides' as relation is a chain.

Since the most common partial order relations are  $\leq$  and  $\geq$  on  $Z$  or  $R$ , a partial order relation  $R$  is generally denoted by  $\leq$  and  $\geq$  and the poset is denoted by  $(A, \leq)$ . Just as by taking complement or intersecting of two sets we construct new sets, from posets we can construct new posets.

### 14. Hasse Diagram

The digraph of a poset can be considerably simplified as follows. For instance, since in a poset, the relation is reflexive, we drop the loops around the vertices. Since in a poset  $R$  is transitive i.e. if  $a R b$  and  $b R c$  then  $a R c$ , we drop the edge from  $a$  to  $c$ . Thus, we drop all edges implied by transitivity. Finally we arrange the whole diagram such that all arrows point upwards and then drop the arrow heads. The resulting diagram is called the Hasse diagram, named after the German mathematician Helmut Hasse who first suggested it.

**Example 1 :** Consider a set  $A = \{1, 2, 3, 4, 12\}$  and the relation of divisibility i.e.  $a R b$  if  $a$  divides  $b$  which we denote as  $a | b$ . Show that  $(A, R)$  is a poset. Also construct the digraph of the poset and its Hasse diagram. (M.U. 2008)

Sol.: Now  $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (12, 12), (1, 2), (1, 3),$

$(1, 4), (1, 12), (2, 4), (2, 12), (3, 12), (4, 12)\}$

Let  $a, b, c$  be any three elements of  $A$ .

- (i) Since  $a | a$ ,  $R$  is reflexive.

- (ii) If  $a | b$  and  $b | c$  then  $a = c$ .

$\therefore R$  is antisymmetric.

- (iii) If  $a | b$  and  $b | c$  then  $a | c$ .

$\therefore R$  is transitive.       $\therefore R$  is a partial order relation on  $A$ .

And  $(A, R)$  is a poset. The digraph of the poset is shown in Fig. 17.22.

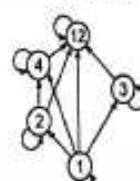


Fig. 17.22

Note ...

If  $n$  is a positive integer then we shall denote the set of all positive divisors of  $n$  by  $D_n$ . Thus, by this notation  $D_4 = \{1, 2, 4\}$ ,  $D_8 = \{1, 2, 4, 8\}$ ,  $D_{12} = \{1, 2, 3, 4, 6, 12\}$ ,  $D_{20} = \{1, 2, 4, 5, 10, 20\}$ . (See Ex. 8, page 17-27, Ex. 10, page 17-29.)

## (a) To Construct Hasse Diagram

Step 1 : Delete the loop at each vertex. The result is Fig. 17.23 (a).

Step 2 : Delete the edges implied by the transitivity. For instance, since  $1 \rightarrow 2, 2 \rightarrow 4$ , hence,  $1 \rightarrow 4$ , we delete the edge from 1 to 4. Similarly, we delete edges from 1 to 12, and from 2 to 12. The result is Fig. 17.23 (c).

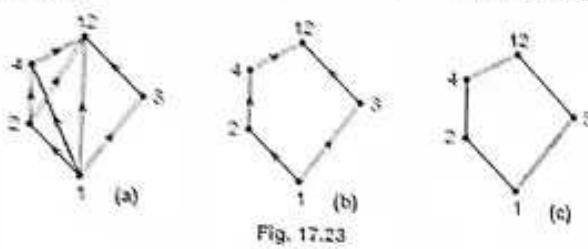


Fig. 17.23

Step 3 : Rearrange the digraph, if necessary, such that all edges go "upward". In the present diagram all the edges are pointing upwards. Hence, we need only to drop the arrow heads. The result is the Hasse diagram shown in Fig. 17.23 (c).

Such a diagram is called Hasse diagram which is defined below.

**Definition :** A Hasse diagram of a poset  $(A, R)$  is a figure in which

- the vertices represent the elements of  $A$ .
- there is an upward line from  $x$  to  $y$  whenever  $x R y$  and  $x \neq y$ .
- the figure has least number of segments that accomplish the property (ii).

**Example 2 :** Construct the digraph and the Hasse diagram for the poset  $(A, |)$  where  $A = \{1, 2, 3, 4, 6, 8\}$  and  $|$  denotes the divisibility relation.

**Sol.:** Now,  $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (6, 6), (8, 8), (1, 2), (1, 3),$

$$(1, 4), (1, 6), (1, 8), (2, 4), (2, 6), (2, 8), (3, 6), (4, 8)\}$$

Let  $a, b, c$  be any three elements of  $A$ .

(i) Since  $a | a$   $R$  is reflexive.

(ii) If  $a | b$  and  $b | a$ , then  $a = b$ .

∴  $R$  is reflexive.

(iii) If  $a | b$  and  $b | c$ , then  $a | c$ .

∴  $R$  is transitive.

∴  $R$  is a partial order relation on  $A$ .

And,  $(A, R)$  is a poset.

The digraph is shown in Fig. 17.24.

From the above digraph we shall obtain the Hasse diagram as follows.

**Step 1 :** Delete the loop at each vertex. The result is Fig. 17.25 (a).

**Step 2 :** Delete all edges that are implied by transitivity. The result is Fig. 17.25 (b).

**Step 3 :** Rearrange the diagram in such a way that all edges go "upward". For this we need to take 3 near 1 and 6 above 3, 4 above 2 and 8 above 4 and 6 as shown in the Fig. 17.26. Also drop the arrow heads. The result is the required Hasse diagram Fig. 17.26.

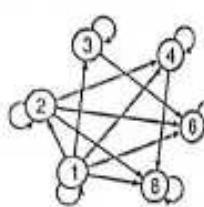


Fig. 17.24

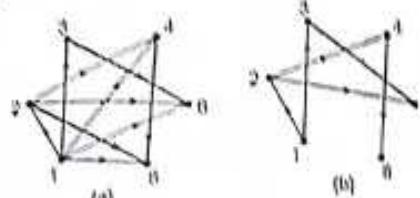


Fig. 17.25 (a)

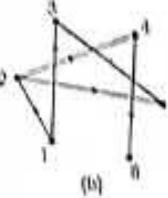


Fig. 17.25 (b)

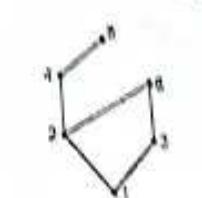


Fig. 17.26

**Example 3 :** Let  $A = \{1, 2, 3, 4\}$  and the relation be

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

Draw the digraph and then the Hasse diagram.

**Sol.:** The digraph is shown in Fig. 17.27 and Hasse diagram in Fig. 17.28.

**Example 4 :** Let  $A = \{a, b, c, d, e\}$  and the relation be

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (c, b), (c, a), (a, b), (d, b), (d, a), (d, e), (b, e)\}$$

Verify that this is a partial order relation. Draw its digraph and then Hasse diagram. Also obtain matrix  $M_R$ .

**Sol.:** (i) Since  $(a, a), (b, b), (c, c), (d, d), (e, e)$ ,

∴  $R$  is reflexive.

(ii) Since  $p R q, q R p$  implies  $p = q$

∴  $R$  is antisymmetric.

(iii) Since  $(c, b), (b, a), (c, a); (d, e), (e, a), (d, a); (d, b), (b, a), (d, a)$

∴  $R$  is transitive.

∴  $R$  is a partial order relation.

Its digraph is shown in Fig. 17.29 (a) and its Hasse diagram is shown in Fig. 17.29 (b) below.

Also the matrix  $M_R$  shows the properties of reflexivity, anti-symmetry and transitivity.

a	b	c	d	e
1	0	0	0	0
b	1	1	0	0
c	1	1	1	0
d	1	1	0	1
e	1	0	0	1

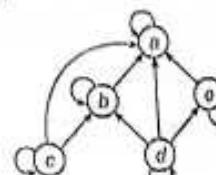


Fig. 17.29 (a)

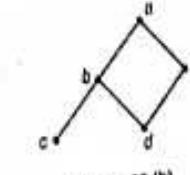


Fig. 17.29 (b)

**Example 5 :** Draw the Hasse diagram of the following sets under partial order relation "divides" and indicate those which are chains.

$$(a) \{1, 3, 9, 18\}, (b) \{3, 5, 30\}, (c) \{1, 2, 5, 10, 20\}$$

(M.U. 2000)

Sol. : (a) The partial order relation "divides" on the set {1, 3, 9, 18} is  
 $R = \{(1, 1), (1, 3), (1, 9), (1, 18), (3, 3), (3, 9), (3, 18), (9, 9), (9, 18), (18, 18)\}$

Matrix of the relation is

$$M_R = \begin{bmatrix} 1 & 3 & 9 & 18 \\ 1 & 1 & 1 & 1 \\ 3 & 0 & 1 & 1 & 1 \\ 9 & 0 & 0 & 1 & 1 \\ 18 & 0 & 0 & 0 & 1 \end{bmatrix}$$

We first find the digraph [Fig. 17.30 (a)].

Step 1 : Delete all the loops [Fig. 17.30 (b)].

Step 2 : Delete the edges that are implied by transitivity. Delete the edges from 1 to 9, 1 to 18 and 3 to 18 [Fig. 17.30 (c)].

Step 3 : Drop the arrow heads [Fig. 17.30 (d)]. The result is the Hasse diagram [Fig. 17.30 (e)]. This is a chain. See the definition (d), page 17-22.

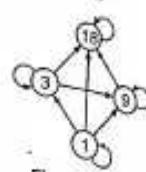
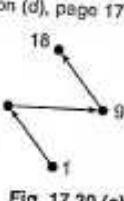
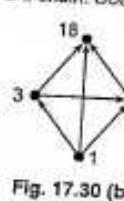


Fig. 17.30 (a)

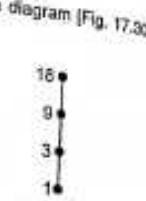
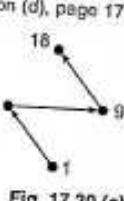


Fig. 17.30 (a)

Note ...

Note that the matrix of the relation  $M_R$  is upper triangular and its Hasse diagram is a chain.

(b) The partial order relation "divides" on the set {3, 5, 30} is  
 $R = \{(3, 3), (3, 30), (5, 5), (5, 30), (30, 30)\}$

Matrix of the relation is

$$M_R = \begin{bmatrix} 3 & 5 & 30 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 30 & 0 & 1 \end{bmatrix}$$

We first find the digraph [Fig. 17.31 (a)].

Step 1 : Delete all the loops [Fig. 17.31 (b)].

Step 2 : Delete all the edges implied by transitivity. There is none such edge.

Step 3 : Drop the arrow heads [Fig. 17.31 (c)]. The result is Hasse diagram [Fig. 17.31 (c)]. The poset is not a chain because  $3 \nmid 5$ . See the definition (d), page 17-22.

(c) The partial order relation "divides" on the set {1, 2, 5, 10, 20} is  
 $R = \{(1, 1), (1, 2), (1, 5), (1, 10), (1, 20), (2, 2), (2, 10), (2, 20), (5, 5), (5, 10), (5, 20), (10, 10), (10, 20), (20, 20)\}$

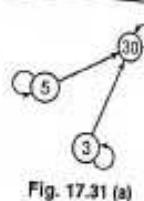


Fig. 17.31 (a)

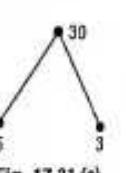


Fig. 17.31 (b)



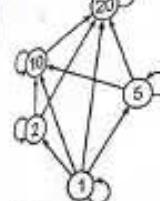
Fig. 17.31 (c)

The matrix of the relation is

$$M_R = \begin{bmatrix} 1 & 2 & 5 & 10 & 20 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 & 1 & 1 \\ 5 & 0 & 0 & 1 & 1 & 1 \\ 10 & 0 & 0 & 0 & 1 & 1 \\ 20 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

We first find the digraph [Fig. 17.32 (a)].

(a)



Step 1 : Delete all the loops [Fig. 17.32 (b)].

(b)

Fig. 17.32 (b)

Step 2 : Delete all the edges implied by transitivity. Delete the edges from 1 to 10, from 1 to 20 and from 5 to 20 [Fig. 17.32 (c)].

(c)

Fig. 17.32 (c)

Step 3 : Drop the arrow heads. The result is the Hasse diagram [Fig. 17.32 (d)]. The poset is not a chain because  $2 \nmid 5$ . See the definition (d), page 17-22.

(d)

Fig. 17.32 (d)

Example 6 : Draw two Hasse diagrams of posets with three elements. (M.U. 2009)

Sol. : Let  $A = \{1, 2, 3\}$ .

Let  $R_1 = (A, \leq)$  and  $R_2 = (A, \geq)$ .

Then both  $R_1$  and  $R_2$  are reflexive, antisymmetric and transitive.

(See Ex. 2 and 3, page 17-20)

Hence,  $R_1$  and  $R_2$  both are posets.

Their Hasse diagrams are shown in Fig. 17.33 (a) and (b).

Fig. 17.33

Example 7 : Determine the Hasse diagram of the relation on  $A = \{1, 2, 3, 4, 5\}$  whose matrix is shown below.

$$(a) M_R = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 1 & 1 \\ 3 & 0 & 0 & 1 & 1 \\ 4 & 0 & 0 & 0 & 1 & 1 \\ 5 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$(b) M_R = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 2 & 0 & 1 & 1 & 1 & 1 \\ 3 & 0 & 0 & 1 & 1 & 1 \\ 4 & 0 & 0 & 0 & 1 & 0 \\ 5 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(M.U. 2000, 08)

(M.U. 2011)

**Applied Mathematics - IV**

(17-27)

**Equivalence Relations & Posets**

(a)

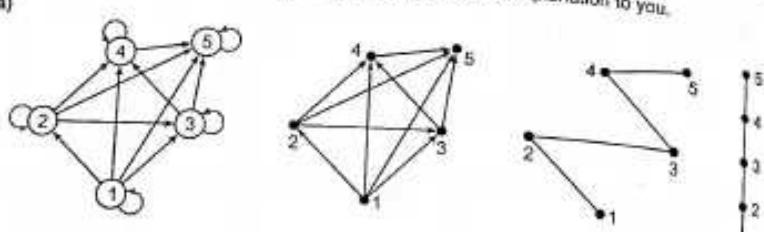


Fig. 17.34

(b)

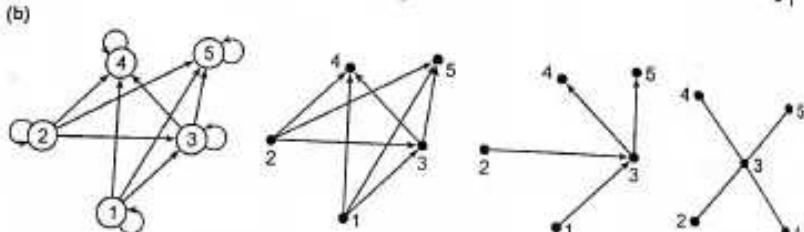


Fig. 17.35

**Example 8 :** Determine the matrix of the partial order relation of "divisibility" on the following set  $S$ . Draw the Hasse diagram of the poset. Indicate those which are chains.

- $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ .
- $B = \{3, 6, 12, 36, 72\}$
- $C = \{2, 4, 8, 16, 32\}$

(M.U. 2003)

**Sol. :** (a) We show below the matrix of the relation and the diagrams involved in the process of finding the Hasse diagram leaving the explanation to you.

$$M_R = \begin{bmatrix} 1 & 2 & 3 & 5 & 6 & 10 & 15 & 30 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 3 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 5 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 6 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 10 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 15 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

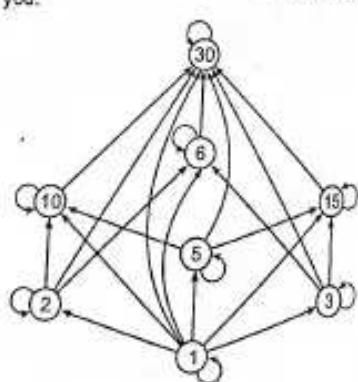


Fig. 17.36 (a)

**Applied Mathematics - IV**

(17-28)

**Equivalence Relations & Posets**

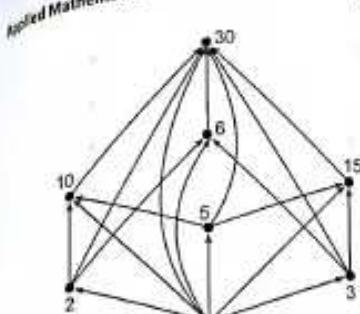


Fig. 17.36 (b)

The poset not a chain.

$$(b) M_R = \begin{bmatrix} 3 & 6 & 12 & 36 & 72 \\ 3 & 1 & 1 & 1 & 1 \\ 6 & 0 & 1 & 1 & 1 \\ 12 & 0 & 0 & 1 & 1 \\ 36 & 0 & 0 & 0 & 1 \\ 72 & 0 & 0 & 0 & 0 \end{bmatrix}$$

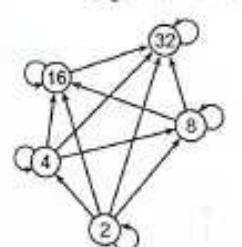


Fig. 17.36 (c)

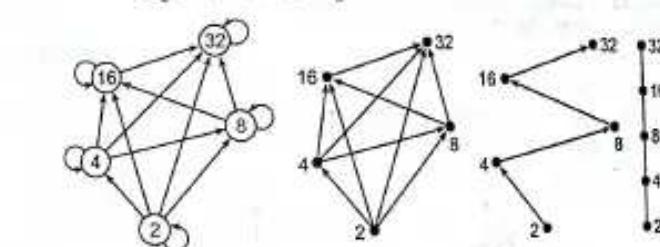
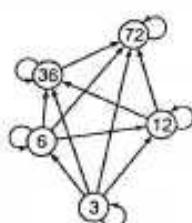


Fig. 17.37

The poset is a chain.

$$(c) M_R = \begin{bmatrix} 2 & 4 & 8 & 16 & 32 \\ 2 & 1 & 1 & 1 & 1 \\ 4 & 0 & 1 & 1 & 1 \\ 8 & 0 & 0 & 1 & 1 \\ 16 & 0 & 0 & 0 & 1 \\ 32 & 0 & 0 & 0 & 0 \end{bmatrix}$$



The poset is a chain.

**Example 9:** Let  $A = \{a, b, c, d, e\}$  and let

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, c), (c, d), (d, e), (a, c), (a, d), (a, e), (b, d), (b, e), (c, e)\}$$

Draw the Hasse diagram.

**Sol.:** The Hasse diagram is as shown in adjoining figure.

Note that the elements are linearly ordered as every pair of  $A$  is comparable.

Note that the Hasse diagram of a finitely linearly ordered set is always of the form of this diagram which looks like a chain. Hence, the finitely linearly ordered set is called a chain.

**Example 10:** Draw the Hasse diagram of the following sets under the partial order relation 'divides' and indicate those which are chains.

$$(a) A = \{2, 4, 12, 24\}, \quad (b) B = \{1, 3, 5, 15, 30\}$$

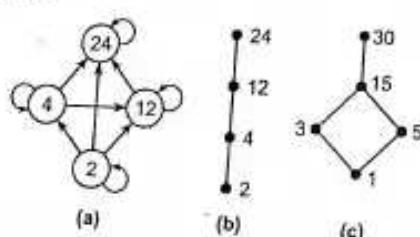
**Sol.:** We leave it to you to write  $R$  and the matrix.

(M.U. 1998, 2016)

The digraph of the poset is shown in Fig. 17.39 (a).

The Hasse diagram is shown in the Fig. 17.39 (b).

$\therefore$  The poset is a chain.



(b) We leave it to you.

The Hasse diagram is shown in the Fig. 17.39 (c).

**Example 11:** Let  $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$  and  $R$  be the relation 'is divisible by'. Obtain the relation matrix and draw the Hasse diagram.

**Sol.:** The relation matrix and the Hasse diagram are shown in Fig. 17.40.

Fig. 17.38

### Equivalence Relations & Posets

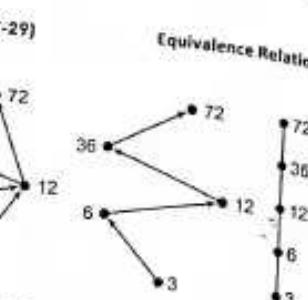


Fig. 17.39

Fig. 17.30

### Applied Mathematics - IV

	1	2	3	5	6	10	15	30
1	1	1	1	1	1	1	1	1
2	0	1	0	0	1	1	0	1
3	0	0	1	0	1	0	1	1
5	0	0	0	1	0	1	1	1
6	0	0	0	0	1	0	0	1
10	0	0	0	0	0	1	0	1
15	0	0	0	0	0	0	1	1
30	0	0	0	0	0	0	0	1

### Equivalence Relations & Posets

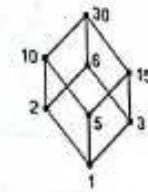


Fig. 17.40

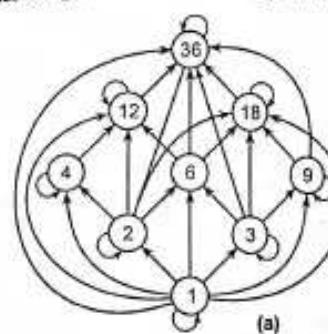
(M.U. 2006, 09)

**Example 12:** Draw the Hasse diagram of  $D_{36}$ .

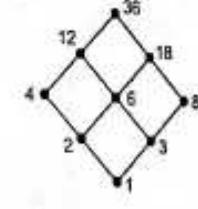
**Sol.:** We have  $A = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

The digraph is shown in the Fig. 17.41 (a).

The Hasse diagram is shown in the Fig. 17.41 (b).



(a)



(b)

Fig. 17.41

**Example 13:** Draw the Hasse diagram for the following set.

$$\{(a, b) \mid a \text{ divides } b\} \text{ on } \{1, 2, 3, 4, 6, 8, 12\}$$

**Sol.:** The matrix of the relation is

	1	2	3	4	6	8	12
1	1	1	1	1	1	1	1
2	0	1	0	1	1	1	1
3	0	0	1	0	1	0	1
4	0	0	0	1	0	1	1
6	0	0	0	0	1	0	1
8	0	0	0	0	0	1	0
12	0	0	0	0	0	0	1

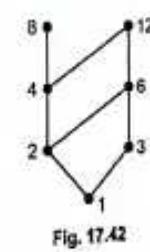


Fig. 17.42

The Hasse diagram is shown in Fig. 17.42.

(M.U. 2002)

**Example 14 :** (a) Let  $A = \{1, 2, 3, 4\}$  and  $R$  be the relation is 'less than or equal to'. (b) Let  $B = \{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}\}$  and  $R$  be the relation  $\subseteq$ . Draw the Hasse diagrams. Show that the sets are chains.

Sol. : The Hasse diagrams are as shown in Fig. 17.43 (a) and 17.43 (b).

Note ....

The sets  $A$  and  $B$  given above are totally ordered.

**Example 15 :** Determine the matrix of the partial order relation of divisibility on the set  $A$ . Draw Hasse diagrams of the posets. Indicate those which are chains.

- (a)  $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$
- (b)  $B = \{3, 6, 12, 36, 72\}$
- (c)  $C = \{2, 4, 8, 16, 32\}$

Sol. : (a)  $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$

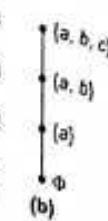


Fig. 17.43

$$R = \{(1, 1), (1, 2), (1, 3), (1, 5), (1, 6), (1, 10), (1, 15), (1, 30), (2, 2), (2, 6), (2, 10), (2, 30), (3, 3), (3, 6), (3, 15), (3, 30), (5, 5), (5, 10), (5, 15), (5, 30), (6, 6), (6, 30), (10, 10), (10, 15), (15, 15), (15, 30), (30, 30)\}$$

Sol. : The matrix of the relation is

$$M = \begin{bmatrix} 1 & 2 & 3 & 5 & 6 & 10 & 15 & 30 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 3 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 5 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 6 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 10 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 15 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

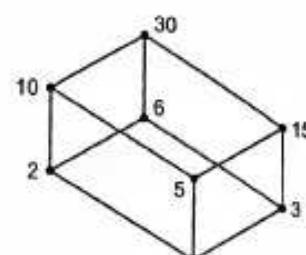


Fig. 17.44

The Hasse diagram is shown in Fig. 17.44.

(b) Consider,  $B = \{3, 6, 12, 36, 72\}$

$$R = \{(3, 3), (3, 6), (3, 12), (3, 36), (3, 72), (6, 6), (6, 12), (6, 36), (6, 72), (12, 12), (12, 36), (12, 72), (36, 36), (36, 72), (72, 72)\}$$

The matrix of the relation is

$$M = \begin{bmatrix} 3 & 6 & 12 & 36 & 72 \\ 3 & 1 & 1 & 1 & 1 \\ 6 & 0 & 1 & 1 & 1 \\ 12 & 0 & 0 & 1 & 1 \\ 36 & 0 & 0 & 0 & 1 \\ 72 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

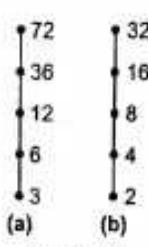


Fig. 17.45

The Hasse diagram is shown in Fig. 17.45 (a).

### Equivalence Relations & Posets

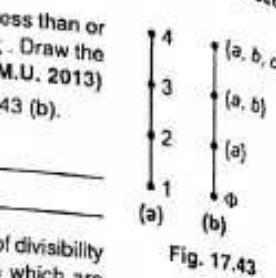


Fig. 17.43

### Applied Mathematics - IV

Consider,  $C = \{2, 4, 8, 16, 32\}$

$$R = \{(2, 2), (2, 4), (2, 8), (2, 16), (2, 32), (4, 4), (4, 8), (4, 16), (4, 32), (8, 8), (8, 16), (8, 32), (16, 16), (16, 32), (32, 32)\}$$

The matrix of the relation is

$$M = \begin{bmatrix} 2 & 4 & 8 & 16 & 32 \\ 2 & 1 & 1 & 1 & 1 \\ 4 & 0 & 1 & 1 & 1 \\ 8 & 0 & 0 & 1 & 1 \\ 16 & 0 & 0 & 0 & 1 \\ 32 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The last two are chains.

The Hasse diagram is shown in Fig. 17.45 (b).

**Example 16 :** Let  $A = \{a, b, c\}$ . Show that  $(P(A), \subseteq)$  is a poset and draw its Hasse diagram.

(M.U. 2013, 15)

Sol. : When  $A = \{a, b, c\}$

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

(i) For  $P(A)$ , set inclusion  $\subseteq$  relation  $R$  is reflexive because for every  $B \in P(A)$ ,

$$\therefore B \subseteq B$$

(ii) If  $B \subseteq C$  and  $C \subseteq B$ , then  $B = C$ .

$$\therefore R$$
 is antisymmetric.

(iii) If  $B \subseteq C$  and  $C \subseteq D$ , then  $B \subseteq D$ .

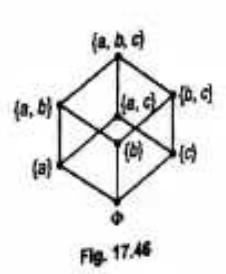
$$\therefore R$$
 is transitive.  $\therefore R$  is a poset.

(b) The partial order relation  $\subseteq$  is given below

$$R = \{(\{\emptyset\}, \{\emptyset\}), (\{\emptyset\}, \{a\}), (\{\emptyset\}, \{b\}), (\{\emptyset\}, \{c\}), (\{\emptyset\}, \{a, b\}), (\{\emptyset\}, \{a, c\}), (\{\emptyset\}, \{b, c\}), (\{\emptyset\}, \{a, b, c\}), (\{\{a\}\}, \{\{a\}\}), (\{\{a\}\}, \{b\}), (\{\{a\}\}, \{c\}), (\{\{a\}\}, \{a, b\}), (\{\{a\}\}, \{a, c\}), (\{\{a\}\}, \{b, c\}), (\{\{a\}\}, \{a, b, c\}), (\{\{b\}\}, \{\{b\}\}), (\{\{b\}\}, \{a\}), (\{\{b\}\}, \{c\}), (\{\{b\}\}, \{a, c\}), (\{\{c\}\}, \{\{c\}\}), (\{\{c\}\}, \{a\}), (\{\{c\}\}, \{b\}), (\{\{c\}\}, \{a, b\}), (\{\{a, b\}\}, \{\{a, b\}\}), (\{\{a, b\}\}, \{c\}), (\{\{a, b\}\}, \{a, c\}), (\{\{a, b\}\}, \{b, c\}), (\{\{a, b\}\}, \{a, b, c\}), (\{\{a, c\}\}, \{\{a, c\}\}), (\{\{a, c\}\}, \{b\}), (\{\{a, c\}\}, \{a, b\}), (\{\{a, c\}\}, \{a, b, c\}), (\{\{b, c\}\}, \{\{b, c\}\}), (\{\{b, c\}\}, \{a\}), (\{\{b, c\}\}, \{a, b\}), (\{\{b, c\}\}, \{a, c\}), (\{\{a, b, c\}\}, \{\{a, b, c\}\})\}$$

(c) The Matrix of the above relation is

$$M_R = \begin{bmatrix} \emptyset & \{a\} & \{b\} & \{c\} & \{a, b\} & \{b, c\} & \{a, c\} & \{a, b, c\} \\ \emptyset & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \{a\} & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ \{b\} & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ \{c\} & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ \{a, b\} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \{b, c\} & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \{a, c\} & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \{a, b, c\} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$



(d) The Hasse diagram is shown in Fig. 17.46.

## (b) To Find the Relation From a Hasse Diagram

To solve the converse of the above problem i.e. to find the relation from the Hasse diagram we reverse the above steps.

- Put a loop at each vertex of the given Hasse diagram.
- Join the vertices which are connected through intermediate points.
- Put upward arrows for all segments.
- The vertices connected as above are related.
- Write the relation set.

**Example 1 :** Find the relation set  $R$  for the Hasse diagram shown in Fig. 17.47.

Sol. : 1. Put a loop at each vertex.

2. Since  $a$  is connected to  $c$  and  $c$  is connected to  $d$ , join  $a$  to  $d$ . Since  $b$  is connected to  $c$  and  $c$  is connected to  $e$ , join  $b$  to  $e$ . Similarly, join  $a$  to  $e$  and  $b$  to  $d$ . (Do not connect  $ad$ . Why? For the same reason do not connect  $ab$ . This is so because arrow head showing the relationship go upwards only.)

3. Now put an arrow head on each segment.

4. Two elements which are thus connected by a line segment with an arrow head are related. In this way we get the following matrix of the relation.

$$M_R = \begin{bmatrix} a & b & c & d & e \\ a & 1 & 0 & 1 & 1 & 1 \\ b & 0 & 1 & 1 & 1 & 1 \\ c & 0 & 0 & 1 & 1 & 1 \\ d & 0 & 0 & 0 & 1 & 0 \\ e & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

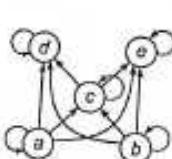


Fig. 17.47

From this matrix, we get the following relation.

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, c), (a, d), (a, e),$$

$$(b, c), (b, d), (b, e), (c, d), (c, e)\}$$

(Note that since a Hasse diagram is related to a poset,  $R$  is not symmetric.)

**15. Dual of Poset**

(M.U. 2009)

**Theorem :** If  $R$  is a partial order relation on  $A$  then  $R^{-1}$  i.e. the inverse relation is also a partial order on  $A$ . I.e., if  $(A, R)$  is a poset then  $(A, R^{-1})$  also is a poset.

(M.U. 2004)

**Proof :** Since  $R$  is a partial order on  $A$ , by definition,

(i)  $R$  is reflexive, i.e.,  $a R a$ .

(ii)  $R$  is antisymmetric, i.e., if  $a R b$  and  $b R a$  then  $a = b$ .

(iii) If  $a R b$  and  $b R c$  then  $a R c$  transitivity.

Also by definition  $R^{-1}$  is a relation obtained by interchanging the order of the elements in  $R$  i.e.,  $b R^{-1} a$  if  $a R b$ .

Hence, if  $a R a$ , then  $a R^{-1} a$  i.e.,  $R^{-1}$  is reflexive.

If  $a R b$  and  $b R a$  imply  $a = b$  then  $b R^{-1} a$  and  $a R^{-1} b$  imply  $a = b$ .

If  $a R b$  and  $b R c$  imply  $a R c$  then  $b R^{-1} a$  and  $c R^{-1} b$ , ( $c R^{-1} b$  and  $b R^{-1} a$ ) imply  $c R^{-1} a$ .

$\therefore R^{-1}$  is also an partial order relation.

Thus, if  $(A, R)$  is a poset then  $(A, R^{-1})$  is also a poset.

**Definition :** The poset  $(A, R^{-1})$  is called the dual of the poset  $(A, R)$  and the partial order

$R^{-1}$  is called dual of the partial order  $R$ .

**Example :** From the Hasse diagram given in Fig. 17.49 (a), find the poset and construct the Hasse diagram of its dual.

Sol.: As discussed earlier (on the previous page), from a given Hasse diagram we obtain the poset by (i) putting the loop on every element (ii) by putting the upward arrows.

We thus get the poset shown in Fig. 17.49 (b).

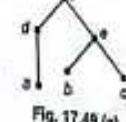


Fig. 17.49 (a)

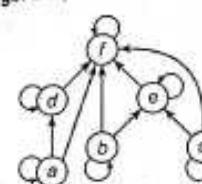


Fig. 17.49 (b)

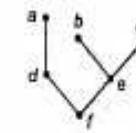


Fig. 17.49 (c)

From the diagram of Fig. 17.49 (b), we get the following partial order relation.

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, d), (d, f), (a, f), (b, e), (e, f), (b, f), (c, e), (c, f)\}$$

The dual of the partial order relation  $R$  is obtained by reversing the order of the elements. Hence,

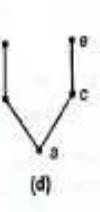
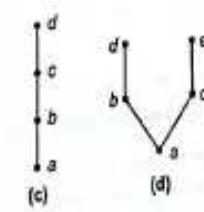
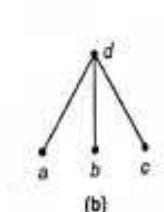
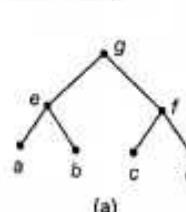
$$\text{Dual of } R = R^{-1}$$

$$= \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (d, a), (f, d), (f, a), (e, b), (f, e), (f, b), (e, c), (f, c)\}$$

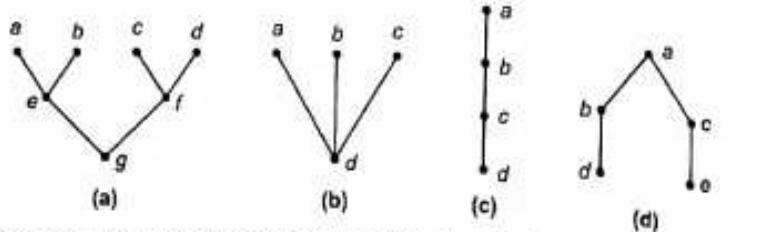
The Hasse diagram of dual of  $R$  is obtained by reversing the order of elements which means by turning the Hasse diagram of  $R$  upside down. [Fig. 17.49 (c)]

**EXERCISE - II**

1. Find the partial order relation from the following Hasse diagrams and obtain the Hasse diagrams of their duals.



[Ans. :



2. Prove that on the set of integers  $\leq$  is a partial order relation and prove that  $\geq$  is its dual.  
Further prove that both partial order relations are chains.

## 16. Extremal Elements of Posets

Certain elements of a poset are of special importance. We shall discuss these elements now and the importance of role played by them latter. In this section and here after we shall denote the poset by  $(A, \leq)$  where  $A$  is the set and  $\leq$  is the partial order relation. (M.U. 2008)

### (a) Maximal and Minimal Elements

**Definition 1 :** An element  $a \in A$  is called a **maximal element** of the poset  $A$  if there is no element  $c \in A$  such that  $a < c$ . (M.U. 2008)

In other words, an element  $a$  in a partially ordered set  $A$  is said to be **maximal** if no other element **succeeds**  $a$  i.e. if  $a \leq x$  then  $a = x$ .

**Definition 2 :** An element  $b \in A$  is called a **minimal element** of the poset  $A$  if there is no element  $c \in A$  such that  $c < b$ .

In other words, an element  $b$  in a partially ordered set  $A$  is said to be **minimal** if no other element **precedes**  $b$  i.e. if  $y \leq b$  then  $y = b$ .

We shall show below (Fig. 17.50) maximal and minimal elements of some posets diagrammatically.

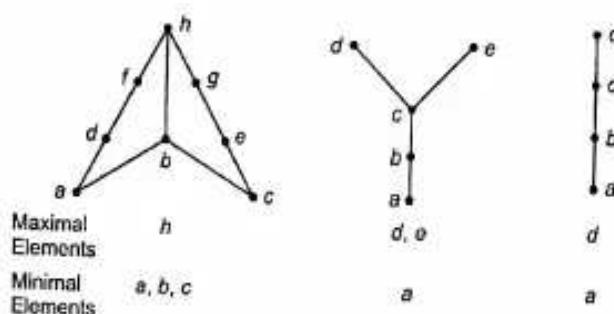


Fig. 17.50

**Example 1 :** Consider  $A = \{x \mid x \text{ is real and } 0 \leq x < 2\}$  with usual partial order  $\leq$ . Then 0 is the minimal element. There is no maximal element. (This so because  $2 \notin A$ )

**Example 2 :** Consider  $A = \{x \mid x \text{ is real and } 0 < x \leq 2\}$  with usual partial order  $\leq$ . (M.U. 2008)  
Then 2 is the maximal element. There is no minimal element. (This is so because  $0 \notin A$ )

**Example 3 :** Consider  $A = \{x \mid x \text{ is real and } 0 \leq x \leq 2\}$ . Then 0 is the minimal elements and 2 is the maximal element.

**Example 4 :** Let  $A$  be the poset of non-negative real numbers with usual partial order relation  $\leq$  (less than or equal to). Then 0 is the minimal element of  $A$  and there is no maximal element.

**Example 5 :** Let  $A$  be the poset of non-positive real numbers with usual partial order relation  $\leq$ . Then 0 is the maximal element and there is no minimal element.

**Example 6 :** Consider the poset  $Z$  with usual partial order relation  $\leq$  (less than or equal to). There is no minimal element of  $Z$ , there is no maximal element of  $Z$ .

**Example 7 :** In Ex. 2 page 17-23 the poset  $A$  has two maximal elements 6 and 8 and one minimal element 1.

**Example 8 :** In Ex. 7 page 17-26, there are two minimal elements 2 and 3 and two maximal elements 24 and 36.

**Example 9 :** Let  $S = \{2, 4, 6, 12, 20\}$  be ordered by the relation of divisibility. Draw Hasse diagram and find the maximal and minimal elements of  $S$ . Sol: 12 and 20 are maximal elements. 2 is the minimal element.

**Example 10 :** Let  $S = \{2, 3, 4, 16\}$  be ordered by the relation of divisibility. Draw Hasse diagram and find the maximal and minimal elements. Sol: 3 and 16 are maximal elements. 2 and 4 are minimal elements.

Note that 3 is both maximal and minimal element because 3 is not comparable with any other element.

**Example 11 :** Find the maximal and minimal element of the poset shown in Fig. 17.53.

Sol:  $d$  and  $g$  are maximal elements,  $a$  and  $b$  are minimal elements.

We note the following properties of maximal and minimal elements of posets.

1. A poset may have more than one maximal element and more than one minimal elements.
2. A poset need not have any maximal element or any minimal element.
3. A poset may have a maximal element but no minimal elements or a minimal element but no maximal elements.

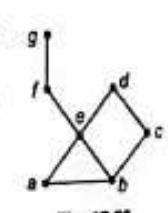


Fig. 17.53

**Theorem 1 :** Every finite non-empty poset  $(A, \leq)$  has at least one minimal element. (Note 'finite')

**Proof :** We accept the theorem without proof.

**Theorem 2 :** Every finite non-empty poset  $(A, \leq)$  has at least one maximal element. (Note 'finite')

**Proof :** We accept the theorem without proof.

## (b) Greatest and Least Elements

Let  $A$  be a finite non-empty poset. An element  $a \in A$  is called a **greatest element** of  $A$  if  $a \leq x$  for all  $x \in A$ . (M.U. 2008)

We show below greatest and least elements of some posets diagrammatically.

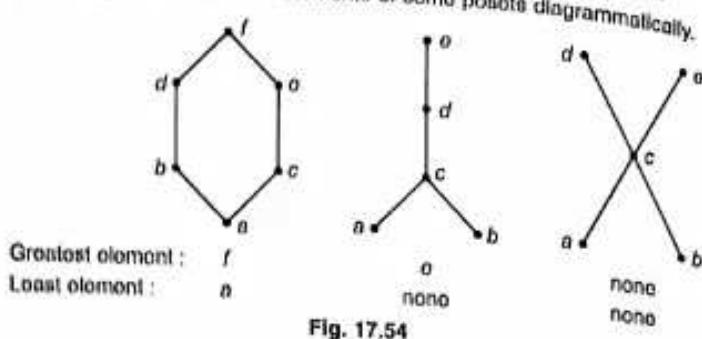


Fig. 17.54

**Example 1 :** Let  $S = \{a, b, c, d\}$  and let  $A = \mathcal{P}(S)$  be the power set of  $S$  and  $\leq$  be the relation is a subset of.

Since  $\emptyset$  is a subset of every set of  $\mathcal{P}(S)$ ,  $\emptyset$  is the least element.

Since  $\{a, b, c, d\}$  is the superset of every set of  $\mathcal{P}(S)$ ,  $\{a, b, c, d\}$  is the greatest element.

**Example 2 :** Let  $A = \{1, 2, 3, 4, 6, 12, 24\}$  with partial order of divisibility.

Since 1 divides every element of  $A$ , 1 is the least element. Since every element divides 24, 24 is the greatest element.

**Example 3 :** Let  $A = \{2, 3, 6, 12, 24, 36\}$  with partial order of divisibility.

Since 2, 3 are not comparable  $A$  has no least element. Similarly, 24, 36 are not comparable. Hence,  $A$  has no the greatest element (See Fig. 17.55).

**Uniqueness :** The greatest element of a poset, if it exists is unique. Similarly, the least element, if it exists, is unique.

**Theorem 3 :** A poset has at most one greatest element and one least element.

**Proof :** We accept it without proof.

The greatest element of a poset, if it exists, is often called the **unit element** and is denoted by  $1$ . The least element of a poset, if it exists, is often called the **zero element** and is denoted by  $0$ .

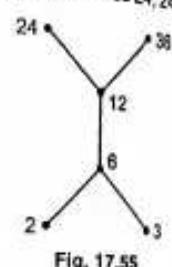


Fig. 17.55

**EXERCISE - III**

Find the maximal and minimal elements in each poset if they exist. (Ex. 1 to 8).

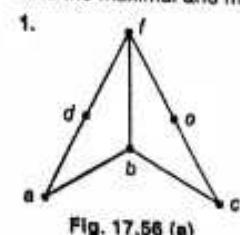


Fig. 17.56 (a)

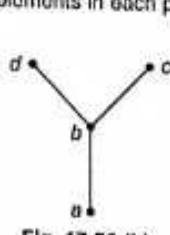


Fig. 17.56 (b)

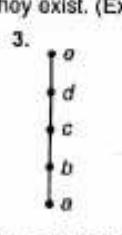


Fig. 17.56 (c)

[Ans. : (1) Minimal  $a, b, c$ ; maximal  $f$ . (2) minimal  $a$ ; maximal  $d, c$ .  
(3) minimal  $a$ ; maximal  $e, f$ .]

4.  $(A, \leq)$ ,  $A$  is the set of positive even integers.

5.  $(A, |)$ ,  $A$  is the set  $\{2, 5, 6, 12, 20\}$  and  $|$  is the relation of divisibility. Draw also Hasse diagram.

[Ans. : Max. 12, 20, Min. 2.]

For Hasse diagram see Fig. 17.57 (a)]

6.  $(A, |)$ ,  $A$  is the set  $\{2, 3, 4, 16\}$ . Draw Hasse diagram.

[Ans. : Max. 3, 16, Min. 3, 2.]

For Hasse diagram see Fig. 17.57 (b)]

7.  $(A, \leq)$ ,  $A$  is the set of negative even integers.

8.  $(A, \leq)$ ,  $A$  is the set of (negative and positive) integers.

9. Find the least and the greatest elements of the poset (i) in Ex. 5. (ii)  $A = \{2, 4, 6, 8, 12, 18, 24, 36, 72\}$  with partial order of divisibility.

[Ans. : (i) least 2, no greatest.  
(ii) least 2, greatest 72.]

10. Find the greatest and the least elements of the given posets (Fig. 17.58). (M.U. 2007)

[Ans. : (a) Least  $a$ , greatest  $h$ .  
(b) No least elements, greatest  $f$ .]

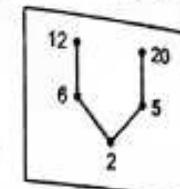


Fig. 17.57 (a)

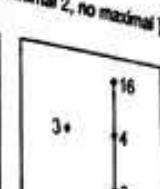


Fig. 17.57 (b)

## (d) Supremum and Infimum (LUB and GLB)

(M.U. 1996, 98)

Consider a poset  $A$  and a subset  $B$  of  $A$ .

**Definition 4 :** An element  $a \in A$  is called an **upper bound** of  $B$  if  $b \leq a$  for all  $b \in B$ .

In other words  $a$  is an upper bound of  $B$  if  $a$  succeeds every element  $b$  of  $B$ .

**Definition 5 :** An element  $a \in A$  is called a **lower bound** of  $B$  if  $a \leq b$  for all  $b \in B$ .

In other words  $a$  is a lower bound of  $B$  if  $a$  precedes every element  $b$  of  $B$ .

**Definition 6 :** Let  $A$  be a poset and  $B$  be a subset of  $A$ . An element  $a \in A$  is called a **least upper bound (LUB)** or **supremum** of  $B$  if  $a$  is an upper bound of  $B$  and  $a \leq a'$  where  $a'$  is an upper bound.

In other words, if an upper bound of  $B$  precedes every other upper bound of  $B$  then it is called a least upper bound of  $B$ .

**Definition 7 :** Let  $A$  be a poset and  $B$  be a subset of  $A$ . An element  $a \in A$  is called a **greatest lower bound (GLB)** or **infimum** of  $B$  if  $a$  is a lower bound of  $B$  and  $a' \leq a$  if  $a'$  is a lower bound.

In other words if a lower bound of  $B$  succeeds every other lower bound of  $B$  then it is called a greatest lower bound of  $B$ .

**Example 1 :** Consider the poset  $A = \{a, b, c, d, e, f, g, h\}$  whose Hasse diagram is shown in Fig. 17.59. Find all upper and lower bounds of the following subsets of  $A$  (i)  $B_1 = \{a, b\}$ . (ii)  $B_2 = \{d, e\}$ . (M.U. 2004)

Sol. : (i) It is clear that since there are no elements in  $A$  below  $a, b$ ,  $B_1$  has no lower bound.

Also since  $c, d, e, f, g, h$  are above i.e. succeed  $a, b$  the upper bounds of  $B_1$  are  $c, d, e, f, g, h$ .

(ii) Since the elements  $a, b, c$  in  $A$  are below i.e. precede  $d, e$  the lower bounds of  $B_2$  are  $a, b, c$ .

Since the elements  $f, g, h$  are above i.e. succeed  $d, e$ , the upper bounds of  $B_2$  are  $f, g, h$ .

**Example 2 :** Consider the poset  $A = \{a, b, c, d, e, f, g, h\}$  whose Hasse diagram is shown in Fig. 17.60. Find all upper bounds and lower bounds of  $B = \{c, d, e\}$ .

Sol. : Since  $f, g, h$  succeed every element of  $B$ ,  $f, g, h$  are the upper bounds of  $B$ .

Since  $a, b$  precede every element of  $B$ ,  $a, b$  are the lower bounds of  $B$ .

From Ex. 1 and Ex. 2, we see that an upper or a lower bounds of  $B$  may or may not belong to  $B$ .

**Example 3 :** Consider  $A = \{1, 3, 5, 7, 15, 21, 35, 105\}$  and let  $R$  be the relation 'a divides b'. Find all upper and lower bounds of  $B_1 = \{3, 7\}$ ,  $B_2 = \{3, 5\}$ . (M.U. 2014)

OR Draw Hasse diagram of  $D_{105}$ .

Sol. : The Hasse diagram is given in Fig. 17.61.

Since 21 and 105 succeed both 3, 7 the upper bounds of  $B_1$  are 21, 105.

Since 15 and 105 succeed both 3, 5 the upper bounds of  $B_2$  are 15, 105.

Since 1 precedes both 3 and 7, the lower bound of  $B_1$  is 1.

Similarly, the lower bound of  $B_2$  is 1.

**Example 4 :** Let  $A$  be the poset considered in Ex. 1. Let the subsets  $B_1$  and  $B_2$  be defined as in the same example. Find least upper bound and greatest lower bound of (i)  $B_1$  and (ii) of  $B_2$ .

Sol. : (i) Since  $B_1$  has no lower bound it has no greatest lower bound.

Since  $c$  precedes all other upper bounds  $d, e, f, g, h$  we have LUB =  $c$ .

(ii) Since  $c$  succeeds all other lower bounds  $a, b$  we have GLB =  $c$ .

Upper bounds of  $B_2$  are  $f, g, h$ . But  $f, g$  are not comparable. We therefore, say that  $B_2$  has no least upper bound.

**Example 5 :** Find the greatest lower bound and the least upper bound of the sets  $\{3, 9, 12\}$  and  $\{1, 2, 4, 5, 10\}$  if they exist in the poset  $(Z, /)$  where  $/$  is the relation of divisibility.

Sol. : (a) We have set  $A = \{3, 9, 12\}$ . (M.U. 2005, 06)

The relation  $R$  is,

$$R = \{(3, 3), (3, 9), (3, 12), (9, 9), (12, 12)\}$$

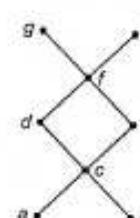


Fig. 17.61

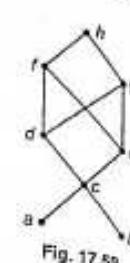


Fig. 17.59

$$\therefore M_R = \begin{bmatrix} 3 & 9 & 12 \\ 1 & 1 & 1 \\ 9 & 0 & 1 & 0 \\ 12 & 0 & 0 & 1 \end{bmatrix}$$

We shall now find the Hasse diagram of  $R$ .

The digraph of  $R$  is as shown in Fig. 17.62 (a). There is no transitivity. Removing the loop we get

Hasse diagram as shown in Fig. 17.62 (b).

The GLB is 3. LUB does not exist.

b) We have  $A = \{1, 2, 4, 5, 10\}$ . The relation  $R$  is

$$R = \{(1, 1), (1, 2), (1, 4), (1, 5), (1, 10), (2, 2), (2, 4), (2, 10), (4, 4), (5, 5), (5, 10), (10, 10)\}$$

$$\therefore M_R = \begin{bmatrix} 1 & 2 & 4 & 5 & 10 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 1 & 0 & 1 \\ 4 & 0 & 0 & 1 & 0 & 0 \\ 5 & 0 & 0 & 0 & 1 & 1 \\ 10 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

We shall now find Hasse diagram of  $R$ .

The digraph is as shown in Fig. 17.63 (a).

Deleting the transitivity and the arrow-heads, we get the Hasse diagram as given in Fig. 17.63 (b).

The GLB is 1, LUB does not exist.

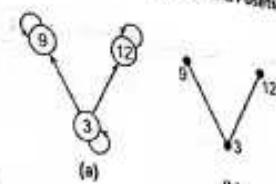


Fig. 17.62

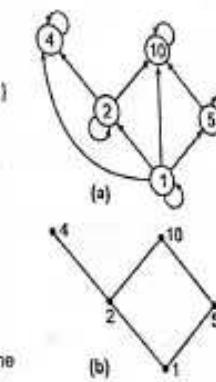


Fig. 17.63

**Example 6 :** Find the GLB and LUB

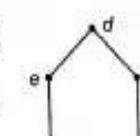
in the following posets whose Hasse diagrams are shown in Fig. 17.64.

Sol. : (i) In (A),  $a$  is the GLB and  $d$  is LUB.

(ii) In (B),  $e$  is the LUB, GLB does not exist.



(A)



(B)

**Example 7 :** Find the lower bounds and upper bounds of the subsets

(i)  $\{a, b, c\}$ , (ii)  $\{j, h\}$ , (iii)  $\{a, c, d, f\}$

in the poset with Hasse diagram shown in the Fig. 17.65.

(M.U. 2005, 06)

Also find GLB and LUB of  $\{b, d, g\}$ .

Sol. : (i) For the subset  $\{a, b, c\}$  lower bound is  $a$  and upper bounds are  $e, f, h$  and  $j$ .

(ii) For the subset  $\{j, h\}$  lower bounds are  $f, e, c, d, b, a$  and there is no upper bound.

(iii) For the subset  $\{a, c, d, f\}$  lower bound is  $a$  and upper bounds are  $f, j, h$ .

(iv) For the subset  $\{b, d, g\}$  GLB is  $b$  and LUB is  $g$ .

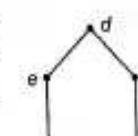


Fig. 17.64



Fig. 17.65

**EXERCISE - IV**

Find (i) all upper bounds, (ii) all lower bounds, (iii) the least upper bound, (iv) the greatest lower bound of  $B$  for the given poset  $A$ .

1. Consider the poset  $A = \{a, b, c, d, e, f, g, h\}$  whose Hasse diagram is shown in Fig. 17.59, page 17-39. Let  $B = \{c, d, e\}$ .

2. Consider the poset  $A = \{a, b, c, d, e, f, g, h\}$  whose Hasse diagram is shown in Fig. 17.59, page 17-39. Let  $B = \{b, g, h\}$ .

[Ans. : (i) No upper bound ; (ii)  $b$  ; (iii) No least upper bound ; (iv)  $b$ ]

3. Consider the poset  $A = \{a, b, c, d, e, f\}$  whose Hasse diagram is shown in Fig. 17.66. Let  $B = \{b, c, d\}$ .

[Ans. : (i)  $d, e, f$ ; (ii)  $b, a$ ; (iii)  $d$ ; (iv)  $b$ ]

4. Let  $A$  be the set of real numbers and  $R$  be the relation  $\leq$ . Let  $B = \{x \mid x$  is a real number and  $2 < x < 3\}$ .

[Ans. : (i)  $\{x \mid x \in [3, \infty)\}$ ; (ii)  $\{x \mid x \in (-\infty, 2]\}$ ; (iii) 3; (iv) 2]

5. Let  $A$  be the set of real numbers and  $R$  be the relation  $\leq$ . Let  $B = \{x \mid x$  is a real number and  $2 \leq x < 3\}$ .

[Ans. : (i)  $\{x \mid x \in [3, \infty)\}$ ; (ii)  $\{x \mid x \in (-\infty, 2]\}$ ; (iii) 3; (iv) 2]

6. Let  $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ . Let  $R$  be the relation 'a divides b',  $B = \{10, 15\}$ . Also draw Hasse diagram.

[Ans. : (i) 30; (ii) 1, 5; (iii) 30; (iv) 5.]

For Hasse diagram see Fig. 17.67.]

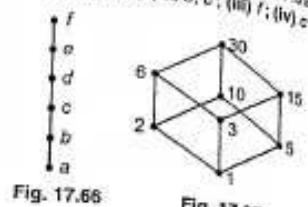


Fig. 17.66

Fig. 17.67

**Theory****EXERCISE - V**

1. Define the following terms with suitable examples.

- (i) Cartesian Product (M.U. 2011)
- (ii) Reflexive Relation, (M.U. 1997, 2011)
- (iii) Symmetric Relation, (M.U. 2005, 2011)
- (iv) Equivalence relation (M.U. 2010)
- (v) Antisymmetric relation (M.U. 2010)
- (vi) Partial order relation (M.U. 2010)

2. Define a relation  $R$  on a non-empty set  $A$  and state when  $R$  is an equivalence relation. (M.U. 1998)

3. Give an example of a relation which is

- (a) (i) Reflexive, symmetric but not transitive.  
(ii) Symmetric, transitive but not reflexive. (M.U. 1997)
- (b) (i) Reflexive, transitive but not symmetric.  
(ii) Symmetric, but neither reflexive nor transitive. (M.U. 1996)
- (c) (i) Transitive but neither reflexive nor symmetric. (M.U. 1996)

4. Define symmetric and antisymmetric relations. Does there exist a relation which is symmetric and antisymmetric both. Justify your answer? (M.U. 2001)

5. If  $R$  is a binary relation on the set of positive integers such that  $R = \{(a, b) \mid a - b$  is an odd positive integer)

Is  $R$  reflexive ? Symmetric ? Transitive ? Is it an equivalence relation ? (M.U. 2001, 05)

(Hint :  $R$  is not reflexive as  $a - a = 0 \neq$  odd. Not symmetric e.g. if  $a - b = 3$  then  $b - a = -3$ ,  $R$  is not transitive  $R$  is not an equivalence relation.)

6. If  $S$  is the set of all points in a plane and  $R$  is the relation that for any two points  $a$  and  $b \in S$  if  $a$  and  $b$  is within 1 inch from  $a$ .

Examine if  $R$  is an equivalence relation. (M.U. 1996)

[Ans. :  $R$  is symmetric, reflexive but not transitive.  $R$  is not an equivalence relation.]

7. Let  $R$  be a binary relation. Let  $S = \{(a, b) \mid a R c$  and  $c R b$  for some  $c\}$ .

Show that if  $R$  is an equivalence relation then  $S$  also is an equivalence relation. (M.U. 1998)

8. Consider the relation "congruence modulo  $m$ " given by  $x R y$  if and only if  $(x - y)$  is divisible by  $m$  over the set of integer.

(i) Show that  $R$  is an equivalence relation.

(ii) Show that if  $x_1 R y_1$  and  $x_2 R y_2$  then  $(x_1 + x_2) R (y_1 + y_2)$ .

9. Let  $R$  be a reflexive relation on a set  $A$ . Show that  $R$  is an equivalence relation if and only if  $(a, b)$  and  $(a, c)$  are in  $R$  implies that  $(b, c)$  is in  $R$ . (M.U. 1996, 98)

(Hint : Putting  $c = a$ , by data  $a R b$  and  $a R a$  implies  $b R a$ . Symmetry.)

10. Let  $m$  be a positive integer greater than 1. Show that the relation  $R = \{(a, b) \mid a \equiv b \pmod{m}\}$  is an equivalence relation on the set of integers. (M.U. 2006)

11. Determine whether the relation  $R$  defined below on set of all integers is reflexive, symmetric, antisymmetric and / or transitive where  $x R y$  if and only if (i)  $xy \geq 1$ , (ii)  $x \equiv y \pmod{7}$ . (M.U. 2005)

[Ans. : Both are equivalence relations. Not antisymmetric.]

12. Define partial order relation. (M.U. 1997, 2001)

13. Define dual of a poset with an example. (M.U. 2009)

14. Define POSET and Hasse Diagram. (M.U. 2010, 13)

15. Define the terms for a subset  $B$  of a poset  $A$  -

(i) upper bound, (ii) least upper bound, (iii) lower bound, (iv) greatest lower bound.

Give one example of each. (M.U. 1996)

16. Explain the terms : (i) Posets (M.U. 1999, 2013)

(ii) Extremal elements. (M.U. 2008)

17. For a given set  $S$ , let  $P(S)$  denote the power set of  $A$ . Consider the relation  $A R B$  if  $A \subseteq B$ . Show that  $R$  is a partial order relation.

18. If  $L$  is a bounded and distribution lattice then prove that the complement is unique if it exists. (M.U. 2004)



# CHAPTER 18

# Lattices

## 1. Introduction

In the previous chapter, we have studied equivalence relations and posets. In this chapter, we shall study a particular type of posets called lattices.

## 2. Lattices

Lattice is a mathematical structure with two binary operations called join and meet which frequently appear in computing and its mathematical applications.

We first define two new terms join and meet with reference to a poset  $L$ .

**Definitions :** Let  $A$  be a poset  $(L, \leq)$ . Let  $a, b$  be two elements  $\in L$ . Now, we define

$a \vee b$  (read as 'a join b') as LUB of  $a$  and  $b$ .

$a \wedge b$  (read as 'a meet b') as GLB of  $a$  and  $b$ .

**Theorem :** Let  $L$  be a poset  $(A, \leq)$  and let  $a, b \in A$  then

(i) If  $a$  and  $b$  have a LUB then this LUB is unique.

(ii) If  $a$  and  $b$  have a GLB then this GLB is unique.

**Proof :** We prove the theorem by reductio-ad-absurdum method.

(I) Let if possible the elements  $a, b$  have two distinct LUB's  $l_1$  and  $l_2$ .

Then by definition of LUB:  $a \leq l_1$  and  $b \leq l_1$

and  $a \leq l_2$  and  $b \leq l_2$

But, since  $l_1$  is a LUB  $l_1 \leq l_2$ . Also since  $l_2$  is a LUB  $l_2 \leq l_1$ .

By antisymmetric property of  $\leq$ ,  $l_1 = l_2$ .

But this contradicts our hypothesis.

$\therefore$  LUB of  $a, b$  is unique.

(II) We can prove the part (ii) in the same way.

**Definition :** A poset  $(L, \leq)$ , in which every pair  $\{a, b\}$  of two elements of  $L$  has a least upper bound (LUB) and a greatest lower bound (GLB), is called a lattice. (M.U. 2005, 07, 13)

We denote LUB  $(a, b)$  by  $a \vee b$  and call it the join of  $a$  and  $b$ . Also we denote GLB  $(a, b)$  by  $a \wedge b$  and call it the meet of  $a$  and  $b$ . Since a lattice is an algebraic system with binary operations  $\vee$  and  $\wedge$ , it is denoted by  $| L, \vee, \wedge |$ .

It may be noted that a totally ordered set is trivially a lattice but not all partially ordered sets are lattices.

As illustrations we show below two lattices diagrammatically.

## Fig. 18.1 (a)

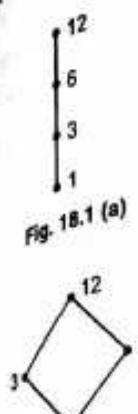


Fig. 18.1 (b)

Fig. 18.1 (b)

(18-2)

v	1	3	6	12
1	1	3	6	12
3	3	3	6	12
6	6	6	6	12
12	12	12	12	12

LUB

$\wedge$	1	3	6	12
1	1	1	1	1
3	3	1	3	3
6	6	1	3	6
12	12	1	3	12

GUB

v	1	3	4	12
1	1	3	4	12
3	3	3	12	12
4	4	12	4	12
12	12	12	12	12

LUB

$\wedge$	1	3	4	12
1	1	1	1	1
3	3	1	3	3
4	4	1	1	4
12	12	1	3	12

GUB

Fig. 18.2 (a)

Fig. 18.2 (a)

(a)	v	$\Phi$	{a}	$\wedge$	$\Phi$	{a}
$\Phi$	$\Phi$	$\Phi$	{a}	$\Phi$	$\Phi$	
{a}		{a}	{a}	{a}	$\Phi$	{a}

Table No. 1

Table No. 2

Since  $(\mathcal{P}(S), \subseteq)$  is a poset and every pair of elements of  $\mathcal{P}(S)$  has an LUB and a GLB, it is a lattice.

Note ...

As noted above, the LUB of two subsets of the power set  $\mathcal{P}(S)$  of the set  $S$  is obtained by taking the union of the subsets. e.g. LUB  $(\{a\}, \{b\})$  is  $\{a, b\}$ . Similarly, the GLB of two subsets of  $\mathcal{P}(S)$  is obtained by taking the intersection of the subsets. e.g. GLB  $(\{a\}, \{b\})$  is  $\emptyset$ . Thus, the join  $\vee$  is equivalent to union  $\cup$  and the meet  $\wedge$  is equivalent to the intersection of two subsets of  $\mathcal{P}(S)$ . This is why join is denoted by  $\vee$  for (union  $\cup$ ) and the meet is denoted by  $\wedge$  (intersection  $\cap$ ).

(II) When  $S = \{a, b\}$ ,  $\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ . Its Hasse diagram and operation tables for  $\vee$  and  $\wedge$  are given below.

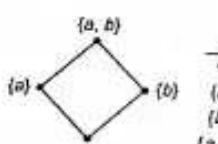


Fig. 18.2 (b)

Table No. 1

Since  $(\mathcal{P}(S), \subseteq)$  is a poset and every pair of elements in  $\mathcal{P}(S)$  has an LUB and a GLB, it is a lattice.

(iii) When  $S = \{a, b, c\}$ ,

$\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ .  
Its Hasse diagram is shown in Fig. 18.2 (c).

The operation tables for  $\vee$  i.e. union and  $\wedge$  i.e. intersection of two sets are given below.

$\vee$	$\emptyset$	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}
$\emptyset$	$\emptyset$	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}
{a}	{a}	{a}	{a, b}	{a, c}	{a, b}	{a, c}	{a, b, c}	{a, b, c}
{b}	{b}	{b}	{b}	{b, c}				
{c}	{c}	{c}	{c}	{c}	{c}	{c}	{c}	{c}
{a, b}	{a, b}	{a, b}	{a, b}	{a, b, c}				
{a, c}	{a, c}	{a, c}	{a, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}
{b, c}	{b, c}	{b, c}	{b, c}	{b, c}	{b, c}	{b, c}	{b, c}	{b, c}
{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}

$\wedge$	$\emptyset$	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}
$\emptyset$								
{a}	{a}	$\emptyset$	$\emptyset$	$\emptyset$	{a}	$\emptyset$	$\emptyset$	{a}
{b}	$\emptyset$	{b}	$\emptyset$	$\emptyset$	$\emptyset$	{b}	$\emptyset$	{b}
{c}	$\emptyset$	$\emptyset$	{c}	$\emptyset$	$\emptyset$	$\emptyset$	{c}	$\emptyset$
{a, b}	{a}	{b}	$\emptyset$	{a, b}	{a}	{b}	{a, b}	$\emptyset$
{a, c}	{a}	$\emptyset$	{c}	{a, c}	$\emptyset$	{c}	{a, c}	$\emptyset$
{b, c}	$\emptyset$	{b}	{c}	$\emptyset$	{b, c}	$\emptyset$	{b, c}	$\emptyset$
{a, b, c}	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}	$\emptyset$

Since  $(\mathcal{P}(S), \subseteq)$  is a poset and every pair of elements in  $\mathcal{P}(S)$  has a LUB and GLB, it is a lattice.

**Example 2 :** Show that the set of all divisions of 70 form a lattice.  
(M.U. 1995, 2015)

**Sol. :** The set of all divisions is the set  $A = \{1, 2, 5, 7, 10, 14, 35, 70\}$ .  
The Hasse diagram of the poset is shown in Fig. 18.3.

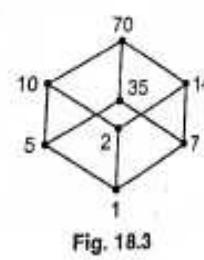


Fig. 18.3

As in the above example, we got the following tables.

$\vee$	1	2	5	7	10	14	35	70
1	1	2	5	7	10	14	35	70
2	2	2	10	14	10	14	70	70
5	5	10	5	35	10	70	35	70
7	7	14	35	7	70	14	35	70
10	10	10	70	10	70	70	70	70
14	14	14	70	14	70	14	70	70
35	35	70	35	35	70	70	35	70
70	70	70	70	70	70	70	70	70

$\wedge$	1	2	5	7	10	14	35	70
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
5	1	1	5	1	5	1	5	5
7	1	1	1	7	1	7	7	7
10	1	2	5	1	10	2	5	10
14	1	2	1	7	2	14	7	14
35	1	1	5	7	5	7	35	35
70	1	2	5	7	10	14	35	70

Since every pair of elements has a LUB and GLB the set is a lattice.

**Example 3 :** Let  $A = \{1, 3, 5, 15, 30, 60, 90, 180\}$  with the relation of divisibility. Draw Hasse diagram. Determine whether it is a lattice. (M.U. 2011)

Sol. : The Hasse diagram of the relation is shown in the Fig. 18.4.

It is a lattice.

**Example 4 :** Let  $L = \{1, 2, 3, 6\}$  and  $R$  be the relation 'is divisible by'. Prove that  $L$  is a lattice.

Sol. : The relation matrix and Hasse diagram are as shown below.

1	2	3	6
1	1	1	1
2	0	1	0
3	0	0	1
6	0	0	1

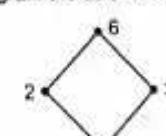


Fig. 18.4

Using the matrix  $M_R$ , we can show that  $(L, R)$  is a poset (Left to you as an exercise).

In the first problem we saw that if  $A$  is the power set of  $A$  and the relation is set inclusion then the LUB or the join  $\vee$  of two elements is the union and the GLB or the meet of two elements is the intersection.

Now, we shall see what  $\vee$  and  $\wedge$  mean when  $A$  is a set of positive integers and the relation is 'is divisible by'.

By applying the definition and also from the above figure, we see that LUB of 2 and 3 is 6, of 2 and 6 is 6 etc.

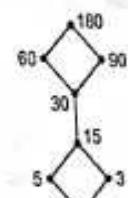


Fig. 18.5

Thus, LUB in this case means the lowest common multiple (LCM) present in the set of two numbers. Thus, so far as numbers are concerned the LUB or the join  $\vee$  means the LCM present in the set.

Similarly, from the definition and also from the above figure, we see that the GLB of 2 and 6 is 2, of 2 and 1 is 1, of 2 and 3 is 1 etc.

Thus, GLB in this case means the greatest common divisor (GCD) present in the set.

Hence, the join  $\vee$  of  $a, b$  means the LCM i.e. the lowest common multiple of  $a, b$  i.e. the smallest number which is divisible by  $a$  and  $b$  both and which is present in  $A$ . The meet  $\wedge$  of  $a, b$  means, the GCD i.e. the greatest common divisor of  $a, b$  i.e. the largest number that divides  $a$  and  $b$  both and which is present in  $A$ .

With these considerations, we get the following tables. The operation table for  $\vee$  and  $\wedge$  are given below.

$\vee$	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

$\wedge$	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

Since  $(L, R)$  is a poset and every pair of elements of  $L$  has an LUB and a GLB, it is a lattice.

**Example 5 :** Let  $L = \{1, 2, 3, 5, 30\}$  and  $R$  be the relation 'is divisible by'. Prove that  $L$  is a lattice.

**Sol. :** The relation matrix and Hasse diagram are shown below.

	1	2	3	5	30
1	1	1	1	1	1
2	0	1	0	0	1
3	0	0	1	0	1
5	0	0	0	1	1
30	0	0	0	0	1

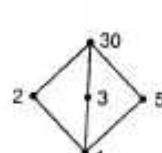


Fig. 18.6

Using matrix  $M_R$ , we can show that  $(L, R)$  is a poset (Left to you as an exercise).

Now, while preparing the tables for  $\wedge$  and  $\vee$  we have to see that I.c.m. and g.c.d. of elements  $a, b$  must be present in  $A$ . Thus, I.c.m. of 2 and 5 is 10 but it is not present in  $A$ . However, 30 is also I.c.m. of 2 and 5 which is present in  $A$ . Hence,  $2 \vee 5 = 30$ . Similarly, we find that  $3 \vee 5 = 30$ ,  $2 \vee 3 = 30$ . Thus, we get the following table for  $\vee$  and  $\wedge$ .

The operation tables for  $\vee$  and  $\wedge$  are given below.

$\vee$	1	2	3	5	30
1	1	2	3	5	30
2	2	2	30	30	30
3	3	30	3	30	30
5	5	30	30	5	30
30	30	30	30	30	30

$\wedge$	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

Since  $(L, R)$  is a poset and every pair of elements of  $L$  has an LUB and a GLB it is a lattice.

If  $n$  is a positive integer then  $D_n$  denotes the set of all divisors of  $n$ . For example,  $D_3$  denotes the set of all divisors of 3 i.e.  $D_3 = \{1, 3\}$ ,  $D_4$  denotes the set of all divisors of 4 i.e.  $D_4 = \{1, 2, 4\}$ .

The posets associated with the relation of divisibility are denote by  $(D_3, \leq)$ ,  $(D_4, \leq)$  etc. The relation  $\leq$  is the relation of Divisibility.

**Example 6 :** Prove that  $(D_8, \leq)$  and  $(D_{10}, \leq)$  are lattices. Show their Hasse diagrams.

**Sol. :** We have  $D_8 = \{1, 2, 4, 8\}$ . The Hasse diagram is shown in Fig. 18.7 (a).

**(b)** We have  $D_{10} = \{1, 2, 5, 10\}$ . The Hasse diagram is shown in Fig. 18.7 (b).

It is left to you to prepare the tables for  $\wedge$  and  $\vee$  and show that they are lattice.

**Example 7 :** Draw the Hasse diagram of the poset  $A = \{1, 2, 3, 6, 12, 24, 36, 72\}$  under the relation of divisibility. Is it a lattice?

**Sol. :** The Hasse diagram is shown in Fig. 18.8. It is a lattice.

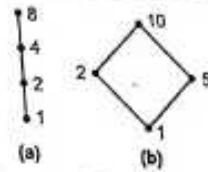


Fig. 18.7

**Example 8 :** Draw the Hasse diagram of the poset  $A = \{1, 2, 5, 10, 20, 40, 100, 200\}$  under the relation of divisibility. Is it a lattice?

**Sol. :** The Hasse diagram is shown in Fig. 18.9 above. It is a lattice.

**Example 9 :** Draw the Hasse diagram of the poset  $A = \{1, 3, 4, 12, 24, 48, 72, 144\}$  under the relation of divisibility. Is it lattice?

**Sol. :** The Hasse diagram is shown in Fig. 18.10 above. It is a lattice.

**Example 10 :** Let  $A = \{1, 2, 3, 4, 6, 8, 12, 24\}$  with the relation of divisibility. Draw Hasse diagram. Determine whether it is a lattice.

**Sol. :** The Hasse diagram is shown in Fig. 18.11 above. The poset is a lattice.

**Example 11 :** Draw the Hasse diagrams of the lattices having  $2^n$  elements for  $n = 1, 2, 3$ . (M.U. 2000)

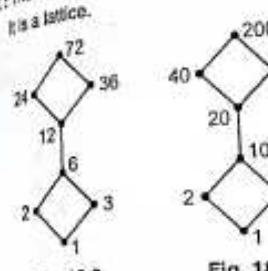


Fig. 18.8

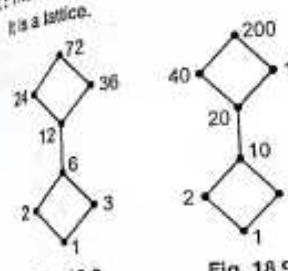


Fig. 18.9

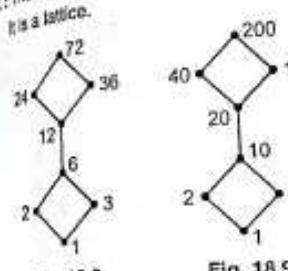


Fig. 18.10

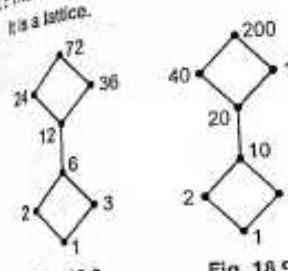


Fig. 18.11

Sol.: For  $n = 0, 1, 2, 3$  the Lattices have  $2^n = 1, 2, 4, 8$  elements. The corresponding Lattices are shown below.

$n$	Elements	Lattice
0	1	.
1	2	↓
2	4	◇
3	8	◆

Fig. 18.12

Example 12 : Determine whether the posets with the Hasse diagram [Fig. 17.90 (a) and (b)] are lattices or not.  
(M.U. 2003, 06, 12)

Sol.: We shall prepare the tables of LUB and GLB for both sets.

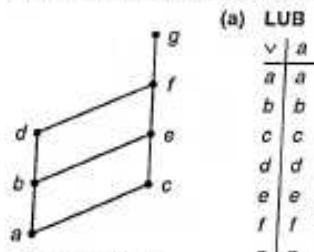


Fig. 18.13 (a)

$\vee$	a	b	c	d	e	f	g	h	i
a	a	b	c	d	e	f	g	h	i
b	b	b	c	d	e	f	g	h	i
c	c	e	c	g	e	f	g	h	i
d	d	d	g	d	g	i	g	i	i
e	e	e	e	g	e	h	g	h	i
f	f	h	f	i	h	f	i	h	i
g	g	g	g	g	g	g	g	h	i
h	h	h	h	i	h	h	i	i	i
i	i	i	i	i	i	i	i	i	i

GLB

$\wedge$	a	b	c	d	e	f	g	h	i
a	a	a	a	a	a	a	a	a	a
b	b	b	g	d	f	g	h	h	h
c	c	g	c	f	e	f	g	h	h
d	d	d	f	d	f	f	h	h	h
e	e	f	e	f	e	f	g	h	h
f	f	f	f	f	f	f	h	h	h
g	g	g	g	h	g	h	g	h	h
h	h	h	h	h	h	h	h	h	h
i	i	i	i	i	i	i	i	i	i

GLB

GLB of  $\{f, g\}$  does not exist, the poset is not a lattice.

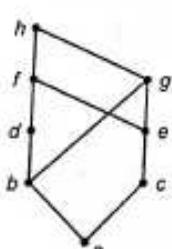


Fig. 18.13 (b)

Example 13 : Draw Hasse diagram of the relation of divisibility on the set  $A = \{2, 4, 12, 16\}$  (M.U. 2009, 11)

check if it is a lattice.

Given : The relation  $R = \{(2, 2), (2, 4), (2, 12), (2, 16), (4, 4), (4, 12), (4, 16), (12, 12), (16, 16)\}$

The matrix of the relation and Hasse diagram (Fig. 17.91) is shown below.

$$M_R = \begin{bmatrix} 2 & 4 & 12 & 16 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

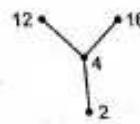


Fig. 18.14

Since there is no LUB for 12 and 16 R is not a lattice.

Example 14 : Determine whether the following Hasse diagram represents a lattice.

Given : LUB

$\vee$	a	b	c	d	e	f	g	h	i
a	a	b	c	d	e	f	g	h	i
b	b	b	e	d	e	h	g	h	i
c	c	e	c	g	e	f	g	h	i
d	d	d	g	d	g	i	g	i	i
e	e	e	e	g	e	h	g	h	i
f	f	h	f	i	h	f	i	h	i
g	g	g	g	g	g	g	g	h	i
h	h	h	h	i	h	h	i	i	i
i	i	i	i	i	i	i	i	i	i

Given : GLB

$\wedge$	a	b	c	d	e	f	g	h	i
a	a	a	a	a	a	a	a	a	a
b	a	b	a	b	a	b	a	b	b
c	a	a	c	a	c	c	c	c	c
d	a	b	a	d	b	a	d	b	d
e	a	b	c	b	e	c	e	e	e
f	a	a	c	a	c	f	c	f	f
g	a	b	c	d	e	c	g	e	g
h	a	b	c	b	e	f	g	h	h
i	a	b	c	d	e	f	g	h	i

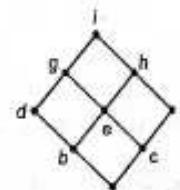


Fig. 18.15

Since every pair of elements has a LUB and GLB, the relation is a lattice.

### Applied Mathematics - IV

(18-9)

**Example 15 :** Determine whether the posets with the following Hasse diagrams (Fig. 18.16) are lattices or not.

(M.U. 2013)

**Sol. :** Both Hasse diagrams are lattices because every pair of elements has GLB and LUB.

**Example 16 :** Determine whether the posets represented by the Hasse diagrams (Fig. 18.17(a)) are lattices.

(M.U. 2002)

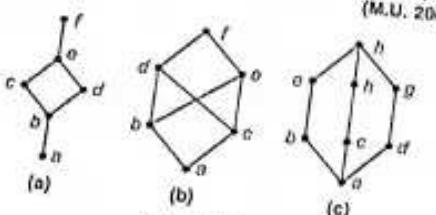


Fig. 18.17

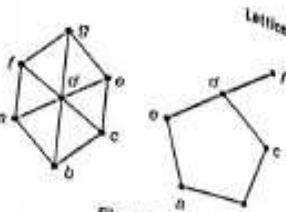


Fig. 18.16

**Sol. :** (i) Fig. 18.17 (a) is a lattice as every pair has a LUB and GLB.

(ii) Fig. 18.17 (b) is not a lattice as LUB of (b, c) and GLB of (d, e) do not exist.

(iii) Fig. 18.17 (c) is a lattice as every pair has a LUB and GLB.

**Example 17 :** Let  $D_m$  denote the set of divisors of a positive integer  $m$ . For  $m = 36$ , prove that  $D_m$  is a lattice under the relation 'a divides b' i.e.,  $(D_m, \leq)$  is a lattice.

(M.U. 2008, 15)

**Sol. :** We see that  $D_{36} = \{1, 2, 3, 4, 6, 12, 18, 36\}$ . Its Hasse diagram is shown in the Fig. 18.18. We leave it to you to prepare the tables for (LUB)  $\wedge$  and (GLB)  $\vee$ .

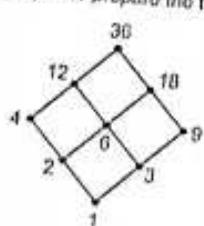


Fig. 18.18

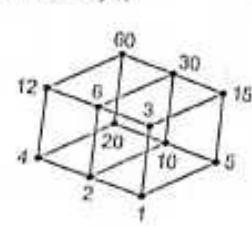


Fig. 18.19

**Example 18 :** Draw the Hasse diagram of  $D_{60}$ . Check if it is a lattice.

**Sol. :** The Hasse diagram of  $D_{60}$  is shown in Fig. 18.10. Proof is left to you.

**Example 19 :** Check whether  $A = \{2, 4, 12, 16\}$  and  $B = \{3, 4, 12, 24\}$  are lattices under divisibility.

Draw their Hasse diagrams.

**Sol. :** (a) The Hasse diagram is shown below.

(M.U. 2010, 11, 12, 15)

(M.U. 2009, 11)

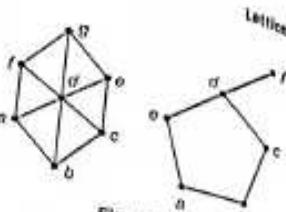


Fig. 18.16

### Applied Mathematics - IV

(18-10)

operation tables for  $\vee$  and  $\wedge$  are given below.

	2	4	12	16		2	4	12	16
2	2	4	12	16		2	2	2	2
4	4	4	12	16		4	2	4	4
12	12	12	12	—		12	2	4	12
16	16	16	—	16		16	2	4	16

From the table that LUB of (12, 16) [and of (16, 12)] does not exist. Hence, it is not a lattice.

Hence, it is not a lattice.

The Hasse diagram is shown below.

The operation tables for (LUB)  $\vee$  and (GLB)  $\wedge$  are given below.

	3	4	12	24		3	4	12	24
3	3	12	12	24		3	—	3	3
4	12	4	12	24		—	4	4	4
12	12	12	12	24		12	3	4	12
24	24	24	24	24		24	3	4	12

From the table that GLB of (3, 4) [and of (4, 3)] does not exist. Hence, it is not a lattice.

**Example 20 :** Prove that the following posets are not lattices. Draw also the Hasse diagram.

(i)  $L = \{a_1, a_2, a_3, a_4, a_5, a_6\}$

$R = \{(a_1, a_2), (a_1, a_4), (a_1, a_5), (a_1, a_6), (a_2, a_4), (a_2, a_5), (a_2, a_6), (a_3, a_4), (a_3, a_5), (a_3, a_6)\}$

(ii)  $L = \{a_1, a_2, a_3, a_4, a_5\}$

$R = \{(a_1, a_2), (a_1, a_4), (a_1, a_5), (a_2, a_4), (a_2, a_5), (a_3, a_4), (a_3, a_5)\}$

(iii)  $L = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$

$R = \{(a_1, a_2), (a_1, a_4), (a_1, a_5), (a_1, a_6), (a_1, a_7), (a_2, a_4), (a_2, a_5), (a_2, a_6), (a_2, a_7), (a_3, a_4), (a_3, a_5), (a_3, a_6), (a_3, a_7), (a_4, a_5), (a_4, a_6), (a_4, a_7), (a_5, a_6), (a_5, a_7)\}$

(iv) The LUB of  $a_5$  and  $a_6$  does not exists. Also the GLB of  $a_1$  and  $a_2$  does not exist. Hence,  $L$  is not a lattice. Hasse diagram is shown in Fig. 18.20 (a).

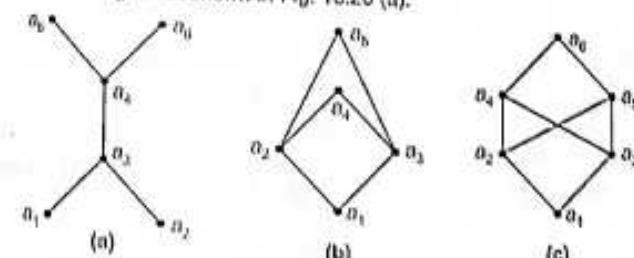


Fig. 18.20

(b) The LUB of  $a_2$  and  $a_3$  does not exist. Also GLB of  $a_4$  and  $a_5$  does not exist. Hence,  $L$  is not a lattice. Hasse diagram is shown in Fig. 18.20 (b).

(c) The LUB of  $a_2$  and  $a_3$  does not exist. Also GLB of  $a_4$  and  $a_5$  does not exist. Hence,  $L$  is not a lattice. Hasse diagram is shown in Fig. 18.20 (c).

(18-11)

**Example 21 :** Show that the set of all divisors of 70 form a lattice.  
**Sol. :** The Hasse diagram of  $L$  is as shown in Fig. 18.21.  
 Since every pair of elements of  $L$  has a LUB and GLB, it is a lattice.

**Example 22 :** Determine whether the Hasse diagram [Fig. 18.22 and (M.U. 1995, 2000)] define a lattice.

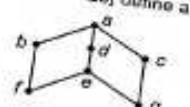


Fig. 18.22

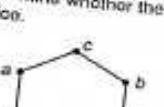


Fig. 18.23

(18-11)

**Sol. :** (I) Since GLB of  $(f, g)$  does not exist, it is not a lattice.  
 (II) Each pair of elements has LUB and GLB.  
 Hence, it is a lattice.

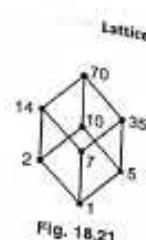


Fig. 18.21

**Example 23 :** Draw the Hasse diagram of the poset  $A = \{2, 3, 6, 12, 24, 36, 72\}$  under the relation of divisibility. Is it a lattice?  
**Sol. :** The relation "is divisible by" is given by the following matrix.

	2	3	6	12	24	36	72
2	1	0	1	1	1	1	1
3	0	1	1	1	1	1	1
6	0	0	1	1	1	1	1
12	0	0	0	1	1	1	1
24	0	0	0	0	1	0	1
36	0	0	0	0	0	1	1
72	0	0	0	0	0	0	1

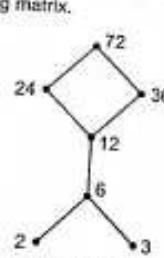


Fig. 18.24

The Hasse diagram is as shown in Fig. 18.24.  
 It is easy to see from the figure that there is no GLB to the pair  $(2, 3)$ .

Hence, it is not a lattice.

### 3. Dual in a Lattice

Consider the two statements (1)  $a \vee a = a$ , (2)  $a \wedge a = a$ .

It can be seen that statement (2) can be obtained from (1) by changing  $\vee$  by  $\wedge$  and statement

(1) can be obtained from (2) by changing  $\wedge$  by  $\vee$ . Such statements are called duals of each other.

**Definition :** The dual of any statement in a lattice  $(L, \vee, \wedge)$  is defined to be the statement obtained by interchanging  $\vee$  and  $\wedge$ .

For example, (1) Dual of  $a \vee b = b \vee a$  is  $a \wedge b = b \wedge a$ .

(2) Dual of  $a \vee (b \vee c) = (a \vee b) \vee c$  is  $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ .

#### Principal of Duality

If a statement is true in a lattice  $(L, \vee, \wedge)$  then its dual is also true in  $(L, \vee, \wedge)$ .

This is called the principal of duality.

(M.U. 2009)

(18-12)

Lattices

Applied Mathematics - IV

**Theorem :** Let  $L$  be a lattice. Then the following properties hold.

1. Idempotent properties :  $a \vee a = a$  and  $a \wedge a = a$

2. Commutative properties :  $a \vee b = b \vee a$  and  $a \wedge b = b \wedge a$

3. Associative properties :  $a \vee (b \vee c) = (a \vee b) \vee c$  and  $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

**Proof :** (1) By definition of LUB and GLB,  $\text{LUB} \{(a, a)\} = a$  and  $\text{GLB} \{(a, a)\} = a$ . Hence,

$a \vee a = a$  and  $a \wedge a = a$ .

(2) Show in the definition of LUB and GLB of  $a, b$  the order does not enter,

$\text{GLB} \{(a, b)\} = \text{GLB} \{(b, a)\}$ .

$a \vee b = b \vee a$  and  $a \wedge b = b \wedge a$ .

(3) By the definition LUB  $a$  is less than or equal to the LUB of  $a$  and  $(b \vee c)$ .

$a \leq a \vee (b \vee c)$

By the same reasoning

$b \vee c \leq a \vee (b \vee c)$

Also  $b \leq (b \vee c)$  and  $c \leq (b \vee c)$

Since  $b \leq (b \vee c)$  and  $b \vee c \leq a \vee (b \vee c)$

By transitivity  $b \leq a \vee (b \vee c)$

Since  $c \leq (b \vee c)$  and  $b \vee c \leq a \vee (b \vee c)$

By transitivity  $c \leq a \vee (b \vee c)$

Now,  $a \leq a \vee (b \vee c)$  and  $b \leq a \vee (b \vee c)$

This means  $a \vee (b \vee c)$  is an upper bound of  $a$  and  $b$ .

Hence, by definition of LUB,  $a \vee b \leq a \vee (b \vee c)$ .

Now,  $a \vee b \leq a \vee (b \vee c)$  and  $c \leq a \vee (b \vee c)$

This means  $a \vee (b \vee c)$  is an upper bound of  $a \vee b$  and  $c$ .

Hence, by definition of LUB,  $(a \vee b) \vee c \leq a \vee (b \vee c)$  ..... (1)

Similarly, we can prove that,  $a \vee (b \vee c) \leq (a \vee b) \vee c$  ..... (2)

Since,  $L$  is a poset having the property of antisymmetry from (1) and (2), we get

$$(a \vee b) \vee c = a \vee (b \vee c).$$

Similarly we can prove that (or it follows from the principle of duality)

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c.$$

(3) By definition of GLB of  $a$  and  $b$ ,  $a \wedge b$  is less than or equal to  $a$ .

$\therefore a \leq b \leq a$  but  $a \leq a$ .

$\therefore a$  is an upper bound of  $a \wedge b$  and  $a$ . Hence, LUB of  $a$  and  $a \wedge b$  is less than or equal to  $a$ .

$$\therefore a \vee (a \wedge b) \leq a$$

By definition of LUB the LUB of  $a$  and  $a \wedge b$  is greater than or equal to  $a$ .

$$\therefore a \leq a \vee (a \wedge b)$$

From (3) and (4), we get  $a \vee (a \wedge b) = a$ .

Similarly, we can prove that (or it follows from the principle of duality)

$$a \wedge (a \vee b) = a.$$

**Example 1:** For any  $a, b, c, d$  in a lattice  $(L, \leq)$ , if  $a \leq b$  and  $c \leq d$ , show that (i)  $a \vee c \leq b \vee d$  and (ii)  $a \wedge c \leq b \wedge d$ .

Sol.: By data  $a \leq b$  and by definition of LUB  $b \leq b \vee d$ .  
 ∴ By transitivity,  $a \leq b \vee d$ .  
 By data  $c \leq d$  and by definition of LUB  $d \leq b \vee d$ .  
 ∴ By transitivity,  $c \leq b \vee d$ .  
 By (i) and (ii)  $b \vee d$  is an upper bound of  $a, c$ .  
 By definition of LUB,  $a \vee c \leq b \vee d$ .  
 Similarly, we can prove that  $a \wedge c \leq b \wedge d$ .

**Example 2:** Let  $(A, \leq)$  be a poset. Let  $\leq_R$  be a binary relation on  $A$  such that for  $a$  and  $b$  in  $A$ ,  $a \leq_R b$  if and only if  $b \leq a$ .

- (i) Show that  $\leq_R$  is a partially ordering relation.
- (ii) Show that if  $(A, \leq)$  is a lattice then  $(A, \leq_R)$  is also a lattice.

Sol.: (a) Since  $\leq$  is a poset, we have

- (i)  $a \leq a$  (Reflexivity).
- (ii) If  $a \leq b$  and  $b \leq a$ , then  $a = b$  (Antisymmetry).
- (iii) If  $a \leq b$ ,  $b \leq c$ , then  $a \leq c$  (Transitivity)

Now, for every  $a$  in  $A$ ,  $a \leq a$ . Hence,  $a \leq_R a$ .

∴  $\leq_R$  is reflexive.

Further, let  $a \leq_R b$  and  $b \leq_R a$ .

∴  $a \leq_R b$  we have  $b \leq a$ .

∴  $b \leq_R a$  we have  $a \leq b$ .

But since  $\leq$  is antisymmetric if  $b \leq a$  and  $a \leq b$ , then  $a = b$ .

Hence, if  $a \leq_R b$  and  $b \leq_R a$ , then  $a = b$ .

∴  $\leq_R$  is antisymmetric.

Further if  $a \leq_R b$  and  $b \leq_R c$ , then  $b \leq a$  and  $c \leq b$ .

This means  $c \leq b$  and  $b \leq a$ .

Hence,  $c \leq a$  ∴  $a \leq_R c$ .

∴  $\leq_R$  is transitive.

∴  $(A, \leq_R)$  is a poset.

(b) Since  $(A, \leq)$  is a lattice for every two elements  $a, b$  in  $A$ , GLB =  $g$  and LUB =  $l$  exist in  $A$ . Consider  $\{a, b, g, l\}$ . Since  $g$  is GLB of  $a, b$ ,  $g \leq a$  and  $g \leq b$ .

∴  $a \leq_R g$  and  $b \leq_R g$

∴  $g$  is the LUB of  $a, b$ .

Also since  $l$  is LUB of  $a, b$ ,  $a \leq l$  and  $b \leq l$ .

∴  $l \leq_R a$  and  $l \leq_R b$ .

Hence,  $l$  is GLB of  $a, b$ . Hence, for  $a, b$ , GLB and LUB exist.

∴  $(A, \leq_R)$  is also a lattice.

**EXERCISE - I**  
 1. State whether the following Hasse diagrams represent lattices.

(i)

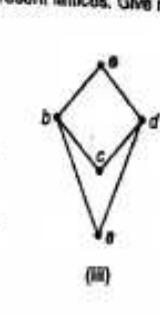
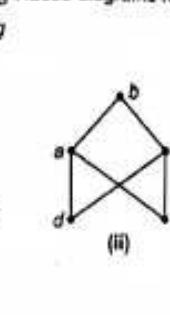
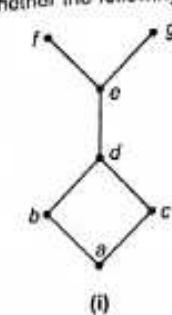
(ii)

(iii)

(iv)

[Ans. : All the diagrams represent lattices]

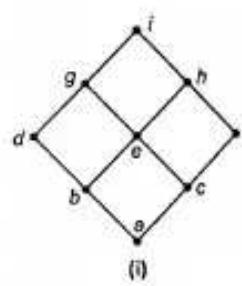
2. State whether the following Hasse diagrams represent lattices. Give reasons.



[Ans. : (i) The LUB of  $\{f, g\}$  does not exist. It is not a lattice. (ii) The GLB of  $\{a, c\}$  does not exist. Also the LUB of  $\{d, e\}$  does not exist. It is not a lattice. (iii) The GLB of  $\{b, d\}$  does not exist. It is not a lattice.]

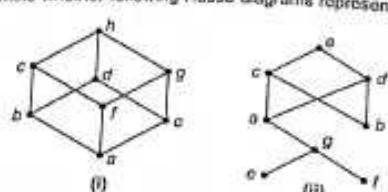
3. Determine whether the following Hasse diagrams represent a lattice. Give reasons.

(M.U. 2008)



[Ans. : (i) Yes. It is a lattice since each pair has a LUB and a GLB. (ii) No. It is not a lattice since GLB of  $\{a, b\}$  does not exist.]

4. Determine whether following Hasse diagrams represent a lattice. Give reasons.



[Ans. : (i) Yes. It is a lattice since each pair has a LUB and GLB. (ii) No. It is not a lattice, since GLB of {b, f} does not exist. Also GLB of {e, f} does not exist.]

5. Draw Hasse diagrams for the following poset under the relation  $R$  'is divisible by' and determine whether it represents lattice.

$$L = \{2, 3, 4, 6, 8, 24, 48\}$$

[Ans. : See adjoining figure.]

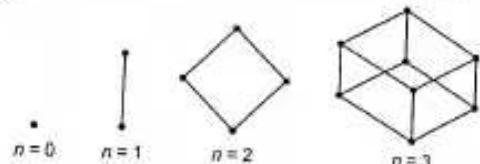
(M.U. 2000)



It is not a lattice since the GLB of {2, 3} does not exist.]

6. Draw Hasse diagrams of lattices having  $2^n$  elements for  $n = 0, 1, 2, 3$ .

Ans. :



(M.U. 1999)

7. Draw the Hasse diagram for  $A = \{1, 3, 5, 15, 30\}$  and  $R$  is "a divides b". Check it is a lattice.

[Ans. : For Hasse diagram see Fig. (a) below; Yes.]

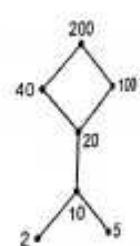
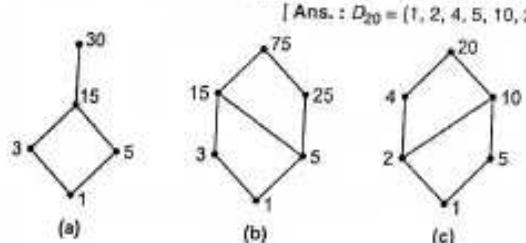
8. Draw Hasse diagram for  $(D_{75}, \leq)$  and check whether it is a lattice.

[Ans. :  $D_{75} = \{1, 3, 5, 15, 25, 75\}$ ; Yes. See Fig. (b) below.]

9. Draw Hasse diagram for  $(D_{20}, \leq)$  and check if it is a lattice.

(M.U. 2010, 12, 13)

[Ans. :  $D_{20} = \{1, 2, 4, 5, 10, 20\}$ ; Yes. See Fig. (c) below.]

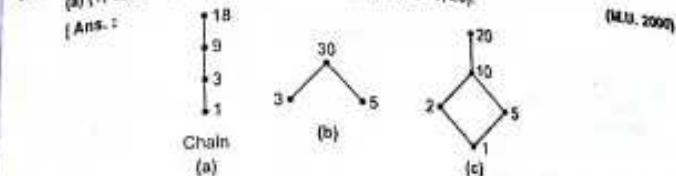


10. Is the poset  $A = \{2, 5, 10, 20, 40, 100, 200\}$  a lattice under the relation of divisibility? [Ans. : No. See adjoining figure.]

11. Draw Hasse diagrams of the following sets under partial ordering relation 'divides' and indicate which are chains.

- (a) {1, 3, 9, 18}, (b) {3, 5, 30}, (c) {1, 2, 5, 10, 20}

[Ans. :



12. Draw the Hasse diagram for  $L = \{1, 2, 3, 5, 6, 10, 15, 30\}$  and let the relation  $R$  be 'a divisible by'. Determine whether it is a lattice.

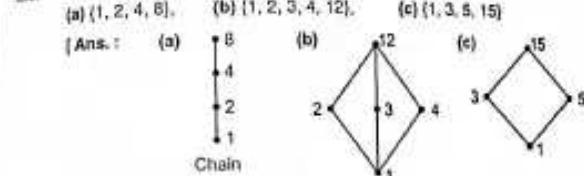
(M.U. 2010, 12, 13)

[Ans. : Hasse diagram shown in adjoining figure. Yes. It is a lattice.]

13. Draw the Hasse diagrams of the following sets under partial order relation divides and indicate which are chains.

- (a) {1, 2, 4, 8}, (b) {1, 2, 3, 4, 12}, (c) {1, 3, 5, 15}

[Ans. :



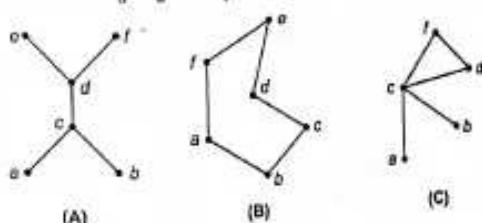
14. Is the poset  $L = \{3, 4, 12, 24, 48, 72, 144\}$  under the relation of divisibility a lattice? Draw the Hasse diagram.

[Ans. : Hasse diagram shown in adjoining figure (a). Not a lattice since the GLB of {3, 4} does not exist.]

15. Is the poset  $L = \{2, 6, 8, 12, 24\}$  under the relation of divisibility a lattice? Draw the Hasse diagram.

[Ans. : Hasse diagram shown in above figure (b). It is a lattice.]

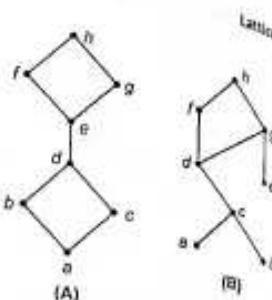
16. Which of the following diagrams represent lattice.



[Ans. : In (A) the LUB of  $a$  and  $f$  does not exist. Also the GLB of  $a$  and  $b$  does not exist. It is not a lattice. In (C) the LUB of  $a$ ,  $b$  does not exist. (B) is a lattice.]

18. Determine whether the Hasse diagrams (Fig. A and Fig. B) represent lattices.

[Ans. : (A) is a lattice, a distributive lattice. (B) is not a lattice.  $a$ ,  $b$  have no GLB.  $d$ ,  $e$  have no GLB.]



#### 4. Special Types of Lattices

##### (1) Sub-lattice

Let  $(L, \leq)$  be a lattice. A non-empty subset  $S$  of  $L$  is called a **sub-lattice** if for each  $a \in S$  and  $b \in S$ ,  $a \vee b \in S$  and  $a \wedge b \in S$ .

In other words, if  $S$  is a non-empty subset of a lattice  $L$  such that every pair  $\{a, b\}$  of  $S$  has a LUB and a GLB (i.e.  $S$  is a lattice) then  $S$  is called a sub-lattice.

**Example 1 :** Let  $L = \{1, 2, 4, 5, 10, 20\}$  and  $S = \{1, 4, 5, 20\}$ . Let the relation be 'is divisible by'. Show that  $S$  is a sub-lattice.

**Sol. :** The Hasse diagram of  $L$  is as shown in Fig. 18.25 (a) below. It is easy to see that  $L$  is a lattice.

The Hasse diagram of  $S$  is as shown in Fig. 18.25 (b) below.

$S$  is also a lattice.  $\therefore S$  is a sub-lattice.

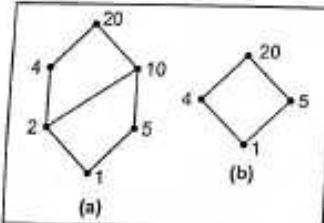


Fig. 18.25

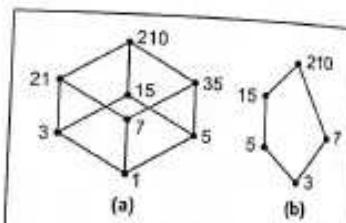


Fig. 18.26

**Example 2 :** Let  $L = \{1, 3, 5, 7, 15, 21, 35, 210\}$  and  $S = \{3, 5, 7, 15, 210\}$ . Let the relation be 'is divisible by'. Show that  $S$  is a sub-lattice.

**Sol. :** The Hasse diagram of  $L$  is as shown in Fig. 18.26 (a) above. It is easy to see that  $L$  is a lattice.

The Hasse diagram of  $S$  is as shown in the Fig. 18.26 (b) above. It is easy to see that  $S$  is a lattice.

$\therefore S$  is a sub-lattice.

**Example 3 :** Let  $L = \{1, 2, 3, 5, 6, 10, 15, 30\}$  and  $S = \{1, 2, 3, 6, 10, 30\}$ . Let the relation be 'is divisible by'. Show that  $S$  is a sub-lattice.

**Sol. :** The Hasse diagram of  $L$  is shown (Fig. 17.40) in Ex. 11, page 17-29. The Hasse diagram of  $S$  is as shown in Fig. 18.27. Since  $S$  is a lattice,  $S$  is a sub-lattice.

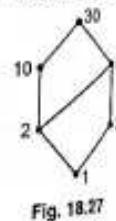


Fig. 18.27

**Example 4 :** Consider the lattice  $L$  given in (a) below. Let  $S_1$  be the poset (b),  $S_2$  be the poset (c) and  $S_3$  be the poset (d). Determine whether  $S_1$ ,  $S_2$  and  $S_3$  are sub-lattices.

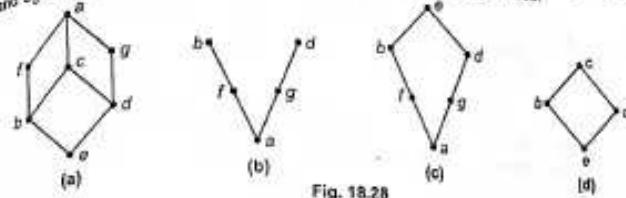


Fig. 18.28

**Sol. :** (i) The partially ordered subset  $S_1$  shown in (b) is not a lattice since the LUB of  $\{b, d\}$  does not exist.

(ii) The partially ordered subset  $S_2$  shown in (c) is not a sub-lattice because the GLB of  $\{b, d\}$  is  $f$  in the given set  $L$  and it does not belong to  $S_2$ .

(However, if we consider the poset  $S_2$  independently, it is a lattice.)

(iii) The partially ordered subset  $S_3$  shown in (d) is a sub-lattice.

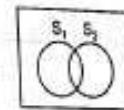


Fig. 18.29

**Example 5 :** Let  $L = \wp(A)$  be the lattice of all subsets of  $A$  under the relation of  $\subseteq$  set inclusion. Let  $S$  be a subset of  $A$ .

Prove that  $\wp(S)$  is a sub-lattice.

**Sol. :** Let us consider any two subsets  $S_1$  and  $S_2$  of  $S$ . Then it is easy to see that  $S_1 \cup S_2 \subseteq \wp(S)$  and  $S_1 \cap S_2 \subseteq \wp(S)$  i.e. LUB of  $S_1$  and  $S_2$  and GLB of  $S_1$  and  $S_2$  belong to  $\wp(S)$ . [Fig. 18.29]

Hence,  $\wp(S)$  is a sub-lattice.

**Example 6 :** Let  $L = \{1, 2, 4, 8, 16, 32\}$  and  $S = \{2, 8, 16\}$ . Let the relation be 'is divisibly by'. Prove that  $S$  is a sub-lattice.

**Sol. :**  $S = \{2, 8, 16\}$  under the relation 'is divisibly by' is a chain as shown in the Fig. 18.30.

Further every pair of elements of  $S$  has the LUB and GLB.

Hence,  $S$  is a sub-lattice.

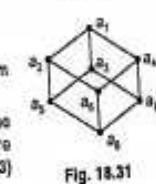


Fig. 18.30

**Example 7 :** Let  $(L, \leq)$  be a lattice in which  $L = \{a_1, a_2, \dots, a_6\}$ . Diagram of  $(L, \leq)$  is given in the Fig. 18.31.

Let  $S_1 = \{a_1, a_2, a_4, a_6\}$ ,  $S_2 = \{a_3, a_5, a_7, a_8\}$ ,  $S_3 = \{a_1, a_2, a_4, a_5\}$  be the subsets of  $L$ . Which of the above subsets  $(S_1, \leq)$ ,  $(S_2, \leq)$ ,  $(S_3, \leq)$  are sub-lattices? (M.U. 2003)

**Sol. :** (i) The Hasse diagram of  $(S_1, \leq)$  is shown in the following left figure.

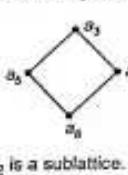
	$\vee$	$a_1$	$a_2$	$a_4$	$a_6$	$\wedge$	$a_1$	$a_2$	$a_4$	$a_6$
$a_1$	$a_1$	$a_1$	$a_1$	$a_1$	$a_1$	$a_1$	$a_1$	$a_1$	$a_1$	$a_1$
$a_2$	$a_1$	$a_2$	$a_2$	$a_2$	$a_2$	$a_2$	$a_2$	$a_2$	$a_2$	$a_2$
$a_4$	$a_1$	$a_2$	$a_4$	$a_4$	$a_4$	$a_4$	$a_4$	$a_4$	$a_4$	$a_4$
$a_6$	$a_1$	$a_2$	$a_4$	$a_6$	$a_6$	$a_6$	$a_6$	$a_6$	$a_6$	$a_6$

LUB

$\therefore S_1$  is a sublattice.

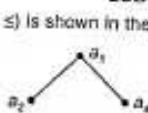
GLB

- (ii) The Hasse diagram of  $(S_2, \leq)$  is shown in the following left figure.



$\therefore S_2$  is a sub-lattice.

- (iii) The Hasse diagram of  $(S_3, \leq)$  is shown in the following figure.

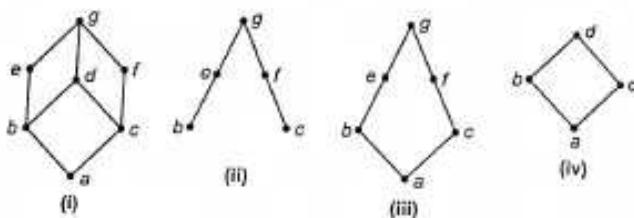


\* Fig. 18.32

Since GLB of  $a_2 \wedge a_3 (= a_6)$  does not belong to  $S_3$ , it is not a lattice.

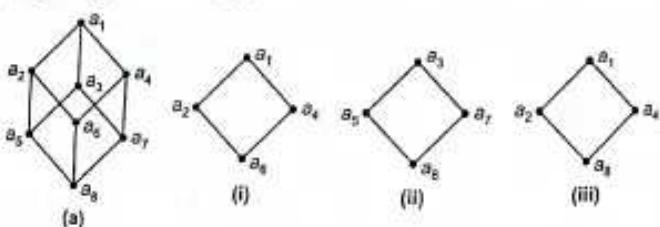
### EXERCISE - II

1. Given the lattice  $(L, \leq)$  where  $L = \{a, b, c, d, e, f, g\}$  shown in (i), examine whether  $S_1 = \{b, c, e, f, g\}$  shown in (ii),  $S_2 = \{a, b, c, e, f, g\}$  shown in (iii) and  $S_3 = \{a, b, c, d\}$  shown in (iv) are sub-lattices.



[Ans. : (i)  $S_1$  is not a sub-lattice as the GLB of  $\{b, c\}$  does not exist. (ii)  $S_2$  is not a sub-lattice as the LUB of  $\{b, c\}$  is  $d$  in  $L$ , it does not belong to  $S_2$ . However, if we consider the poset  $S_2$  independently, it is a lattice. (iii)  $S_3$  is a sub-lattice.]

2. Given the lattice  $(L, \leq)$  where  $L = \{a_1, a_2, a_3, \dots, a_8\}$  as shown in (a),  $S_1 = \{a_1, a_2, a_4, a_5\}$  as shown in (i),  $S_2 = \{a_3, a_5, a_7, a_8\}$  as shown in (ii),  $S_3 = \{a_1, a_2, a_4, a_6\}$  as shown in (iii). Examine whether  $S_1, S_2$  and  $S_3$  are sub-lattices.



[Ans. : (i)  $S_1$  is a sub-lattice, (ii)  $S_2$  is a sub-lattice, (iii)  $S_3$  is not a sub-lattice as the GLB of  $\{a_2, a_4\}$  is  $a_5$  in  $L$  and it does not belong to  $S_3$ . However, if we consider  $S_3$  independently then it is a lattice.]

3. Let  $L = \{1, 2, 3, 4, 6, 12\}$  and  $S = \{1, 3, 4, 12\}$ . Let the relation be 'is divisible by'. Show that  $S$  is a sub-lattice.

[See adjoining figure.]

4. Let  $S = \{a, b, c\}$  and let  $L = \wp(S)$  the set of all subsets of  $S$  be a lattice under the relation of set inclusion. Let  $T = \{a, b\}$ . Prove that  $\wp(T)$  is a sub-lattice of  $L$  where  $\wp(T)$  is the set of all subsets of  $T$ .

5. Show that a subset of a linearly ordered poset is a sub-lattice.

[Hint : Let  $a, b$  be any two elements of the poset. Then either  $a R b$  or  $b R a$ . Let  $a R b$  then  $a \wedge b = a$  and  $a \vee b = b$ . Hence, the result.]

### (ii) Distributive Lattices

(M.U. 2005, 14, 18)

Definition : A lattice  $L$  is called distributive if for any elements  $a, b, c$  of  $L$  the following distributive properties are satisfied.

- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Example 1 : Let  $L$  be the power set  $\wp(A)$  of  $A$  and  $R$  be the relation 'is a subset of'.  $L$  is a distributive lattice.

Sol. : Consider  $A = \{a, b, c\}$  then  $L = \wp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ . If  $R$  is the relation 'is a subset of' the Hasse diagram is shown in adjoining figure.

The LUB  $\{\{a\}, \{b\}\} = \{a, b\}$ . i.e., LUB  $\{\{a\}, \{b\}\} = \{a\} \cup \{b\}$ .

The GLB  $\{\{a\}, \{b\}\} = \emptyset$ . i.e., GLB  $\{\{a\}, \{b\}\} = \{a\} \cap \{b\}$ .

Thus, the join and meet correspond to union and intersection and since union and intersection satisfy distributive property  $L$  is a distributive lattice.

Example 2 : Consider the lattice shown in Fig. 18.34. Show that it is distributive.

Sol. : Consider the three elements  $a, b, c$ .

$$a \wedge b = b, b \wedge c = c, a \vee c = c$$

$$a \wedge b = a, b \wedge c = a, a \wedge c = a$$

$$\text{Now, } a \wedge (b \vee c) = a \wedge c = a \quad \text{and} \quad (a \wedge b) \vee (a \wedge c) = a \vee a = a$$

$$\text{Also, } a \vee (b \wedge c) = a \vee a = a \quad \text{and} \quad (a \vee b) \wedge (a \vee c) = b \vee c = a$$

In this way we can show that distributive property is satisfied for any three elements of  $a, b, c$ .

$\therefore L$  is a distributive lattice.

Note ...

There are 12 triples to be checked.

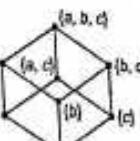
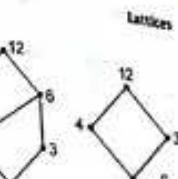


Fig. 18.33



Fig. 18.34

**Example 3 :** Show that the lattices whose Hasse diagrams are given below (Fig. 18.35) are not distributive.

Sol. : For (i)  $b \vee d = d$ ,  $b \vee c = e$ ,  $d \vee c = e$   
 $b \wedge d = b$ ,  $b \wedge c = a$ ,  $d \wedge c = a$   
Now,  $d \wedge (b \vee c) = d \wedge e = d$   
 $(d \wedge b) \vee (d \wedge c) = b \vee a = b$   
 $\therefore$  The distributive property is not satisfied.  
Hence, the lattice is not distributive.

For (ii)  $b \vee c = e$ ,  $b \wedge d = a$ ,  $c \vee d = e$   
 $b \wedge c = a$ ,  $b \wedge d = a$ ,  $c \wedge d = a$   
Now,  $d \wedge (c \vee d) = d \wedge e = d$   
 $(b \wedge c) \vee (b \wedge d) = a \vee a = a$   
 $\therefore$  The distributive property is not satisfied.  
Hence, the lattice is not distributive.

For (iii), we see that  
 $a \wedge (b \vee c) = a \wedge f = a$   
and  $(a \wedge b) \vee (a \wedge c) = a \vee a = a$   
 $\therefore a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$   
But  $b \vee (d \wedge e) = b \vee a = a$   
and  $(b \vee d) \wedge (b \vee c) = d \wedge f = d$ .  
 $\therefore$  The distributive property is not satisfied.  
Hence, the lattice is not distributive.

**Notes**

- For a distributive lattice  $L$ , it is necessary that the property of distributivity must be satisfied for all  $a, b, c \in L$ . Note Ex. 3(iii) carefully.
  - The following theorem which we accept without proof is highly useful to show that a given lattice is non-distributive.
- "A lattice is non-distributive if and only if it contains a sub-lattice which is isomorphic to one of the first two lattices of Example 3 above."**

**Example 4 :** Show that in a distributive lattice  $(A, \leq)$  if  $a \wedge x = a \wedge y$  and if  $a \vee x = a \vee y$  then  $x = y$ .

Sol. : By definition of LUB  $y$  is less than or equal to the LUB of  $y$  and  $y \wedge a$ .

$$\begin{aligned} & \therefore y \leq y \vee (y \wedge a). \quad \text{But } y \wedge y = y \\ & \therefore y \leq (y \vee y) \vee (y \wedge a) = y \vee (y \wedge a) \quad [\text{By distributivity}] \\ & \text{But } y \vee a = a \vee x \quad [\text{Data}] \\ & \therefore y \leq y \wedge (a \vee x) = (y \wedge a) \vee (y \wedge x) \\ & \text{But } y \wedge a = a \wedge x \quad [\text{Data}] \\ & \therefore y \leq (a \wedge x) \vee (y \wedge x) = x \wedge (a \vee y) \quad [\text{By distributivity}] \end{aligned}$$

By definition of GLB  $x$  is greater than or equal to the GLB of  $x$  and  $a \vee y$ .

Lattices  
(M.U. 2001, 03, 09)

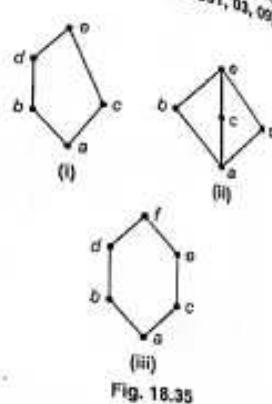


Fig. 18.35

But  $a \vee x = a \vee y$   
 $\therefore x$  is greater than or equal to  $x$  and  $a \vee y$ .  
 $\therefore x \wedge (a \vee y) \leq x \quad \therefore y \leq x$ .  
Similarly, we can prove that  
 $x \leq y \quad \therefore x = y$ .

**Example 5 :** Consider the lattice shown in the Fig. 18.36. Show that it is distributive lattice but is not a complemented lattice.

sol. : This is a distributive lattice with zero '0' and unit '1'. A lattice is said to be distributive if it satisfies two laws  
 $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$   
and  $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$   
Let  $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$   
L.H.S. =  $a \wedge (b \vee c) = a \wedge d = a$   
R.H.S. =  $(a \wedge b) \vee (a \wedge c) = a \vee a = a$

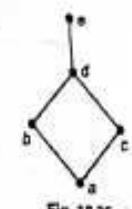


Fig. 18.36

It is not complemented since there is no any  $y$  corresponding to  $a$  such that  $a \vee y = 0$  and  $a \wedge y = 1$ .

**Example 6 :** In the diagrams shown in the Figs. 18.37 (a) and (b), a partially ordered  $\leq$  of a set  $A$  is represented. Is it a distributive lattice? A complemented lattice?

Sol. : (a) This is not a lattice. Since  $f$  and  $g$  have no lub.  
(b) This is a lattice with  $a$  as zero and  $f$  as 1, but it is not complemented since  $c$  has no complement and not distributive since  $d \wedge (b \vee c) = d \wedge e = d$  while  $(d \wedge b) \vee (d \wedge c) = d \vee a = b$ .

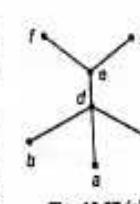


Fig. 18.37 (a)

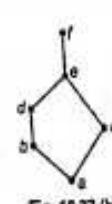


Fig. 18.37 (b)

**EXERCISE - III**

- Let  $L$  be the power set  $P(A)$  of  $A$  where  $A = \{a, b\}$ . Let  $R$  be the relation ' $\subseteq$ '. Show that  $L$  is a distributive lattice.
- Let  $L = \{1, 2, 3, 4, 6, 12\}$  and the relation be 'is divisible by'. Show that  $L$  is a distributive lattice.
- Let  $L = \{1, 2, 3, 4, 12\}$  and the relation be 'is divisible by'. Show that  $L$  is not a distributive lattice. (M.U. 2006)
- Let  $L = \{1, 2, 3, 5, 30\}$  and the relation be 'is divisible by'. Show that  $L$  is not a distributive lattice.
- Let  $L = \{1, 2, 3, 4, 9, 36\}$  and the relation be 'is divisible by'. Show that  $L$  is not a distributive lattice.
- Let  $L = \{1, 3, 5, 12, 20, 60\}$  and the relation be 'is divisible by'. Show that  $L$  is not a distributive lattice.

7. Let  $L = \{1, 3, 5, 6, 10, 60\}$  and the relation be 'is divisible by'. Show that  $L$  is not a distributive lattice.
8. Let  $L = \{1, 3, 5, 6, 9, 15, 45\}$  and the relation be 'is divisible by'. Show that  $L$  is not a distributive lattice. (M.U. 2008)
9. Show that the lattices shown in Fig. 18.38 are not distributive.

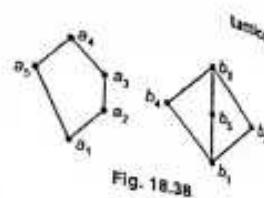


Fig. 18.38

**(3) Bounded Lattice**

A lattice  $L$  is said to be bounded if it has a greatest element and a least element.

**Example 1 :** The lattice  $L = \{1, 2, 3, 4, \dots, 10\}$  under partial order  $\leq$  is bounded since its least element is 1 and greatest element is 10.

**Example 2 :** The lattice  $L = \mathcal{P}(S)$  of all subsets of  $S$  is bounded since  $\emptyset$  is its least element and  $S$  is its greatest element.

**(4) Complement of an element**

Let  $L$  be a bounded lattice with greatest element 1 and least element 0. Let an element  $a \in L$ . An element  $\bar{a}$  belonging to  $L$  is called complement of  $a$  if

$$\text{LUB}(\{a, \bar{a}\}) \text{ i.e. } a \vee \bar{a} = 1 \quad \text{and} \quad \text{GLB}(\{a, \bar{a}\}) \text{ i.e. } a \wedge \bar{a} = 0$$

Note that  $\bar{\bar{a}} = a$  and  $\bar{\bar{0}} = 0$  where bars denote the complement.

**Remarks** ....

- Some authors use dash (') to denote the complement. A lattice  $L$  is called complemented if it is bounded and if every element of  $L$  has a complement.
- Note that if  $a$  is a complement of  $b$  then  $b$  is a complement of  $a$ . The relation is symmetric.

**Example 1 :** Let  $S = \{a, b, c\}$  and  $L = \mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ . Let the relation be 'is a subset of'. Show that every element has a complement.

**Sol. :** If  $A \in L$  then the complement set  $\bar{A}$  of  $A$  is the complement of  $A$  since  $A \vee \bar{A} = A \cup \bar{A} = S$  and  $A \wedge \bar{A} = A \cap \bar{A} = \emptyset$  and  $S$  is the greatest element and  $\emptyset$  is the least element. (See Fig. 18.2 (c), page 18-3).

The list of complements of all elements is given below.

Element	$\emptyset$	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}
Complement	{a, b, c}	{b, c}	{a, c}	{a, b}	{c}	{a}	{b}	$\emptyset$

**Example 2 :** Consider the lattices given in the Fig. 18.39. List the complements of all elements.

**Sol. :** Using the definition, we find that

For (i)

Element	0	b	a	c	1
Complement	1	c	c	a, b	0

For (ii)

Element	0	a	b	c	1
Complement	1	b, c	a, c	a, b	0

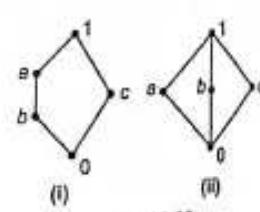


Fig. 18.39

Theorem : Let  $L$  be bounded distributive lattice. Show that the complement of an element of  $L$  exists is unique.

**Sol. :** Let  $a \in L$  and let  $a$  have a complement. We shall prove the result by reduction ad absurdum method.

Let, if possible  $a_1$  and  $a_2$  be the complements of  $a$ .

By definition of complement

$$a \vee a_1 = 1 \quad \text{and} \quad a \wedge a_1 = 0$$

$$a \vee a_2 = 0 \quad \text{and} \quad a \wedge a_2 = 0$$

Since, 0 is the least element, the LUB of  $\{a, 0\} = a_1$ .

$$\therefore a_1 = a_1 \vee 0 = a_1 \vee (a \wedge a_2) \quad [\text{By (2)}]$$

$$= (a_1 \vee a) \wedge (a_1 \vee a_2) \quad [\text{By distributivity}]$$

$$= 1 \wedge (a_1 \vee a_2) \quad [\text{By (1)}]$$

Since, 1 is the greatest element, the GLB  $\{a_1 \vee a_2, 1\}$  is  $a_1 \vee a_2$ .

$$\text{i.e. } 1 \wedge (a_1 \vee a_2) = a_1 \vee a_2$$

$$\therefore a_1 = a_1 \vee a_2 \quad [\text{By (2) and (3)}]$$

Similarly, arguing in the same way, we can prove that

$$a_2 = a_1 \vee a_2$$

Hence, from (4) and (5), we get  $a_1 = a_2$ .

**Example 4 :** Let  $L = \{1, 2, 4, 5, 10, 20\}$  and the relation be 'is divisible by'. List the complements of all elements of  $L$ . (M.U. 2006, 07, 12, 13)

**Sol. :** [ See Fig. 18.40 below.]

Element	1	4	5	2	10	20
Complement	20	5	4	No compl.	No compl.	1

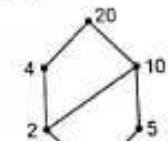


Fig. 18.40

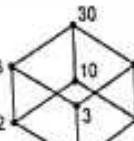


Fig. 18.41

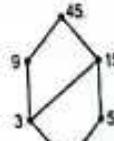


Fig. 18.42

**Example 5 :** Let  $L = \{1, 2, 3, 5, 6, 10, 15, 30\}$  and the relation be 'is divisible by'. List the complements of all elements of  $L$ . (M.U. 2010, 12, 13)

**Sol. :** [ See Fig. 18.41 above.]

Element	1	2	5	3
Complement	30	15	6	10

**Example 6 :** Let  $L = \{1, 3, 5, 9, 15, 45\}$  and the relation be 'is divisible by'. List the complements of all elements of  $L$ . (M.U. 2006)

**Sol. :** [ See Fig. 18.42 above.]

Element	:	1	3	5	9	15	45
Complement	:	45	No Compl.	9	5	No. Compl.	1

Note ...

In Ex. 2, we find that some elements can have more than one complement. In Ex. 4, we find that some elements may not have a complement.

However, if  $L$  is a distributive bounded lattice then if an element has a complement, then it is unique. (See Theorem, page 18-24)

**EXERCISE - IV**

1. Let  $S = \{a, b\}$  and  $L = \wp(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ . Let the relation be 'is a subset of'. Show that every element has a complement.

Ans. : Element :  $\emptyset$  {a} {b} {a, b}  
Complement : {a, b} {b} {a}  $\emptyset$ .

2. Let  $L = \{1, 2, 3, 6\}$  and the relation be 'is divisible by'. Write the complements of the elements of  $L$ .

Ans. : Element : 1 2 3 6  
Complement : 6 3 2 1

3. Let  $L = \{1, 2, 3, 5, 30\}$ . Let the relation be 'is divisible by'. Write the complements of the elements of  $L$ . (See Fig. of Ex. 5 on page 18-5)

Ans. : Element : 1 2 3 5 30  
Complement : 30 3, 5 2, 5 2, 3 1 (M.U. 2013)

4. Let  $L = \{1, 2, 3, 4, 12\}$ . Let the relation be 'is divisible by'. Write the complements of elements of  $L$ . (See Fig. 17.23 (c), page 17-23)

Ans. : Element : 1 2 3 4 12  
Complement : 12 3 2, 4 3 1

5. Let  $L = \{2, 6, 8, 12, 24\}$ . Let the relation be 'is divisible by'. Write the complements of elements of  $L$ .

Ans. : Element : 2 6 12 8 24  
Complement : 24 8 8 6, 12 2

6. Let  $L = \{2, 3, 5, 7, 15, 21, 35, 105\}$ . Let the relation be 'is divisible by'. Write the complements of elements of  $L$ . (Draw figure similar to Fig. 17.61 page 17-39)

Ans. : Element : 2 3 5 7  
Complement : 105 35 21 15

7. Let  $L = \{1, 2, 3, 4, 6, 12\}$ . Let the relation be 'is divisible by'. Write the complements of  $L$ .

Ans. : Element : 1 2 3 4 6  
Complement : 12 No compl. 4 3 No compl.

8. Let  $L = \{1, 2, 3, 6, 10, 30\}$ . Let the relation be 'is divisible by'. Write the complements of  $L$ . (See Fig. 18.27, page 18-17)

Ans. :	Element	:	1	2	3	6	10	10
	Complement	:	30	No compl.	10	No compl.	3	3

9. Find the complement of each element in  $D_{12}$ . ( $D_{12}$  denotes the set of all positive divisors of 42)

(M.U. 1998, 2000, 05, 07, 14)

(Hint :  $L = \{1, 2, 3, 6, 7, 14, 21, 42\}$ )

Ans. :	Element	:	1	2	3	6
	Complement	:	42	21	14	7

**(a) Complemented Lattice**

A lattice  $L$  is called complemented if it is bounded and if every element of  $L$  has at least one complement.

Example 1 : Let  $S = \{a, b, c\}$  and  $L = \wp(S)$  with 'set inclusion' as the relation.

As seen earlier (Ex. 1, page 18-23),  $L$  is bounded and each element has a complement.

$\therefore L$  is a complemented lattice.

Example 2 : Let  $L = \{1, 2, 3, 5, 6, 10, 15, 30\}$  with 'divisibility' relation.

As seen earlier (Ex. 5, page 18-24),  $L$  is bounded and each element has a complement.

$\therefore L$  is a complemented lattice.

Example 3 : Let  $L = \{1, 2, 3, 6, 7, 14, 21, 42\}$  with 'divisibility' relation.

As seen earlier (Ex. 9 above),  $L$  is bounded and each element has a complement.

$\therefore L$  is a complemented lattice.

Example 4 : Let  $L = \{1, 2, 3, 5, 30\}$  with 'divisibility' relation.

As seen earlier (Ex. 3, page 18-25),  $L$  is bounded and each element has a complement.

$\therefore L$  is a complemented lattice.

Example 5 : Let  $L = \{1, 2, 4, 5, 10, 20\}$  with divisibility relation.

As seen earlier (Ex. 4, page 18-25), the elements 2, 10 have no complements.

$\therefore L$  is not a complemented lattice.

**EXERCISE - V**

1. In the previous Exercise - III, page 18-22 show that the lattices given in Ex. 1, 2, 3, 4, 5, 6 and 9 are complemented, while those given in Ex. 7 and 8 are not complemented.

2. Show that the lattice shown in Fig. 18.43 is neither distributive nor complemented. (M.U. 1998)

3. Show that the lattice shown in Fig. 18.44 is distributive but not complemented. (M.U. 2002, 07)

4. Show that the lattice shown in Fig. 18.45 is neither distributive nor complemented. (M.U. 2002, 07)

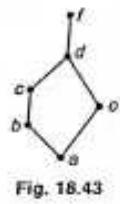


Fig. 18.43

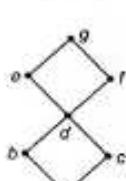


Fig. 18.45

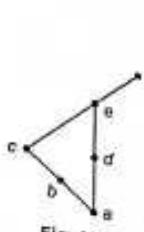
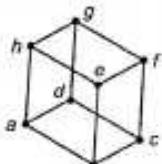


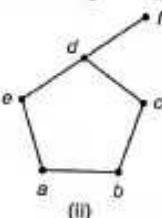
Fig. 18.46

**EXERCISE - VI**

State with justification which of the following are lattices.



(i)



(ii)

[ Ans. : (i) Yes, (ii) No ]

**5. Boolean Lattice and Boolean Algebra**Let  $(L, \leq)$  be a lattice, A complemented lattice and distributive lattice is called a Boolean Lattice.**(a) Boolean Lattice**Since every element belongs to boolean lattice has unique complement, so we define a unary operation on  $L$  denoted by symbol ' $\neg$ ', so that for every element ' $a$ ' in  $L$  ' $\bar{a}$ ' is the complement of ' $a$ '. The unary operation ' $\neg$ ' is called as complementation operation.Thus, a boolean lattice  $(L, \leq)$  defines an algebraic system  $(L, \vee, \wedge, \neg)$  is known as Boolean Algebra where  $\vee$  = join operation,  $\wedge$  = meet operation and  $\neg$  = complementation operation.A Boolean algebra will generally denoted by  $(L, \vee, \wedge, \neg, 0, 1)$  alternatively  $(L, +, *, \bar{\cdot}, 0, 1)$  in which  $(L, \vee, \wedge)$  or  $(L, +, *)$  is lattice with two binary operations. The corresponding poset will be denoted by  $(L, \leq)$  and the bounds of lattice are '0' and '1' least and greatest element of  $(L, \leq)$  respectively. Since,  $(L, \vee, \wedge)$  is distributive lattice each element of  $L$  has unique complement, we denote complementation operation by ' $\neg$ ' (or ' $\bar{\cdot}$ ').**(b) De Morgan's Law**Theorem : If  $(L, \leq, \neg, 0, 1)$  is a Boolean lattice, then (i)  $\overline{a \wedge b} = \bar{a} \vee \bar{b}$ , and (ii)  $\overline{a \vee b} = \bar{a} \wedge \bar{b}$ .Proof : Let  $a, b$  be any elements belongs to  $L$ . We will show that  $\bar{a} \vee \bar{b}$  acts like the complement of  $a \wedge b$ .By uniqueness of complement  $\overline{a \wedge b} = \bar{a} \vee \bar{b}$  and  $\overline{a \vee b} = \bar{a} \wedge \bar{b}$ .

$$\text{Let } (a \wedge b) \wedge (\bar{a} \vee \bar{b}) = (a \wedge b \wedge \bar{a}) \vee (a \wedge b \wedge \bar{b}) \\ = [(a \wedge \bar{a}) \wedge b] \vee [a \wedge (\bar{b} \wedge \bar{b})] \\ = [0 \wedge b] \vee [a \wedge 0] \\ = 0 \vee 0 = 0$$

$$\text{Now, } (a \wedge b) \vee (\bar{a} \vee \bar{b}) = [(a \wedge b) \vee \bar{a}] \vee \bar{b} \\ = [(a \vee \bar{a}) \wedge (b \vee \bar{a})] \vee \bar{b} \\ = [1 \wedge (b \vee \bar{a})] \vee \bar{b} \\ = (b \vee \bar{a}) \vee \bar{b} = (b \vee \bar{b}) \vee \bar{a} \\ = 1 \vee \bar{a} = 1$$

A complement of an element  $a$  is  $\bar{a}$  such that  $a \wedge \bar{a} = 0$  and  $a \vee \bar{a} = 1$ .  
Therefore,  $\bar{a} \vee \bar{b}$  is a complement of  $a \wedge b$  i.e.,  $\overline{a \wedge b} = \bar{a} \vee \bar{b}$ .

Similarly, it is possible to show  $\overline{a \vee b} = \bar{a} \wedge \bar{b}$ .  
We summaries all the basis properties of Boolean algebra  $(L, \vee, \wedge, \neg, 0, 1)$ . Also we list the corresponding properties for subsets of a finite set  $S$  with the relation ' $\subseteq$ ' recall  $(P(S), \subseteq)$  is a lattice and is boolean lattice having universal upper bound  $S$  and lower bound  $\Phi$  and complement  $\bar{S}$  ( $\bar{S}'$ ).

**(d) Properties**Let  $a, b, c$  are the elements in  $L$  and  $A, B, C$  be subsets of  $S$ . Denote greatest and least element of  $L$  by  $I$  and  $O$  respectively.

- |  |   |
|--|---|
| 1. $a \leq b$ iff $a \vee b = b$   | (I) $A \subseteq B$ iff $A \cup B = B$  |
| 2. $a \leq b$ iff $a \wedge b = a$   | (II) $A \subseteq B$ iff $A \cap B = A$   |
| 3. (i) $a \vee a = a$<br>(ii) $a \wedge a = a$   | (III) (i) $A \cup A = A$<br>(ii) $A \cap A = A$   |
| 4. (i) $a \vee a = b \vee a$<br>(ii) $a \wedge b = b \wedge a$   | (IV) (i) $A \cup B = B \cup A$<br>(ii) $A \cap A = A$   |
| 5. (i) $a \vee (b \vee c) = (a \vee b) \vee c$<br>(ii) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ | (V) (i) $A \cup (B \cup C) = (A \cup B) \cup C$<br>(ii) $A \cap (B \cap C) = (A \cap B) \cap C$ |
| 6. (i) $a \vee (a \wedge b) = a$<br>(ii) $a \wedge (a \vee b) = a$                                     | (VI) (i) $A \cup (A \cap B) = A$<br>(ii) $A \cap (A \cup B) = A$                                |
| 7. $0 \leq a \leq 1$   | (VII) (i) $A \cup \Phi = A$<br>(ii) $A \cap \Phi = \Phi$  |
| (i) $a \vee 0 = a$<br>(ii) $a \wedge 0 = 0$  | (VIII) (i) $A \cup S = S$<br>(ii) $A \cap S = A$  |
| 8. (i) $a \vee 1 = 1$<br>(ii) $a \wedge 1 = a$   | (IX) (i) $A \cup \bar{A} = S$<br>(ii) $A \cap \bar{A} = \Phi$                                   |
| 9. (i) $a \wedge a' = 0$<br>(ii) $a \vee a' = 1$<br>(iii) $0' = 1$<br>(iv) $1' = 0$                    | (X) (i) $\bar{S} = S$<br>(ii) $\bar{\Phi} = \Phi$   |

10. (i)  $(a \wedge b)' = a' \vee b'$   
(ii)  $(a \vee b)' = a' \wedge b'$

11.  $(L, \leq)$  poset, then

(i)  $a \wedge b = \text{glb}\{a, b\}$

(ii)  $a \vee b = \text{lub}\{a, b\}$

(iii)  $a \leq b$  iff  $a \wedge b = a$  iff  $a \vee b = b$

(iv)  $a \leq b$  iff  $a \wedge b' = 0$  iff  $b' \leq a'$  iff  $a' \vee b = 1$

12. (i)  $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ ; (X)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$   
(ii)  $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ ;  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Thus, to show at a lattice  $L$  is not a Boolean Algebra it is sufficient to show it does not possess one or more properties.

#### (d) Properties of Boolean Algebra

1. Idempotent :  $x + x = x$  and  $x \cdot x = x$
2. Identity :  $x + 0 = x$  and  $x \cdot 1 = x$
3. Dominance :  $x + 1 = 1$  and  $x \cdot 0 = 0$
4. Commutativity :  $x + y = y + x$  and  $x \cdot y = y \cdot x$
5. Distributivity :  $x + (y \cdot z) = (x + y) \cdot (x + z)$  and  $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
6. Associativity :  $(x + y) + z = x + (y + z)$  and  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
7. Complement :  $x + \bar{x} = 1$  and  $x \cdot \bar{x} = 0$
8. Double negation :  $\overline{\overline{x}} = x$
9. De Morgan's law :  $\overline{x + y} = \bar{x} \cdot \bar{y}$  and  $\overline{(x \cdot y)} = \bar{x} + \bar{y}$
10. Redundancy :  $x + \bar{x} \cdot y = x + y$  and  $x \cdot (\bar{x} + y) = x \cdot y$

Example 1 : Prove that (i)  $a \wedge a = a$ , (ii)  $a \vee a = a$ .

Sol. : (i) Let  $a = a \wedge 1$  (ii) Let  $a = a \vee 0$   
 $= a \wedge (a \vee a')$   $= a \vee (a \wedge a')$   
 $= (a \wedge a) \vee (a \wedge a')$   $= (a \vee a) \wedge (a \vee a')$   
 $= a \wedge 0$   $= a \wedge 1$   
 $= a$   $= a$

Example 2 : Prove that (i)  $a \vee 1 = 1$ , (ii)  $a \wedge 0 = 0$ .

Sol. : (i)  $a \vee 1 = (a \vee 1) \wedge 1$  (ii)  $a \wedge 0 = (a \wedge 0) \vee 0$   
 $= (a \vee 1) \wedge (a \vee a')$   $= (a \wedge 0) \vee (a \wedge a')$   
 $= a \vee (1 \wedge a')$   $= a \wedge (0 \vee a')$   
 $= a \vee a'$   $= a \wedge a'$   
 $= 1$   $= 0$

Example 3 : Prove that  $(a \vee b) \vee c = a \vee (b \vee c)$ .

Sol. : Let  $a \vee (b \vee c)$ . From the definition of lub, we have  $a \leq a \vee (b \vee c)$  and  $b \vee c \leq a \vee (b \vee c)$  moreover  $b \leq b \vee c$  and  $c \leq b \vee c$ .

(X) (i)  $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$   
(ii)  $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$

Lattices

So by transitivity,  $b \leq a \vee (b \vee c)$  and  $c \leq a \vee (b \vee c)$ ,  
thus,  $a \vee (b \vee c)$  is an upperbound of  $a$  and  $b$ , so by definition of lub

$$a \vee b \leq a \vee (b \vee c)$$

Now, since  $a \vee (b \vee c)$  is an upper bound of  $a \vee b$  and  $c$ , we obtain,  
 $(a \vee b) \vee c \leq a \vee (b \vee c)$

$$(a \vee b) \vee c \leq (a \vee b) \vee c$$

Similarly,  $a \vee (b \vee c) \leq (a \vee b) \vee c$

By antisymmetry of  $\leq$  property,  
 $(a \vee b) \vee c = a \vee (b \vee c)$

Example 4 : In a Boolean algebra  $(B, \wedge, \vee, ', 0, 1)$ . Prove that if  $x \wedge y' = 0$ , then  $x \wedge y = x$  for all

$x, y \in B$ .

Given  $x \wedge y' = 0$   
Sol. : Now,  $x = x \wedge 1$   
 $\therefore x = x \wedge (y \vee y')$   
 $= (x \wedge y) \vee (x \wedge y')$   
 $= (x \wedge y) \vee 0$  [ By hypothesis ]  
 $= x \wedge y$

Example 5 : Let  $(B, \wedge, \vee, ', 0, 1)$  be a Boolean algebra and  $a \in B$  be any element. Let  $x, y \in B$  be elements such that  $a \wedge x = a \wedge y$  and  $a' \wedge x = a' \wedge y$ . Prove that  $x = y$ .

Sol. : We have  $x = x \wedge 1$   
 $= x \wedge (a \vee a')$   
 $= (x \wedge a) \vee (x \wedge a')$   
 $= (a \wedge x) \vee (a' \wedge x)$   
 $= (a \wedge x) \vee (a' \wedge y)$  [ By hypothesis ]  
 $= y \wedge (a \vee a')$   
 $= y \wedge (1)$   
 $= y$

Example 6 : Simplify the following Boolean expressions :

(1)  $(A + B)(A + C)$ , (2)  $A + A\bar{A}$ , (3)  $AB + A\bar{B}$ , (4)  $AB + AB'C + AB'C'$

Sol. : (1)  $(A + B)(A + C) = AA + AC + BA + BC$

$$= A(1 + C) + BA + BC$$

$$= A(1) + BA + BC$$

$$= A + BA + BC$$

$$= A(1 + B) + BC$$

$$= A(1) + BC$$

$$= A + BC$$

(2)  $A + A\bar{A} = A(1 + \bar{A})$

$$= A(1)$$

[ Since if  $A = 0$ , then  $\bar{A} = 1$  and  $1 + 1 = 1$  ]

$$= A$$

$$(3) AB + A\bar{B} = A(B + \bar{B}) \\ = A(1) \\ = A$$

Observe truth table column of  $A$  and  $F$  is same output, it is not affecting of  $B$ .

$$(4) AB + AB'C + AB'C' \\ = A[B + B'C + B'C'] \\ = A[B + B'(C + C')] \\ = A[B + B'(1)] \quad \dots [A + A' = 1] \\ = A[B + B'] \\ = A[1] \\ = A$$

Lattice		
A	B	$F = AB + AB'$
0	0	0
0	1	0
1	0	0
1	1	1

Truth Table

**EXERCISE - VII**

- Simplify the following Boolean expressions.
  - $A \cdot B + A' \cdot C + B \cdot C$  [Reduction property]
  - $(A + B + C)(A + B' + C)(A + B + C')$   
(Hint : Use distributive law.)
  - $(A + B)(A + B')(A' + B)(A' + B')$
- Prove the following Boolean identities.
  - $a \vee (a' \wedge b) = a \vee b$
  - $a \wedge (a' \vee b) = a \wedge b$
  - $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$
  - $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$
- In a Boolean algebra  $(B, \wedge, \vee, ', 0, 1)$ , prove that if  $x \vee y' = 1$ , then  $x \wedge y = x$ .
- In a Boolean algebra,  $(B, \wedge, \vee, ', 0, 1)$  prove that
  - If  $x \wedge y = 0$  then  $x \wedge y' = x$
  - If  $x \vee y = 1$  then  $x \vee y' = x$
  - $x \wedge (x' \vee y) = x \wedge y$
  - $x' \wedge (x \vee y) = x' \wedge y$
  - $x \vee (x' \wedge y) = x \vee y$
  - $x' \vee (x \wedge y) = x' \vee y$
- Prove that In a Boolean algebra  $(B, \wedge, \vee, ', 0, 1)$ , if  $a, x, y \in B$  and  $a \vee x = a \vee y$  and  $a' \vee x = a' \vee y$ , then  $x = y$ .
- In a Boolean algebra  $B$  for any  $x, y, z$ , prove that the following :
  - $(x + y') + xz = x + y'$  or  $(x \vee y') \vee (x \wedge z) = x \vee y'$
  - $xy + xy' = x$  or  $x \wedge y + x \wedge y' = x$
  - $x + x'y = x + y$  or  $x \vee (x' \wedge y) = x \vee y$
- Simplify the following Boolean expressions :
  - $(x \vee y) \wedge (x \vee z) \vee (x' \vee y')$
  - $[x \vee (y \wedge (z \vee x'))]'$
  - $(x \wedge (y' \vee z)) \vee z'$

**Finite Boolean Algebra**

A finite Boolean algebra is one with a finite number of elements. It is possible to show that a finite Boolean algebra has exactly  $2^n$  elements for some  $n > 0$ . Moreover there is a unique Boolean algebra of  $2^n$  elements for every  $n > 0$ .

Illustrative example : Investigate the structure of the Boolean lattice  $L$  of order 8 given in Fig. 18.128, this is essentially the power set of a 3 element set labeled differently.

Sol. Since  $L$  is a finite Boolean lattice, it can be divided into  $n$  different levels. Let say the bottom level where the minimum 0 is located level 0, the next level up elements above 0 Level 1 and so on. Here  $L$  is 3 levels above 0. The atoms of the lattice at level 1 are  $a, b$  and  $c$ . These atoms generate the lattice above it via the operation ' $\vee$ '.

Level 2 of lattice  $L$  consists of elements  $d, e, f$ . Note that these  $2^3 = 8$  elements are all possible joins  $\vee$  of the atoms and are  $a \vee b, a \vee c$  and  $b \vee c$ .

Level 3 consists only of the maximum element 1. It lies directly above all the elements on level 2. Just as importantly, it can be thought of as the ' $\vee$ ' of atoms taken together as  $a \vee b \vee c$  and  $a \vee b \vee c \vee 1 = 1$ . Way to denote the elements have uses triplet binary notation for indicating the elements representing the elements as power set of  $S$ , viz.,  $S = \{p, q, r\}$ .

The example generalises to any finite Boolean lattice. This turns out to severely restrict the structure of finite Boolean lattice, they are all of cardinality  $2^n$  for some  $n$ .

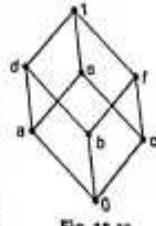


Fig. 18.128

**i) Boolean Expressions**

Let  $(L, \vee, \wedge, \neg)$  be a Boolean algebra. A Boolean expression over  $(L, \vee, \wedge, \neg)$  is defined as follows :

- Any element of  $L$  is a Boolean expression.
- Any variable name is a Boolean expression.
- If  $E_1$  and  $E_2$  are Boolean expressions, then  $\neg E_1, E_1 \vee E_2, E_1 \wedge E_2$  are Boolean expressions.

For example, consider Boolean algebra  $(\{0, 1, 2\}, \vee, \wedge, \neg)$ ,  $a \in L$ . Now,  $0', 0 \vee a, 1 \wedge 2, 1 \vee 0$  are Boolean expressions.

**ii) Boolean Functions and Boolean Expressions**

Theorem : Let  $(L, \vee, \wedge, \neg)$  be a finite Boolean algebra. Let  $S$  be the set of atoms. Then  $(L, \vee, \wedge, \neg)$  is isomorphic to the algebraic system defined by the lattice  $(\mathcal{P}(S), \subseteq)$ .

It follows immediately from above theorem that, there exists a unique finite Boolean algebra of  $2^n$  elements for  $n > 0$ , moreover there are no other finite Boolean algebra.

Let  $(L, \vee, \wedge, \neg)$  be a Boolean algebra. Let the function from  $L^n$  to  $L$ , for example,  $f: \{0, 1\}^3 \rightarrow \{0, 1\}$  shown in the adjoining Table 4.1 on the next page.

Also function from  $\{0, 1, 2, 3\}^2$  to  $\{0, 1, 2, 3\}$  shows as shown in Table 4.2 on the next page.

Alternative ways of describing function by closed-form expression.

Let  $E(x_1, x_2, \dots, x_n)$  be a Boolean expression of  $n$  variables over a Boolean algebra  $(L, \vee, \wedge, \neg)$ . By an assignment values to the variables  $x_1, x_2, \dots, x_n$  we mean an assignment of elements of  $L$  to the values of the variables. For an assignment of values to the variables we can evaluate the expression  $E(x_1, x_2, x_3, \dots, x_n)$  by substituting the variables in the expression by their values. e.g., for the Boolean expression

Table 18.1

	$f$
(0, 0, 0)	0
(0, 0, 1)	0
(0, 1, 0)	1
(0, 1, 1)	0
(1, 0, 0)	1
(1, 0, 1)	1
(1, 1, 0)	0
(1, 1, 1)	1

Table 18.2

	$f$
(0, 0)	1
(0, 1)	0
(0, 2)	0
(0, 3)	3
(1, 0)	1
(1, 1)	1
(1, 2)	0
(1, 3)	3
(2, 0)	2
(2, 1)	0
(2, 2)	1
(2, 3)	1
(3, 0)	3
(3, 1)	0
(3, 2)	0
(3, 3)	2

$$E(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (\bar{x}_1 \vee \bar{x}_2) \wedge (x_2 \vee x_3)$$

over the Boolean algebra  $\{(0, 1), \vee, \wedge, \neg\}$  the assignment values  $x_1 = 0, x_2 = 1, x_3 = 0$  yields,

$$\begin{aligned} E(0, 1, 0) &= (0 \vee 1) \wedge (\bar{0} \vee \bar{1}) \wedge (1 \vee 0) \\ &= 1 \wedge 1 \wedge 0 \\ &= 0 \end{aligned}$$

Two Boolean expressions of  $n$  variables are said to be equivalent if they assume the same value for every assignment of values to the  $n$  variables e.g.,  $(x_1 \wedge x_2) \vee (x_1 \wedge \bar{x}_3)$  is equivalent to  $x_1 \wedge (x_2 \vee \bar{x}_3)$ . We write as

$$E_1(x_1, x_2, \dots, x_n) = E_2(x_1, x_2, \dots, x_n)$$

means  $E_1$  and  $E_2$  two expressions are equivalent.

### (c) Boolean Function

A function  $f: B^n \rightarrow B$  can be viewed as a function  $f(x_1, x_2, \dots, x_n)$  of  $n$  variables each of which may assume the value 0 or 1. Suppose that  $x_k$  represents propositions and the function  $f(x_1, x_2, \dots, x_n)$  represents a compound statements constructed from the  $x_k$ 's. If we think 0 for false statement and 1 for true statement.

**Definition :** Any function  $f: B^n \rightarrow B$  is called Boolean function of  $n$  Boolean variables  $x_1, x_2, \dots, x_n$ .

**Example :** If  $B = \{0, 1\}$ , then  $f: B^2 \rightarrow B$ ,  $f(x_1, x_2) = x_1' + x_2$  is a Boolean function of two variables  $x_1$  and  $x_2$ .

Here,  $B^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$

Let  $f(x_1, x_2) = x_1' + x_2$ . Therefore,

$$\begin{aligned} f(0, 0) &= 0' + 0 = 1 + 0 = 1, & f(0, 1) &= 0' + 1 = 1 + 1 = 1, \\ f(1, 0) &= 1' + 0 = 0 + 0 = 0, & f(1, 1) &= 1' + 1 = 0 + 1 = 1 \end{aligned}$$

**Definition :** Any expression involving Boolean variables  $(x_1, x_2, \dots, x_n) \in B^n$  and possibly two elements of  $B$  is called a Boolean Expression in  $B$ .

(i)  $(x_1 + x_2)$  and (ii)  $(x_1 + x_2')(x_3' + 0) = 1$  are Boolean expressions 2 and 3 variables respectively.

**Note ...** Every Boolean expression in  $n$ -variables defines Boolean function in  $n$ -variables. Every Boolean expression defines a Boolean function.

For example,  $f: B^2 \rightarrow B$  where domain of a Boolean function is a set of  $n$ -tuples of  $\{0, 1\}$  whose co-domain or range is an element of the basic Boolean set  $\{0, 1\}$ .

Consider the Boolean function  $f(x, y) = (x \wedge y) \vee (x' \wedge y')$  where  $x, y$  are Boolean variables. The function  $f(x, y)$  computes the compound statement containing ' $\wedge$ ' or ' $\vee$ '.

**Truth Table :** the Boolean function can be represented by using truth tables, where the values of Boolean function are obtained by putting 0 and 1 for the variables in the expression. The following table displays function  $f$ .

$x$	$y$	$x \wedge y$	$x' \wedge y'$	$f(x, y) = (x \wedge y) \vee (x' \wedge y')$
0	0	0	0	0
0	1	0	1	1
1	0	0	0	0
1	1	1	0	1

**Example 1 :** Consider the Boolean expression  $f(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \vee (x_2' \wedge x_3))$ . construct the truth table for the Boolean function  $f: B^3 \rightarrow B$ , determined by this Boolean expression.

**Sol. :** The Boolean function  $f: B^3 \rightarrow B$  is described by substituting all the  $2^3$  ordered triples of values from  $B$  for  $x_1, x_2$  and  $x_3$ . The truth table for the resulting function is as below.

$x_1$	$x_2$	$x_3$	$f(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \vee (x_2' \wedge x_3))$
0	0	0	0
0	0	1	1
0	1	0	0
1	0	0	1
0	1	1	0
1	0	1	1
1	1	0	1
1	1	1	1

**Example 2 :** Consider Boolean expression  $E(x, y, z) = (x \wedge y) \vee (y \wedge z)$ . If  $B = \{0, 1\}$ , compute the truth table of the function  $f: B^3 \rightarrow B$  defined by  $E$ .

**Sol. :**  $f: B^3 \rightarrow B$  is  $f(x, y, z) = (x \wedge y) \vee (y \wedge z)$

$x$	$y$	$z$	$(x \wedge y)$	$(y \wedge z)$	$f(x, y, z) = (x \wedge y) \vee (y \wedge z)$
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	0	0
1	0	0	0	1	1
0	1	1	0	0	0
1	0	1	0	0	0
1	1	0	1	1	0
1	1	1	1	0	1

**Example 3 :** Construct the truth table for the Boolean expression.

$$E(x_1, x_2, x_3) = (x_1 + x_2) \cdot (x_1 + (x_2 \cdot x_3))$$

**Sol. :** Truth table for given Boolean expression is as below :

$x_1$	$x_2$	$x_3$	$x_1 + x_2$	$x_1'$	$x_2 \cdot x_3'$	$x_1 + (x_2 \cdot x_3')$	$E$
1	1	1	1	0	0	1	1
1	1	0	1	1	1	1	1
1	0	1	1	0	0	1	1
1	0	0	1	1	0	1	1
0	1	1	1	0	0	0	0
1	1	0	1	1	1	1	1
0	0	1	0	0	0	0	0
0	0	0	0	1	0	0	0

**Example 4 :** Let the Boolean expression  $E(x, y, z) = x \wedge (y \vee z')$ . If  $B = \{0, 1\}$ , compute the truth table of the function  $f : B^3 \rightarrow B$  defined by  $E$ .

**Sol. :** Let  $E(x, y, z) = x \wedge (y \vee z')$ .

The Boolean function  $f : B^3 \rightarrow B$  is described by substituting all the  $2^3$  ordered triples of values from  $B = \{0, 1\}$  for  $x, y, z$ . The resulting truth table is as below.

$x$	$y$	$z$	$z'$	$y \vee z'$	$f(x, y, z) = x \wedge (y \vee z')$
0	0	0	1	1	0
0	0	1	0	0	0
0	1	0	1	1	0
1	0	0	1	1	1
0	1	1	0	1	0
1	0	1	0	0	0
1	1	0	1	1	1
1	1	1	0	1	1

**Definition :** Let  $x$  be a Boolean variable. A symbol  $x^*$  which stands for  $x$  or  $x'$  is called literal.

This,  $x \cdot x^*$  is a product of literals. It represents any one of the following 4 products,

$x_1 x_2, x_1 x_2', x_1' x_2, x_1' x_2'$

**Definition :** A meet (product) of literals in which no two literals involve the same variable is called fundamental product.

For example, (i)  $x, x', xy', x'yz'$  are fundamental products.

(ii)  $x'yz, xyzx$  are not fundamental products.

Since, in  $x'yx$ , the literal  $x$  and  $x'$  corresponds to the same  $x$ . In  $xyzx$ , we clearly see that  $x$  is repeated.

Note that any Boolean product is reducible to either 0 or a fundamental product. If a variable  $x$  and its complement  $x'$  is repeated, the product reduces to 0 ( $xx' = 0$ ). If a variable  $x$  is repeated in product, then by idempotency, it reduces to  $x$  ( $xxx = x$ ).

**Definition :** A Boolean expression is called a sum-of-product form or minterm form, if it is a fundamental product or sum of fundamental products none of which is included in another.

**Example 1 :** Express into sum-of-product form the following Boolean expression.

$$((xy)^* z)' ((x' + z)(y' + z'))'$$

**Sol.:** Step 1 : Remove complement operation into parenthesis, then

$$\begin{aligned} \text{Expression} &= ((xy)^* + z') ((x' + z)' + (y' + z')') \\ &= ((xy)^* + z') ((xz') + (yz)) \end{aligned}$$

**Step 2 :** Use distributive laws to transform the expression into sum of products, then

$$\begin{aligned} \text{Expression} &= (xy) ((xz') + (xz)) + (y' ((xz') + (xz))) \\ &= ((xy)(xz')) + ((xy)(xz)) + (z'(xz')) + (z'(xz)) \end{aligned}$$

**Step 3 :** Use commutativity, idempotent laws, complementation, etc. to get a sum of fundamental products, then

$$\begin{aligned} \text{Expression} &= (xyz') + (xyz) + (xz') + (0) \\ &= (xyz') + (xyz) + (xz') \end{aligned}$$

**Step 4 :** Use absorption law to remove a fundamental product contained in another fundamental product, then

$$\begin{aligned} \text{Expression} &= [(xyz') + (xz')] + (xyz) \\ &= (xz') + (xyz) \end{aligned}$$

This is required sum of product form.

**Example 2 :** Express following expression in the sum-of-product form.

$$E = (x + y)' xz + yz$$

$$\begin{aligned} \text{Sol. : } \text{Expression} &= (x + y)' xz + yz \\ &= (x' y') xz + yz \quad [\text{By DeMorgan's law}] \\ &= y' (x' x) z + yz \quad [\text{Commutativity and Associativity}] \\ &= y' (0) z + yz \quad [\text{Complement}] \\ &= 0 + yz = yz \end{aligned}$$

**Example 3 :** Express the following Boolean expression into complete sum-of-product form.

**Sol. :** A Boolean expression is said to be complete sum-of-product form if it is (i) in sum-of-product form, and (ii) each product term contains all the variables.

$$\begin{aligned} \text{Expression} &= (x+y)(x'+y') \\ &= x(x'+y') + y(x'+y') \\ &= xx' + xy' + x'y + yy' \\ &= 0 + xy' + x'y + 0 \\ &= xy' + x'y \end{aligned}$$

## 7. Propositional Calculus

**Proposition :** A proposition is a declarative statement that is either true or false.

Two or more existing propositions can be combined to yield new proposition by using logical operators.

### (1) Negation

**Definition :** A negation is a compound statement obtained by negating a simple statement.

We denote the negation of a statement by putting  $\sim$  (curl) before it. Thus, the negation of  $p$  is  $\sim p$ . It is clear that if  $p$  is true then  $\sim p$  is false and if  $p$  is false then  $\sim p$  is true. We have, therefore, the truth table given on the right.

Thus, a negation is true if the statement is false and false otherwise.

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

### (2) Conjunction

**Definition :** A conjunction is a compound statement obtained by combining two simple statements by 'and' (or its equivalent).

Thus, the conjunction of 'Gold is yellow' and 'Iron is black' is 'Gold is yellow and Iron is black'. Such a statement is called a conjunction and its component statements are called conjuncts. If  $p$  and  $q$  are two statements we denote their conjunction by putting  $\wedge$  between them as  $p \wedge q$ . Depending upon the truth value of  $p$  and  $q$  there are four possibilities for the truth value of  $p \wedge q$ . They are:

If  $p$  is true and  $q$  is true,  $p \wedge q$  is true,

If  $p$  is true and  $q$  is false,  $p \wedge q$  is false,

If  $p$  is false and  $q$  is true,  $p \wedge q$  is false,

If  $p$  is false and  $q$  is false,  $p \wedge q$  is false.

Thus, we have the following truth-table for conjunction.

Thus, a conjunction is true if and only if both conjuncts are true and false otherwise.

### (3) Disjunction

**Definition :** A disjunction is a compound statement obtained by combining two simple statements by 'or' (or its equivalent).

Thus, the disjunction of "Rama was cruel" and "Ravan was guilty" is "Rama was cruel or Ravan was guilty." Such a statement is called a disjunction and the component statements are

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

two disjuncts. If  $p$  and  $q$  are two statements, their disjunction is denoted by putting  $\vee$  (vol) between  $p$  and  $q$ . Depending upon the truth values of  $p$  and  $q$  there are four possibilities for the truth value of  $p \vee q$ . They are :

If  $p$  is true and  $q$  is false,  $p \vee q$  is true,

If  $p$  is false and  $q$  is true,  $p \vee q$  is true,

If  $p$  is false and  $q$  is false,  $p \vee q$  is false.

Thus, we have the following truth table for disjunction.

Thus, disjunction is false if and only if both disjuncts are false and true otherwise.

Let an algebraic system  $\langle \{F, T\}, \vee, \wedge, \neg \rangle$  where definitions of operations  $\vee, \wedge, \neg$  are as shown in the adjoining tables.

$\langle \{F, T\}, \vee, \wedge, \neg \rangle$  is a Boolean algebra of two elements within such an algebraic framework, an atomic proposition is a variable that can assume either the value F (false) or the value T (true). Tautology is T and contradiction is F. The disjunction of two propositions  $p$  and  $q$  is denoted by algebraic expression  $p \vee q$ . The definition of disjunction is consistent with the definition of two propositions  $p$  and  $q$  (shown above tables).

Similarly, the conjunction ( $\wedge$ ) of  $p$  and  $q$  propositions can be represented by  $p \wedge q$  and negation of  $p$  by  $\neg p$ . The definition of ' $\wedge$ ' and ' $\neg$ ' are consistent with that of conjunction and negation of proposition as above.

Every Boolean term corresponds to a propositional formula of propositional logic. e.g.,  $p \vee q, p \wedge q, p', \dots$  Application of propositional calculus is the analysis of propositions and deductive arguments in natural language.

An axiomatization of propositional calculus is a set of tautologies called axioms and one or more inference rules for producing new tautologies from old.

## EXERCISE - VIII

1. If  $B = \{0, 1\}$  is a Boolean algebra, determine Boolean functions defined by following Boolean expressions.

(i)  $x' \wedge y$ , (ii)  $x' \vee z$

2. Construct a truth table for the following :

(i)  $xy + x\bar{y} + \bar{x}z$ , (ii)  $x\bar{y} + xy$

(iii)  $xyz + \bar{x}\bar{y}z$ , (iv)  $x\bar{y} + y\bar{z} + z\bar{x}$

3. Construct a function for two variables whose truth table is given below.

(i)	$x$	$y$	$f_1$
0	0	0	0
0	1	0	0
1	0	1	1
1	1	0	0

[Ans. :  $f_1 = x\bar{y}$ ]

(ii)	$x$	$y$	$f_2$
0	0	1	1
0	1	0	0
1	0	1	1
1	1	1	1

[Ans. :  $f_2 = x + \bar{y}$ ]

x	y	$f_3$
0	0	1
0	1	0
1	0	0
1	1	1

[ Ans. :  $f_3 = xy + \bar{x}\bar{y}$  ]

x	y	$f(x, y)$
0	0	1
0	1	1
1	0	0
1	1	0

[ Ans. :  $f(x, y) = x^2 = (x' \wedge y') \vee (x' \wedge y)$  ]

4. Express the following expressions in the sum-of-product forms.
- $(x+y)(x+z)(x'y)$
  - $(a+b'c)(b+c')$
  - $x_1 + x_2$
  - $(x_1 + x_2)' + (x_1' \cdot x_3)$
  - $x + \bar{y}z + \bar{x}y$  (- indicate ')
- $(x+y)(z+x')$
  - $(x+y)'xz + yz$
  - $x_1 + (x_2 x_3)'$
  - $xy + xz + yz$
  - $xy + yz'$
5. Express the following in complete sum-of-product form.
- $E = (x' + y' + y'z)$
  - $E = C(A' + B) + B'$
  - $E = z(x' + y) + y'$
  - $E(x, y, z) = (x+y')' + yz'$
  - $E(x, y, z) = (x'+y)' + xz$
  - $(x'+y)' + xy + x'yz$

### EXERCISE - IX

#### Theory

- Explain the terms : Lattice.
- Define distributive Lattice and complemented Lattice.  
Give an example. (M.U. 1999, 2013)
- Let  $L$  be a distributive Lattice. Show that if a complement exists then it is unique. (M.U. 2014, 16)



(18-39)

(iv)

x	y	$f_4$
0	0	0
0	1	1
1	0	1
1	1	1

[ Ans. :  $f_4 = x + y$  or  $f_4 = xy + x\bar{y} + \bar{x}y$  ]

Lattice



## Coding Theory

### 1. Coding : Introduction

A word is a sequence of letters carrying some meaning. For example, 'o-x-a-m-p-i-e' is a sequence of letters o, x, a, m, p, i, e. If the sequence changes to e.g. 'm a x e l p e' it may not carry any meaning or if new letters appears instead of the desired one e.g. 'e t a m p s e' then also it may not carry any meaning. When a message is transmitted over a long distance there may be some interference because of which the sequence may change and the message may not be received exactly as it was sent. In such situations we desire to detect the errors and if possible rectify them. In ordinary language. This is possible on many occasions though not always because some arrangements of letters do not have any meaning and from the context we can correct the error. For example, if the message sent is "happy birth day" and if it is received as "happy dirth bay" we can easily find out the error.

Suppose we decide to send a message in terms of 0 and 1 by using a code. (i.e. a system of symbols 0 and 1). Suppose we decide the code to represent

A	by	00
B	by	01
C	by	10
D	by	11

then the word 'cab' can be sent as "10 00 01". But if it is received as "11 00 01" it will mean 'dab' or if it is received as "01 00 11", it will mean 'bad'. The problem obviously then is how to find out the error and if possible how to correct it. If we decide to use 0, 1 to represent a word then the only error possible is 0 will be received as 1 or 1 will be received as 0.

We have seen above that in transmitting data, interference from external sources such as noise may cause an error in transmission. As a result the data received may be different from data transmitted. In the binary code it is possible to detect an error and even to correct it as explained below.

Consider the codes  $C_2$  with two digits,  $C_3$  with three digits and  $C_6$  with six digits. Suppose further that we use the following codes for the words given

Code	Words			
	small	large	tall	short
$C_2$	00	10	01	11
$C_3$	000	110	011	101
$C_6$	000000	111000	001110	110011

In the code  $C_2$  if the message sent is 00 and the message received is 10, it means the word transmitted is "small" but the word received is exactly the opposite "large". This happens because both words "00" and "10" belong to the code. The receiver in this case will not be able to detect the

error. He will think that the word transmitted was "large" as it is received. He has no way to know that the received word is wrong.

In the code  $C_3$  if the message sent is '110' and the message received is '100' it means the word transmitted is 'large' but the word (100) received is not in the code. Thus, the error is detected. This code can detect any one error but it cannot correct it. In practice, error detection without error correction is useful only when the receiver can ask for repetition of the message when the error is detected.

The code  $C_6$  can detect and also correct the message in some cases. If there is only one error in the received message it is possible to detect and correct the error. Suppose the word received is 010000 which is not in the code. The only code word which can be obtained by altering one bit is 000000. Thus, we can infer that the message sent was "small". We can in this way detect and correct an error of one digit.

As seen above if we can send our message in terms of 0 and 1, there is a possibility to detect an error and also in some cases correct it.

Hence, the set  $B = \{0, 1\}$  is our basic unit of information. A word then will be a sequence of some 0's and 1's.

If a word has  $n$  0's and 1's then the word is said to be of length  $n$ . It is convenient to use words of the same length in a given case. We shall denote the complete set of all words of length  $n$  by  $V^n$ . Naturally in  $V^n$  there will be  $2^n$  words. For example,

$$\begin{aligned} B &= \{0, 1\} \\ B^2 &= \{00, 01, 10, 11\} \\ B^3 &= \{000, 001, 010, 011, 100, 101, 110, 111\} \\ &\dots \\ B^n &= \{000\dots0, 000\dots1, \dots, 111\dots1\} \end{aligned} \quad (1)$$

The set  $B = \{0, 1\}$  is a group under the binary operation + whose table is shown below.

+	0	1
0	0	1
1	1	0

(A)

In other words,  $B$  is a group under addition mod 2. It can be proved that  $B^n = B \times B \times \dots \times B$  ( $n$  times) is a group under addition. The identity of this group is  $\bar{0} = (0, 0, \dots, 0)$  and every element is its inverse. We shall denote an element of the group  $B^n$  by  $(b_1, b_2, \dots, b_n)$  or by  $b_1, b_2, \dots, b_n$ . We shall say that the order of the group  $B^n$  is  $n$ .

In order to reduce the possibility of error in transmission i.e. the possibility of receiving a different word than the word sent we define a new function called encoding function.

#### (a) Encoding Function

**Definition :** If an integer  $n > m$  and if there is one to one correspondence  $e : B^m \rightarrow B^n$  then  $e$  is called an  $(m, n)$  encoding function. In this way every word in  $B^m$  is represented by a word in  $B^n$ . If  $b \in B^m$  then  $e(b)$  is called the code word representing  $b$ .

Since  $n > m$  there will be some more 0's and 1's in  $e(b)$  than in  $b$ . These additional zeros and ones help us to detect and correct the errors as seen earlier in an example.

**Weight :** If a word  $x \in B^n$  then the number of 1's in  $x$  is called the weight of  $x$  and is denoted by  $|x|$ .

**Example 1 :** Find the weights of each of the following words in  $B^5$ .

- (i)  $x = 00100$       (ii)  $x = 01010$       (iii)  $x = 00000$       (iv)  $x = 11110$

sol: (i)  $|x| = 1$ , (ii)  $|x| = 2$ , (iii)  $|x| = 0$ , (iv)  $|x| = 4$ .

#### (b) Parity Check Code

**Definition :** The encoding function  $e : B^m \rightarrow B^{m+1}$  is called parity  $(m, m+1)$  check code, if  $b = b_1, b_2, \dots, b_m \in B^m$  defines

$$e(b) = b_1, b_2, \dots, b_m, b_{m+1} \quad \text{where } b_{m+1} = \begin{cases} 0, & \text{if } |b| \text{ is even} \\ 1, & \text{if } |b| \text{ is odd} \end{cases}$$

The encoding function defined above enables us to detect an error. We first observe that  $b_{m+1} = 0$  if and only if the number of 1's in  $b$  is an even number i.e. every code word  $e(b)$  has even weight. A single error in transmission of a code word will change the received word to a word of odd weight and as such can be detected. Similarly,  $b_{m+1} = 1$  if and only if the number of 1's in  $b$  is an odd number i.e. every code word  $e(b)$  has odd weight. A single error in transmission of a code word will change the received word to a word of even degree and thus error can be detected.

**Example 1 :** Consider the  $(3, 4)$  parity check code. For each of the following received words, determine whether an error will be detected.

- (i) 0100,      (ii) 1100

sol: (i) Since  $x_1 = 0100$ ,  $|x_1| = 1$   
Since  $|x_1|$  is odd, the last digit should have been 1 but it is zero and hence there is an error.  
∴ The error is detected.

- (ii) Since  $x_1 = 1100$ ,  $|x_1| = 2$

Since  $|x_1|$  is even, the last digit should have been zero and it is zero.  
∴ The error cannot be detected.

**Example 2 :** Consider the  $(3, 4)$  parity check code for  $m = 3$ .

$$\begin{array}{lll} e(b) = x & e(000) = 0000 & e(001) = 0011 \\ e(010) = 0101 & e(011) = 0110 & e(100) = 1001 \\ e(101) = 1010 & e(110) = 1100 & e(111) = 1111 \end{array}$$

Can you detect an error if  $b = 001$  and  $e(b) = 0111$ ?

sol: Since  $b = 001$ ,  $e(b) = 0111$ .

But by data  $e(b) = 0111$  and  $|x_1| = 3$ . Hence, odd number of errors (at least one) has occurred.

It should be noted that if the received word is of even weight then we cannot conclude that the code word was transmitted correctly, since this encoding function does not detect even number of errors. Still the parity check is widely used.

#### EXERCISE - I

1. Find the weights of the words given below.

- (i) 1011      (ii) 1110      (iii) 0110      (iv) 010101      (v) 111111  
[Ans. : (i) 3, (ii) 3, (iii) 2, (iv) 3, (v) 3, (vi) 6.]

2. Consider (3, 4) parity check code. For each of the following received words find whether an error will be detected.
- (i) 0010    (ii) 1001    (iii) 1101    (iv) 1010    (v) 1111    (vi) 0011  
 { Ans. : (i) Yes, (ii) No, (iii) Yes, (iv) No, (v) No, (vi) No }
3. Consider the (6, 7) parity check code. For each of the following received words, find whether an error will be detected.
- (i) 1101010    (ii) 011111    (iii) 1010011    (iv) 1001101  
 { Ans. : (i) No, (ii) Yes, (iii) No, (iv) No }

## 2. Group Codes, Decoding and Error Correction

So far we have not made use of the fact that  $(B^n, \oplus)$  is a group. Now we shall consider an encoding function  $e$  that makes use of this property. First we shall define the term group code.

### (a) Group Code

**Definition :** An  $(m, n)$  coding function  $e : B^m \rightarrow B^n$  is called a **group code** if  
 $e(B^m) = \{ e(b) | b \in B^m \}$       (M.U. 1999, 2000, 05)  
 $= \text{Range } (e)$

is a subgroup of  $B^n$ .

To prove that a given encoding function is a group code we have to show that (i) the identity element of  $B^n$  is in  $N$ , (ii) if  $x, y$  belong to  $N$  then  $x \oplus y$  belongs to  $N$ , (iii) if  $x$  is in  $N$  then its inverse is in  $N$ .

We need not check (iii) because every element of  $B^n$  is its inverse.

**Example 1 :** Show that the (2, 5) encoding function  $e : B^2 \rightarrow B^5$  defined by  
 $e(00) = 00000, \quad e(01) = 01110, \quad e(10) = 10101, \quad e(11) = 11011$

is a group code.

**Sol. :** Let  $N = \{00000, 01110, 10101, 11011\}$ . We have to show that  $N$  is a subgroup of  $B^5$ . We shall now prepare the following table for  $B^5$ .

We prepare the following table by using the table (A) given on page 19-2 i.e., by using  
 $0+0=0, 0+1=1, 1+0=0$  and  $1+1=0$ .

For example,  $01110 + 10101 = 11011; \quad 11011 + 01110 = 10101$

$\oplus$	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

(i) From the diagonal elements of the above table we see that the identity (00000) of  $B^5$  is in  $N$ .

(ii) From the table we see that if  $x, y$  belong to  $N$  then  $x \oplus y$  also belongs to  $N$ .

(iii) Every element is its inverse.

$\therefore N$  is a subgroup of  $B^5$  and the given encoding function is a group code.

Example 2 : Consider (3, 6) encoding function defined below.

$$\begin{aligned} e(000) &= 000110, & e(010) &= 010010, \\ e(011) &= 010100, & e(100) &= 100101, \\ e(110) &= 110111, & e(111) &= 110001. \end{aligned}$$

Show that the encoding function is a group code.

(M.U. 1998)

Let  $N = \{000000, 000110, 010010, 010100, 100101, 100011, 110111, 110000\}$

We have to show that  $N$  is a subgroup of  $B^6$ .

We shall now prepare the following table for  $B^6$ .

$\oplus$	000000	000110	010010	010100	100101	100011	110111	110001
000000	000000	000110	010010	010100	100101	100011	110111	110001
000110	000110	000000	010100	010010	000110	110111	110001	100101
010010	010010	010100	000000	000110	000000	110001	110111	100011
010100	010100	010010	000110	000000	110001	000000	000110	010100
100101	100101	100011	110111	110001	000000	000110	010100	010010
100011	100011	100101	110001	110111	000110	000000	010100	000110
110111	110111	110001	100101	100011	010010	010100	000000	000110
110001	110001	110111	100011	100101	010100	010010	000110	000000

(i) From the diagonal elements of the above table we see that the identity (000000) of  $B^6$  is in  $N$ .

(ii) From the table we see that if  $x, y$  belong to  $N$  then  $x \oplus y$  belongs to  $N$ .

(iii) Every element is its inverse.

$\therefore N$  is a subgroup of  $B^6$  and the given encoding function is a group code.

### b) Hamming Distance

**Definition :** If  $x, y$  are words in  $B^m$  then the weight of  $x \oplus y$  i.e.  $|x \oplus y|$  is called the Hamming

distance between  $x$  and  $y$  and is denoted by  $d(x, y)$ . In other words, the distance between  $x = x_1, x_2, \dots, x_m$  and  $y = y_1, y_2, \dots, y_m$  is the number of values of  $i$  such that  $x_i \neq y_i$  i.e. the number of positions in which  $x$  and  $y$  differ. The weight of  $x \oplus y$  helps us to find the number of different positions.

**Example 1 :** Find the distance between  $x$  and  $y$  where

$$(i) x = 110110, \quad y = 000101; \quad (ii) x = 001100, \quad y = 010110$$

Sol :  $x \oplus y$  is obtained from the table

+	0	1
0	0	1
1	1	0

for every digit.

$$(i) x \oplus y = \frac{110110}{000101} \quad \therefore |x \oplus y| = 4$$

$$(ii) x \oplus y = \frac{001100}{010110} \quad \therefore |x \oplus y| = 3$$

**Example 2 :** Find the distance between  $x$  and  $y$  where  
 (i)  $x = 1100010$ ,  $y = 1010011$ ;      (ii)  $x = 0100100$ ,  $y = 0011010$

Sol.: As explained above.

$$\begin{aligned} \text{(i)} \quad x \oplus y &= 0110001 \quad \therefore |x \oplus y| = 3 \\ \text{(ii)} \quad x \oplus y &= 0111110 \quad \therefore |x \oplus y| = 5 \end{aligned}$$

(c) **Theorem (Properties of Hamming Distance)**

Let  $x, y, z$  be elements of  $B^m$ , then

- (a)  $\delta(x, y) = \delta(y, x)$
- (b)  $\delta(x, y) \geq 0$
- (c)  $\delta(x, y) = 0$  if and only if  $x = y$
- (d)  $\delta(x, y) \leq \delta(x, z) + \delta(z, y)$

Sol.: (i) By definition,

$$\delta(x, y) = |x \oplus y|$$

$$\text{By the same definition, } \delta(y, x) = |y \oplus x|$$

$$\text{Since } |x \oplus y| = |y \oplus x| \text{ an integer}$$

$$\text{(ii) Since } \delta(x, y) = |x \oplus y| \quad \delta(x, y) = \delta(y, x)$$

$$\text{(iii) Clearly, } \delta(x, x) = 0 \quad \delta(x, y) \geq 0$$

$$\text{(iv) For } a, b \in B^m \quad |a \oplus b| \leq |a| + |b|$$

Since at any position where  $a$  and  $b$  differ one of them must contain a 1.

Further, if  $a \in B^m$  then  $a \oplus a = \bar{0}$ , the identity element in  $B^m$ .

$$\therefore \delta(x, y) = |x \oplus y| = |x \oplus \bar{0} \oplus y|$$

$$= |x \oplus z + z \oplus y|$$

$$\leq |x \oplus z| + |z \oplus y|$$

$$\therefore \delta(x, y) \leq \delta(x, z) + \delta(z, y) \quad [\text{By (1)}]$$

(d) **Minimum Distance**

**Definition :** Let  $e : B^m \rightarrow B^n$  be a coding function. The minimum of the distance between all pairs of distinct code words is called the **minimum distance** of the code.

Symbolically,  $\min \left\{ [e(x), e(y)] / x, y \in B^m \right\}$  is called the minimum distance of the code.

**Example 1 :** Consider the following (2, 5) encoding function  $e$ .

$$\left. \begin{array}{l} e(00) = 00000 \\ e(10) = 00111 \\ e(01) = 01110 \\ e(11) = 11111 \end{array} \right\} \text{Code words}$$

Find the minimum distance of the code.

Sol.: If we denote these words as  $x, y, z$  and  $u$  then

$$\delta(x, y) = 3, \quad \delta(x, z) = 3, \quad \delta(x, u) = 5,$$

$$\delta(y, z) = 2, \quad \delta(y, u) = 2, \quad \delta(z, u) = 2.$$

$\therefore$  Minimum distance of  $e = 2$ .

**Theorem**  
An  $(m, n)$  coding function  $e : B^m \rightarrow B^n$  can detect  $k$  or less errors if and only if its minimum distance is at least  $k+1$ .  
We shall accept this theorem without proof but will illustrate it through an example.

**Example 1 :** Consider the (2, 4) encoding function. How many errors can it detect ?

$$\left. \begin{array}{l} e(00) = 0000 \\ e(10) = 0110 \\ e(01) = 1011 \\ e(11) = 1100 \end{array} \right\} \text{Code words}$$

Sol.: Let  $x, y, z, u$  denote the words. Then the distances are given by

$$\delta(x, y) = \delta(0000, 0110) = 2, \quad \delta(x, z) = \delta(0000, 1011) = 3,$$

$$\delta(x, u) = \delta(0000, 1100) = 2, \quad \delta(y, z) = \delta(0110, 1011) = 3,$$

$$\delta(y, u) = \delta(0110, 1100) = 2, \quad \delta(z, u) = \delta(1011, 1100) = 3.$$

$$\therefore \text{Minimum distance} = 2 \quad \therefore k+1 = 2 \quad \therefore k = 1$$

The code will detect 1 or less errors.

**Example 2 :** Consider (2, 6) encoding function  $e : B^2 \rightarrow B^6$  defined as

$$\left. \begin{array}{l} e(0, 0) = 000000 \\ e(0, 1) = 011110 \\ e(1, 0) = 101010 \\ e(1, 1) = 111000 \end{array} \right\}$$

(i) Find the minimum distance of the code.

(ii) How many errors can be detected ?

(M.U. 2006, 08, 11, 12)

Sol.: (i) If we denote the words by  $x, y, z$  and  $u$  then

$$\delta(x, y) = \delta(000000, 011110) = 4, \quad \delta(x, z) = \delta(000000, 101010) = 3,$$

$$\delta(x, u) = \delta(000000, 111000) = 3, \quad \delta(y, z) = \delta(011110, 101010) = 3,$$

$$\delta(y, u) = \delta(011110, 111000) = 3, \quad \delta(z, u) = \delta(101010, 111000) = 3.$$

$\therefore$  The minimum distance is 3. Since the minimum distance is 3,

$$k+1 = 3 \quad \therefore k = 2.$$

The coding function can detect  $k = 2$  or less errors.

**Example 3 :** Consider the following (3, 8) encoding function  $e : B^3 \rightarrow B^8$  defined by

$$\left. \begin{array}{l} e(000) = 00000000 \\ e(001) = 10111000 \\ e(010) = 00101101 \\ e(011) = 10010101 \\ e(100) = 10100100 \\ e(101) = 10001001 \\ e(110) = 00011100 \\ e(111) = 00110001 \end{array} \right\} \text{Code words}$$

How many errors can  $e$  detect ?

Sol.: There will be  ${}^8C_2 = 28$  pairs of code words. The minimum distance is 3. By the above theorem if minimum distance is  $k+1 = 3$ , then the coding function can detect  $2 = k$  or less errors.

**Example 4 :** Show that (3, 7) encoding function  $e$  defined below is a group code.

$e(000) = 0000000,$	$e(001) = 0010110,$	$e(010) = 0101000,$
$e(011) = 0111110,$	$e(100) = 1000101,$	$e(101) = 1010011,$
$e(110) = 1101101,$	$e(111) = 1111011,$	

How many errors can it detect?

Sol. :

⊕	0000000	0010110	0101000	0111110	1000101	1010011	1101101	1111011
0000000	0000000	0010110	0101000	0111110	1000101	1010011	1101101	1111011
0010110	0000000	0111110	0101000	1010011	1000101	1101101	1111011	
0101000	0101000	0111110	0000000	0010110	1101101	1111011	1101101	
0111110	0111110	0101000	0010110	0000000	1111011	1000101	1010011	
1000101	1000101	1010011	1101101	1111011	1101101	1010011	1000101	
1010011	1010011	1000111	1111011	1101101	0010110	0101000	0111110	
1101101	1101101	1111011	1010011	0000000	0010110	0111110	0101000	
1111011	1111011	1101101	1000111	0111110	0101000	0010110	0000000	

(M.U. 2005, 07)

- (i) From the diagonal elements of the above table we see that (0000000) is an identity and it belongs to  $N$ .
- (ii) From the table we also see that if  $x, y$  belong to  $N$  then  $x \oplus y$  belongs to  $N$ .
- (iii) Every element is its inverse.

$\therefore N$  is a subgroup of  $B^7$  and the given encoding function is a group code. The minimum distance is 2. Hence, the code can detect 1 or less errors.

**Example 5 :** Consider the following (3, 9) encoding function  $e$ .

$$\begin{aligned} e(000) &= 000000000, \\ e(001) &= 011100101, \\ e(010) &= 010101000, \\ e(011) &= 110010001, \\ e(100) &= 010011010, \\ e(101) &= 111101011, \\ e(110) &= 001011000, \\ e(111) &= 110000111. \end{aligned}$$

Find the minimum distance. How many errors can it detect?

Sol. : It can be seen that the minimum distance is 3.  
Hence,  $e$  can detect 2 or less errors.

(M.U. 2002)

### EXERCISE - II

t. Consider the (3, 6) encoding function  $e : B^3 \rightarrow B^6$  defined by

$e(000) = 000000,$	$e(001) = 001100,$	$e(010) = 010011,$
$e(011) = 011111,$	$e(100) = 100101,$	$e(101) = 101001,$
$e(110) = 110110,$	$e(111) = 111010.$	

Show that the encoding function is a group code.

2. Find the minimum distance of the following (2, 4) encoding function [Ans. : 2]

$$e(00) = 0000, \quad e(10) = 0110, \quad e(01) = 1011, \quad e(11) = 1100.$$

3. Consider the following (2, 6) encoding function  $e$ .

$$e(00) = 000000, \quad e(10) = 101010, \quad e(01) = 011110, \quad e(11) = 111000$$

(a) Find the minimum distance of  $e$ . (b) How many errors will  $e$  detect?

(M.U. 2008) [Ans. : (a) 2, (b) 1]

### 1 Mod-2 Boolean Product

**Definition :** If  $D = [d_{ij}]$  is an  $m \times p$  Boolean matrix (matrix whose elements are 0 and 1) and  $E = [e_{ij}]$  is a  $p \times n$  Boolean matrix then we define a product  $D * E$  called the mod-2 Boolean product as the  $m \times n$  matrix  $F$  where

$$f_{ij} = d_{i1} \cdot e_{1j} + d_{i2} \cdot e_{2j} + \dots + d_{ip} \cdot e_{pj}, \quad 1 \leq i \leq m, 1 \leq j \leq n$$

Example 1 : Find the mod-2 Boolean product of the following two Boolean matrices

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Sol. : First we note that

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \text{ and } \begin{array}{c|cc} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

We take the product of the above matrices as usual and use the above results.

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 0 & 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 \\ 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 & 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 \end{bmatrix} = \begin{bmatrix} 1+1+0 & 0+1+0 \\ 0+1+0 & 0+1+1 \end{bmatrix}$$

(But  $1 \cdot 1 = 1$  and  $1 + 1 = 0$ .)

Hence, we get

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

We thus note that if an odd number of corresponding pairs consist of two 1's then the product is 1 and if an even number of corresponding pairs consist of two 1's then the product is zero.

Mod-2 Boolean product in general terms is shown below.

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1p} \\ a_{21} & a_{22} & \dots & a_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rp} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mp} \end{bmatrix} * \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{p1} & b_{p2} & \dots & b_{pn} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{bmatrix}$$

↓

$$\begin{bmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{1p} \end{bmatrix} \begin{bmatrix} b_{11} \\ b_{12} \\ \vdots \\ b_{1n} \end{bmatrix} \quad \begin{bmatrix} a_{21} \\ a_{22} \\ \vdots \\ a_{2p} \end{bmatrix} \begin{bmatrix} b_{21} \\ b_{22} \\ \vdots \\ b_{2n} \end{bmatrix} \quad \dots \quad \begin{bmatrix} a_{m1} \\ a_{m2} \\ \vdots \\ a_{mp} \end{bmatrix} \begin{bmatrix} b_{m1} \\ b_{m2} \\ \vdots \\ b_{mn} \end{bmatrix}$$

If an odd number of corresponding pairs consists of two 1's, then  $c_y = 1$  and if an even number of corresponding pairs consists of two 1's, then  $c_y = 0$

### (b) Parity Check Matrix

**Definition :** Let  $m < n$  and  $r = n - m$ . An  $n \times r$  Boolean matrix  $H$  given by

$$H = \begin{cases} \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1r} \\ h_{21} & h_{22} & \dots & h_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ h_{m1} & h_{m2} & \dots & h_{mr} \end{bmatrix} \\ n-m = r \text{ rows} \begin{cases} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{cases} \end{cases} \quad (A)$$

where last  $r$  rows form the  $r \times r$  identity matrix is called a parity check matrix.

The parity check matrix  $H$  defined above is used to define an encoding function  $e_H : B^m \rightarrow B^n$  as illustrated in the following examples.

If  $b = b_1, b_2, \dots, b_m$ ,

let  $x = e_H(b) = b_1, b_2, \dots, b_m, x_1, x_2, \dots, x_r$  ..... (1)

where,  $x_1 = b_1 \cdot h_{11} + b_2 \cdot h_{21} + \dots + b_m \cdot h_{m1}$

$x_2 = b_1 \cdot h_{12} + b_2 \cdot h_{22} + \dots + b_m \cdot h_{m2}$

$\dots$

$x_r = b_1 \cdot h_{1r} + b_2 \cdot h_{2r} + \dots + b_m \cdot h_{mr}$  ..... (2)

Example 1 : Consider the parity matrix  $H$  given by

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Determine the group code  $e_H : B^2 \rightarrow B^5$ .  
Since  $B = \{0, 1\}$ , we have  $B^2 = \{00, 01, 10, 11\}$ . [ See (I), page 19-2 ]

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

$$e_H(00) = 00 x_1 x_2 x_3$$

where  $x_1 x_2 x_3$  are given by the following equations

$$x_1 = b_1 h_{11} + b_2 h_{21}$$

$$x_2 = b_1 h_{12} + b_2 h_{22}$$

$$x_3 = b_1 h_{13} + b_2 h_{23}$$

From the given matrix  $H$ , [ Comparing (A) and (B) ]

$$h_{11} = 1, h_{12} = 1, h_{13} = 0; \quad h_{21} = 0, h_{22} = 1, h_{23} = 1;$$

$$h_{31} = 1, h_{32} = 0, h_{33} = 0; \quad h_{41} = 0, h_{42} = 1, h_{43} = 0;$$

$$h_{51} = 0, h_{52} = 0, h_{53} = 1.$$

and from (3),  $b_1 = 0, b_2 = 0$ .

Putting these values in (C), we get

$$x_1 = 0 \cdot 1 + 0 \cdot 0 = 0; \quad x_2 = 0 \cdot 1 + 0 \cdot 1 = 0; \quad x_3 = 0 \cdot 0 + 0 \cdot 1 = 0$$

$$\therefore e(00) = 00 x_1 x_2 x_3 = 00000 \text{ where } b_1 = 0, b_2 = 0$$

$$\text{Further, } e(10) = 10 x_1 x_2 x_3 \text{ where } (b_1 = 1, b_2 = 0)$$

$$x_1 = 1 \cdot 1 + 0 \cdot 0 = 1; \quad x_2 = 1 \cdot 1 + 0 \cdot 1 = 1; \quad x_3 = 1 \cdot 0 + 0 \cdot 1 = 0$$

$$\therefore e(10) = 10110$$

$$\text{Again } e(01) = 01 x_1 x_2 x_3 \text{ where } (b_1 = 0, b_2 = 1)$$

$$x_1 = 0 \cdot 1 + 1 \cdot 0 = 0; \quad x_2 = 0 \cdot 1 + 1 \cdot 1 = 1; \quad x_3 = 0 \cdot 0 + 1 \cdot 1 = 1$$

$$\therefore e(01) = 01011$$

$$\text{Lastly } e(11) = 11 x_1 x_2 x_3 \text{ where } (b_1 = 1, b_2 = 1)$$

$$x_1 = 1 \cdot 1 + 1 \cdot 0 = 1; \quad x_2 = 1 \cdot 1 + 1 \cdot 1 = 0; \quad x_3 = 1 \cdot 0 + 1 \cdot 1 = 1$$

$$\therefore e(11) = 11101$$

The group code function  $e_H : B^2 \rightarrow B^5$  is

$$e(00) = 00000, \quad e(01) = 01011,$$

$$e(10) = 10110, \quad e(11) = 01011.$$

Example 2 : Consider the parity matrix  $X$  given by

$$X = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Determine  $(2, 5)$  group code function  $e_H: B^2 \rightarrow B^5$ .  
Sol.: Since  $B = \{0, 1\}$ , we have  $B^2 = \{00, 01, 10, 11\}$ .

As in Example 1, from (1) and (2), page 19-10, we get  
 $e_H(00) = 0 \ 0 \ x_1 \ x_2 \ x_3$  where  $b_1 = 0, b_2 = 0$   
where  $x_1, x_2, x_3$  are given by the following equations:

$$x_1 = b_1 h_{11} + b_2 h_{21}$$

$$x_2 = b_1 h_{12} + b_2 h_{22}$$

$$x_3 = b_1 h_{13} + b_2 h_{23}$$

But from the given matrix  $H$ ,

$$h_{11} = 0, \quad h_{12} = 1, \quad h_{13} = 1, \quad h_{21} = 0, \quad h_{22} = 1, \quad h_{23} = 1,$$

$$h_{31} = 1, \quad h_{32} = 0, \quad h_{33} = 0, \quad h_{41} = 0, \quad h_{42} = 1, \quad h_{43} = 0,$$

$$h_{51} = 0, \quad h_{52} = 0, \quad h_{53} = 1 \quad \text{and from (3), } b_1 = 0, b_2 = 0.$$

Putting these values in (A), we get

$$x_1 = 0 \cdot 0 + 0 \cdot 0 = 0, \quad x_2 = 0 \cdot 1 + 0 \cdot 1 = 0, \quad x_3 = 0 \cdot 1 + 0 \cdot 1 = 0.$$

Hence, from (3), we get

$$e(00) = 0 \ 0 \ 0 \ 0 \ 0 \quad \text{where } b_1 = 0, b_2 = 0.$$

Further,  $e(01) = 0 \ 1 \ x_1 \ x_2 \ x_3$  where  $b_1 = 0, b_2 = 1$ .

$$x_1 = 0 \cdot 0 + 1 \cdot 0 = 0, \quad x_2 = 0 \cdot 1 + 1 \cdot 1 = 1, \quad x_3 = 0 \cdot 1 + 1 \cdot 1 = 1,$$

$$\therefore e(01) = 0 \ 1 \ 0 \ 1 \ 1$$

Further,  $e(10) = 1 \ 0 \ x_1 \ x_2 \ x_3$  where  $b_1 = 1, b_2 = 0$ .

$$x_1 = 1 \cdot 0 + 0 \cdot 0 = 0, \quad x_2 = 1 \cdot 1 + 0 \cdot 1 = 1, \quad x_3 = 1 \cdot 1 + 0 \cdot 1 = 1,$$

$$\therefore e(10) = 1 \ 0 \ 0 \ 1 \ 1$$

Further,  $e(11) = 1 \ 1 \ x_1 \ x_2 \ x_3$  where  $b_1 = 1, b_2 = 1$ .

$$x_1 = 1 \cdot 0 + 1 \cdot 0 = 0, \quad x_2 = 1 \cdot 1 + 1 \cdot 1 = 0, \quad x_3 = 1 \cdot 1 + 1 \cdot 1 = 0,$$

$$\therefore e(11) = 1 \ 1 \ 0 \ 0 \ 0$$

Hence, the group code function,  $e_H: B^2 \rightarrow B^5$  is

$$e(00) = 0 \ 0 \ 0 \ 0 \ 0, \quad e(01) = 0 \ 1 \ 0 \ 1 \ 1,$$

$$e(10) = 1 \ 0 \ 0 \ 1 \ 1, \quad e(11) = 1 \ 1 \ 0 \ 0 \ 0.$$

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Example 3 : Let  $H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$  be parity check matrix.

Determine the group code  $e_H: B^2 \rightarrow B^5$ .

Sol.: Since  $B = \{0, 1\}$ , we have  $B^2 = \{00, 01, 10, 11\}$ .

As in Example 2, from (1) and (2), page 19-10, we get

$$e_H(00) = 0 \ 0 \ x_1 \ x_2 \ x_3 \quad \text{where } b_1 = 0, b_2 = 0$$

where  $x_1, x_2, x_3$  are given by the following equations,

$$x_1 = b_1 h_{11} + b_2 h_{21}$$

$$x_2 = b_1 h_{12} + b_2 h_{22}$$

$$x_3 = b_1 h_{13} + b_2 h_{23}$$

$$\text{Get from the given matrix } H,$$

$$h_{11} = 1, \quad h_{12} = 0, \quad h_{13} = 0, \quad h_{21} = 1, \quad h_{22} = 1, \quad h_{23} = 0,$$

$$h_{31} = 0, \quad h_{32} = 1, \quad h_{33} = 1, \quad h_{41} = 1, \quad h_{42} = 0, \quad h_{43} = 0,$$

$$h_{51} = 0, \quad h_{52} = 1, \quad h_{53} = 0, \quad h_{61} = 0, \quad h_{62} = 0, \quad h_{63} = 1$$

$$h_{71} = 0, \quad h_{72} = 0, \quad h_{73} = 0.$$

Put these values in (A), we get

$$x_1 = 0 \cdot 1 + 0 \cdot 1 = 0, \quad x_2 = 0 \cdot 0 + 0 \cdot 1 = 0, \quad x_3 = 0 \cdot 0 + 0 \cdot 0 = 0.$$

Hence, from (3), we get

$$e(00) = 0 \ 0 \ 0 \ 0 \ 0 \quad \text{where } b_1 = 0, b_2 = 0.$$

Further,  $e(01) = 0 \ 1 \ x_1 \ x_2 \ x_3$  where  $b_1 = 0, b_2 = 1$ .

$$x_1 = 0 \cdot 1 + 1 \cdot 1 = 1, \quad x_2 = 0 \cdot 0 + 1 \cdot 1 = 1, \quad x_3 = 0 \cdot 0 + 1 \cdot 0 = 0,$$

$$\therefore e(01) = 0 \ 1 \ 1 \ 1 \ 0 \quad \text{where } b_1 = 0, b_2 = 1.$$

Further,  $e(10) = 1 \ 0 \ x_1 \ x_2 \ x_3$  where  $b_1 = 1, b_2 = 0$ .

$$x_1 = 1 \cdot 1 + 0 \cdot 1 = 1, \quad x_2 = 1 \cdot 0 + 0 \cdot 1 = 0, \quad x_3 = 1 \cdot 0 + 0 \cdot 0 = 0,$$

$$\therefore e(10) = 1 \ 0 \ 1 \ 0 \ 0 \quad \text{where } b_1 = 1, b_2 = 0.$$

Further,  $e(11) = 1 \ 1 \ x_1 \ x_2 \ x_3$  where  $b_1 = 1, b_2 = 1$ .

$$x_1 = 1 \cdot 1 + 1 \cdot 1 = 0, \quad x_2 = 1 \cdot 0 + 1 \cdot 1 = 1, \quad x_3 = 1 \cdot 0 + 1 \cdot 0 = 0,$$

$$\therefore e(11) = 1 \ 1 \ 0 \ 1 \ 0 \quad \text{where } b_1 = 1, b_2 = 1.$$

Hence, the group code function,  $e_H: B^2 \rightarrow B^5$  is

$$e(00) = 0 \ 0 \ 0 \ 0 \ 0, \quad e(01) = 0 \ 1 \ 1 \ 1 \ 0,$$

$$e(10) = 1 \ 0 \ 1 \ 0 \ 0, \quad e(11) = 1 \ 1 \ 0 \ 1 \ 0.$$

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Example 4 : Let  $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$  be a parity check matrix.

$b_{11} = 1, b_{12} = 0, b_{13} = 0,$   
 $b_{21} = 0, b_{22} = 1, b_{23} = 1,$   
 $b_{31} = 1, b_{32} = 1, b_{33} = 1$   
and  $b_1 = 0, b_2 = 0, b_3 = 0.$

Putting these values in (E), we get

$$x_1 = 0 \cdot 1 + 0 \cdot 0 + 0 \cdot 1 = 0;$$

$$x_2 = 0 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0$$

Further  $e(001) = 001 x_1 x_2 x_3$  where

$$x_1 = 0 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 = 1;$$

$$x_3 = 0 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1$$

And  $e(010) = 010 x_1 x_2 x_3$  where

$$x_1 = 0 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 = 0;$$

$$x_3 = 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1$$

And  $e(011) = 011 x_1 x_2 x_3$  where

$$x_1 = 0 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 = 1;$$

$$x_3 = 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0$$

And  $e(100) = 100 x_1 x_2 x_3$  where

$$x_1 = 1 \cdot 1 + 0 \cdot 0 + 0 \cdot 1 = 1;$$

$$x_3 = 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0$$

And  $e(101) = 101 x_1 x_2 x_3$  where

$$x_1 = 1 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 = 0;$$

$$x_3 = 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1$$

And  $e(110) = 110 x_1 x_2 x_3$  where

$$x_1 = 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 = 1;$$

$$x_3 = 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1$$

Lastly  $e(111) = 111 x_1 x_2 x_3$  where

$$x_1 = 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 = 0;$$

$$x_3 = 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0$$

$$\therefore e(000) = 000000$$

$$\therefore e(001) = 001111$$

$$\therefore e(010) = 010100$$

$$\therefore e(011) = 011100$$

$$\therefore e(100) = 100100$$

$$\therefore e(101) = 101011$$

$$\therefore e(110) = 110111$$

$$\therefore e(111) = 111000$$

Hence, the group code function,  $e_H : B^3 \rightarrow B^6$  is

$$e(000) = 000000, \quad e(001) = 001111,$$

$$e(010) = 010100, \quad e(011) = 011100,$$

$$e(100) = 100100, \quad e(101) = 101011,$$

$$e(110) = 110111, \quad e(111) = 111000.$$

### EXERCISE - III

1. Let  $H = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$  be a parity check matrix.

Find the (2, 5) group code function  $e_H : B^2 \rightarrow B^5$ .

[Ans.:  $e(00) = 00000, \quad e(01) = 01011, \quad e(10) = 10011, \quad e(11) = 11000$ ]

#### 4. Maximum Likelihood Decoding Technique

It is natural to expect a decoding function when an encoding function is given. When an  $(m, n)$  encoding function  $e : B^m \rightarrow B^n$  is given we can find  $(n, m)$  decoding function  $d : B^n \rightarrow B^m$  associated with  $e$ .

Definition : The technique used to find  $d$  from  $e$  is known as maximum likelihood technique.

Without going into theoretical part of maximum likelihood technique we shall learn the procedure of obtaining maximum likelihood decoding function with  $e$ .

##### Procedure To Prepare Decoding Table

In the first row write all given encoded words starting from 000 ... 00.

2. Then in the first column write the words with weight 1 viz. 00001, 00010, 00100 and so on.

3. Then take the sum of the word on the left and the word at the top and write it in the table.

and in this way fill up the table.

4. Underline the word to be decoded and find the column.

5. Note the word at the top in that column.

6. Decode that word and thus get the required result.

The following examples will make the procedure easy to understand.

Example 1 : Consider (2, 5) group encoding function  $e : B^2 \rightarrow B^5$  defined by

$$e(00) = 00000, \quad e(01) = 01110, \quad e(10) = 10101, \quad e(11) = 11011$$

Decode the following words relative to maximum likelihood function

$$(i) 11110, (ii) 10011, (iii) 10100.$$

(M.U. 2007)

Sol. : We first prepare the blank table in which in the first row we write encoded words 00000, 01110, 10101 and 11011.

In the first column we write the words with minimum weight 1 i.e. we write in the first column, 00001, 00010, 00100, 01000, 10000.

##### Blank Decoding Table

00000	01110	10101	11011
00001			
00010			
00100			
01000			
10000			

Now we take the sum of the words in 2nd, 3rd and 4th column and the word in each row successively.

Thus, we have  $01110 + 00001 = 01111$ , we enter this sum under 01110. Then we take the sum  $10101 + 00001 = 10100$  and enter it under 10101 and continuing in this way we fill up the table and get the following.

Decoding Table			
00000	01110	10101	11011
00001	01111	10100	11010
00010	01100	10111	11001
00100	01010	10001	11111
01000	00110	11101	<u>10011</u>
10000	<u>11110</u>	00101	01011

- (i) The received word 11110 is in the second column and is underlined. The word at the top in its column is 01110.  
Since by data  $e(01) = 01110$ , we decode 11110 as 01 i.e.,  $d(11110) = 01$ .
- (ii) The received word 10011 is in the fourth column and is underlined. The word at the top in its column is 11011.  
Since by data  $e(11) = 11011$ , we decode 10011 as 11 i.e.,  $d(10011) = 11$ .
- (iii) The received word 10100 is in the third column and is underlined. The word at the top is 10101.  
Since by data  $e(10) = 10101$ , we decode 10100 as 10 i.e.,  $d(10100) = 10$ .

**Example 2 :** Consider (2, 6) group encoding function  $e : B^2 \rightarrow B^6$  defined by  
 $e(00) = 000000; e(01) = 011110; e(10) = 101101; e(11) = 110011.$

Decode the following relative to maximum likelihood decoding function.

(i) 001110, (ii) 111101, (iii) 110010

(M.U. 2012)

**Sol. :** We first prepare a blank table in which we write encoded words 000000, 011110, 101101, 110011 in the first row. Now we write the words with minimum weight in the first column and prepare a blank table.

Decoding Table			
000000	011110	101101	110011
00001	011110	101100	<u>110010</u>
00010	011100	101111	110001
00100	011010	101001	110111
01000	010110	100101	111011
010000	<u>001110</u>	<u>111101</u>	100011
10000	111110	001101	010011

As explained in the previous example, we get

$$d(001110) = 01, \quad d(111101) = 10, \quad d(110010) = 11.$$

**Example 3 :** Let  $H = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$  be a parity check matrix.

Decode the following words relative to maximum likelihood decoding function.

(i) 0101, (ii) 1010, (iii) 1101.

(M.U. 2003, 07)

**Sol. :** First we compute the encoding function  $e_H : B^2 \rightarrow B^4$ .  
We have  $B^2 = \{00, 01, 10, 11\}$

$$e(00) = 00 \ x_1 \ x_2$$

$$\therefore x_1 = 0 \cdot 1 + 0 \cdot 1 = 0, \quad x_2 = 0 \cdot 1 + 0 \cdot 0 = 0$$

$$\therefore e(00) = 0000$$

$$\text{Next } e(01) = 01 \ x_1 \ x_2$$

$$\therefore x_1 = 0 \cdot 1 + 1 \cdot 1 = 1, \quad x_2 = 0 \cdot 1 + 1 \cdot 1 = 0$$

$$\therefore e(01) = 0110$$

$$\text{Next } e(10) = 10 \ x_1 \ x_2$$

$$\therefore x_1 = 1 \cdot 1 + 0 \cdot 1 = 1, \quad x_2 = 1 \cdot 1 + 0 \cdot 0 = 1$$

$$\therefore e(10) = 1011$$

$$\text{Next } e(11) = 11 \ x_1 \ x_2$$

$$\therefore x_1 = 1 \cdot 1 + 1 \cdot 1 = 0, \quad x_2 = 1 \cdot 1 + 1 \cdot 1 = 1$$

$$\therefore e(11) = 1101$$

Now prepare the decoding table.

In the first row of the table write all the encoded words viz. 0000, 0110, 1011, 1101.

0000	0110	1011	1101
0001	0111	<u>1010</u>	1100
0010	0100	1001	1111
1000	1110	0011	0101

- (i) Now, the received word is 0101 which can be found in 4th column. The word at the top is 1101.  
Since  $e(11) = 1101$ , we decode 0101 as 11.

- (ii) The second received word is 1010 which can be found in the third column. The word at the top is 1011.

Since  $e(10) = 1011$ , we decode 1010 as 10.

- (iii) The third received word is 1101 which is located in the fourth column. The word at the top is the same viz. 1101.

Since  $e(11) = 1101$ , we decode 1101 as 11.

**Example 4 :** Consider the parity check matrix  $H$  given by

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Decode the following words relative to the maximum likelihood decoding function associated with  $e_H : 01111, 11001$ .  
(M.U. 1999, 2009)

**Sol. :** We first compute encoding function  $e_H : B^2 \rightarrow B^5$ .

$$\text{Now, } B^2 = \{00, 01, 10, 11\}$$

**Applied Mathematics - IV**

(19-18)

**Coding Theory**

$$\begin{aligned}
 \text{(i)} \quad e(00) &= 00 x_1 x_2 x_3 \\
 x_1 &= 0 \cdot 1 + 0 \cdot 0 = 0; \quad x_2 = 0 \cdot 1 + 0 \cdot 1 = 0; \quad x_3 = 0 \cdot 0 + 0 \cdot 1 = 0 \\
 \therefore e(00) &= 00000 \\
 \text{(ii)} \quad e(01) &= 01 x_1 x_2 x_3 \\
 x_1 &= 0 \cdot 1 + 1 \cdot 0 = 0; \quad x_2 = 0 \cdot 1 + 1 \cdot 1 = 1; \quad x_3 = 0 \cdot 0 + 1 \cdot 1 = 1 \\
 \therefore e(01) &= 01011 \\
 \text{(iii)} \quad e(10) &= 10 x_1 x_2 x_3 \\
 x_1 &= 1 \cdot 1 + 0 \cdot 0 = 1; \quad x_2 = 1 \cdot 1 + 0 \cdot 1 = 1; \quad x_3 = 1 \cdot 0 + 0 \cdot 1 = 0 \\
 \therefore e(10) &= 10110 \\
 \text{(iv)} \quad e(11) &= 11 x_1 x_2 x_3 \\
 x_1 &= 1 \cdot 1 + 1 \cdot 0 = 1; \quad x_2 = 1 \cdot 1 + 1 \cdot 1 = 0; \quad x_3 = 1 \cdot 0 + 1 \cdot 1 = 1 \\
 \therefore e(11) &= 11101
 \end{aligned}$$

Now, we construct the decoding table.

**Decoding Table**

00000	01011	10110	11101
00001	01010	10111	11100
00010	01001	10100	11111
00100	<u>01111</u>	10010	11001
01000	00011	11110	10101
10000	11011	00110	01101

- (i) The received word 01111 is in the second column and is underlined. The word at the top in its column is 01011.  
 Since  $e(01) = 01011$ , we decode 01111 as 01 i.e.  $d(01111) = 01$ .
- (ii) The received word 11001 is in the fourth column and is underlined. The word at the top in the fourth column is 11101.  
 Since  $e(11) = 11101$ , we decode 11001 as 11 i.e.  $d(11001) = 11$ .

**Example 4 :** Consider the (2, 5) group encoding function  $e : B^2 \rightarrow B^5$  defined by

$$\begin{aligned}
 e(00) &= 00000, \quad e(01) = 01110, \\
 e(10) &= 10101, \quad e(11) = 11011.
 \end{aligned}$$

Decode the following words relative to maximum likelihood decoding function  $e_H$

- (i) 01110, (ii) 10011, (iii) 10100.

(M.U. 2007, 10)

**Sol. :** We first prepare the decoding table.

**Decoding Table**

00000	01110	10101	11011
00001	01111	<u>10100</u>	11010
00010	01100	10111	11001
00100	01010	10001	11111
01000	00110	11101	<u>10011</u>
10000	11110	00101	01011

**Applied Mathematics - IV**

(19-19)

**Coding Theory**

- (i) The received word 11110 is in the second column. The word at the top is 01110.  
 Since, by data  $e(01) = 01110$ , we decode 11110 as 01  
 i.e.,  $d(11110) = 01$ .
- (ii) The received word 10011 is in the last column. The word at the top is 11011.  
 Since, by data  $e(11) = 11011$ , we decode 10011 as 11  
 i.e.,  $d(11011) = 11$ .
- (iii) The received word 10100 is in the third column. The word at the top is 10101.  
 Since, by data  $e(10) = 10101$ , we decode 10100 as 10  
 i.e.,  $d(10101) = 10$ .

$$\text{Example 5 : Let } H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

be the parity check matrix.

Decode the following words relative to maximum likelihood decoding function  $e_H$   
 (i) 011001 (ii) 1010001 (iii) 1101010 (M.U. 2009, 14)

**Sol. :** We first compute encoding function  $e_H : B^3 \rightarrow B^6$ .  
 Since  $B = \{0, 1\}$ , we have  $B^3 = \{000, 001, 010, 100, 101, 110, 111\}$

$$\begin{aligned}
 \text{Now, } e(000) &= 000 x_1 x_2 x_3 \\
 x_1 &= 0 \cdot 1 + 0 \cdot 1 + 0 \cdot 0 = 0 \\
 x_2 &= 0 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0 \\
 x_3 &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 = 0 \quad \therefore e(000) = 000000.
 \end{aligned}$$

$$\begin{aligned}
 \text{Now, } e(001) &= 001 x_1 x_2 x_3 \\
 x_1 &= 0 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 = 0 \\
 x_2 &= 0 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1 \\
 x_3 &= 0 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 = 1 \quad \therefore e(001) = 001011.
 \end{aligned}$$

$$\begin{aligned}
 \text{Now, } e(010) &= 010 x_1 x_2 x_3 \\
 x_1 &= 0 \cdot 1 + 1 \cdot 1 + 0 \cdot 0 = 1 \\
 x_2 &= 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1 \\
 x_3 &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 = 0 \quad \therefore e(010) = 010110.
 \end{aligned}$$

$$\begin{aligned}
 \text{Now, } e(011) &= 011 x_1 x_2 x_3 \\
 x_1 &= 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 = 1 \\
 x_2 &= 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0 \\
 x_3 &= 0 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 = 1 \quad \therefore e(011) = 011101.
 \end{aligned}$$

$$\begin{aligned}
 \text{Now, } e(100) &= 100 x_1 x_2 x_3 \\
 x_1 &= 1 \cdot 1 + 0 \cdot 1 + 0 \cdot 0 = 1 \\
 x_2 &= 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0 \\
 x_3 &= 1 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 = 0 \quad \therefore e(100) = 100100.
 \end{aligned}$$

$$\text{Now, } e(101) = 101x_1x_2x_3 \\ \therefore x_1 = 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 = 1 \\ x_2 = 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1 \\ x_3 = 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 = 1$$

$$\therefore e(101) = 101111.$$

$$\text{Now, } e(110) = 110x_1x_2x_3 \\ \therefore x_1 = 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 0 = 0 \\ x_2 = 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1 \\ x_3 = 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 = 0$$

$$\therefore e(110) = 110010.$$

$$\text{Now, } e(111) = 111x_1x_2x_3 \\ \therefore x_1 = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 = 0 \\ x_2 = 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0 \\ x_3 = 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 1 = 1$$

Decoding Table

000000	001011	010110	011101	100100	101111	110010	111001
000001	001010	010111	011100	100101	101110	110011	111000
000010	001001	010100	011111	100110	101101	110000	111010
000100	001111	010010	011001	100000	101011	110000	111011
000100	000011	011110	010101	101100	100111	110100	111000
010000	011011	000110	001101	110100	111010	100001	101100

- (i) Now, the received word is 011001. The word at the top is 011101.  
Since  $e(011) = 011101$ . We decode 011001 as 011.  
i.e.,  $d(011001) = 011$ .

- (ii) The received word is 101001. The word at the top is 111001.  
Since  $e(111) = 111001$ . We decode 111001 as 111.  
i.e.,  $d(111001) = 111$ .

- (iii) The received word is 111010. The word at the top is 110010.  
Since  $e(110) = 110010$ . We decode 111010 as 110.  
i.e.,  $d(111010) = 110$ .

**Example 6 :** Consider the (3, 5) group encoding function  $e : B^3 \rightarrow B^5$  defined by

$$\begin{aligned} e(000) &= 00000, & e(100) &= 10011, & e(001) &= 00110, \\ e(101) &= 10101, & e(010) &= 01001, & e(110) &= 11010, \\ e(011) &= 01111, & e(111) &= 11100. \end{aligned}$$

Decode the following words relative to maximum likelihood decoding function.

- (a) 11001, (b) 01010, (c) 00111.

(M.U. 2009, 10, 13, 15)

Sol:

00000	00110	01001	01111	10011	10101	11010	11100
00001	00111	01000	01110	10010	10100	11011	11101
00010	00100	01011	01101	10001	10111	11000	11110
00100	00010	01101	01011	10111	10001	11110	11000
01000	01110	00001	00111	11011	11101	10010	10100
10000	10110	11001	11111	00011	00101	01010	01100
10001	10111	11000	11110	00010	00100	01011	01101
10010	10100	11011	11101	00001	00111	01000	01110

- (i) The received word 11001 is in the third column and is underlined. The word at the top in its column is 01001.  
Since by data  $e(010) = 01001$ , we decode 11001 as 010. i.e.,  $d(11001) = 010$ .
- (ii) The received word 01010 is in the seventh column and is underlined. The word at the top is 11010.  
Since by data  $e(110) = 11010$  we decode 01010 as 110. i.e.,  $d(01010) = 110$ .
- (iii) The received word 00111 is in the second column and is underlined. The word at the top in its column 00110.  
Since by data  $e(001) = 00110$  we decode 00111 as 001. i.e.,  $d(00111) = 001$ .

**EXERCISE - IV**

1. Consider the (3, 6) encoding function  $e : B^3 \rightarrow B^6$  defined by  
 $e(000) = 000000, \quad e(001) = 001100, \quad e(010) = 010011,$   
 $e(011) = 011111, \quad e(100) = 100101, \quad e(101) = 101001,$   
 $e(110) = 110110, \quad e(111) = 111010.$

Decode the following word 000101.

[Ans. : 100]

2. Consider the (3, 6) group encoding function  $e : B^3 \rightarrow B^6$  defined by  
 $e(000) = 000000, \quad e(001) = 000110, \quad e(010) = 010010,$   
 $e(011) = 010100, \quad e(100) = 100101, \quad e(101) = 100011,$   
 $e(110) = 110111, \quad e(111) = 110001.$

Decode (i) 110010, (ii) 101101, (iii) 101011.

[Ans. : (i) 010, (ii) 100, (iii) 101]

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

3. Let  $H$  be a parity check matrix.Decode the following words relative to a maximum likelihood decoding function  $e_H$ .

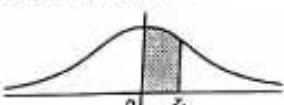
- (i) 011 001, (ii) 101001, (iii) 111010.

(M.U. 1997, 2005, 14)

[Ans. : (i) 011, (ii) 111, (iii) 110]

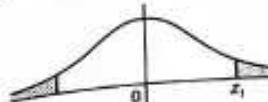


## Area Under Standard Normal Curve



The table gives the area under the standard normal curve from  $z = 0$  to  $z = z_1$ , which is the probability that  $z$  will lie between  $z = 0$  and  $z = z_1$ .

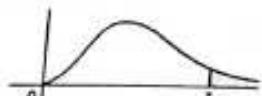
<b><i>z</i></b>	.00	.01	.02	.03	.04	.05	.06	.07	.08	.09
0.0	0.0000	0.0040	0.0080	0.0120	0.0160	0.0199	0.0239	0.0279	0.0319	0.0359
0.1	0.0398	0.0438	0.0478	0.0517	0.0557	0.0596	0.0636	0.0675	0.0714	0.0753
0.2	0.0793	0.0832	0.0871	0.0910	0.0948	0.0987	0.1026	0.1064	0.1103	0.1141
0.3	0.1179	0.1217	0.1255	0.1293	0.1331	0.1368	0.1406	0.1443	0.1480	0.1517
0.4	0.1554	0.1591	0.1628	0.1664	0.1700	0.1736	0.1772	0.1808	0.1844	0.1879
0.5	0.1915	0.1950	0.1985	0.2019	0.2054	0.2088	0.2123	0.2157	0.2190	0.2224
0.6	0.2257	0.2291	0.2324	0.2357	0.2389	0.2422	0.2454	0.2486	0.2517	0.2549
0.7	0.2580	0.2611	0.2642	0.2673	0.2703	0.2734	0.2764	0.2794	0.2823	0.2852
0.8	0.2881	0.2910	0.2939	0.2967	0.2995	0.3023	0.3051	0.3078	0.3106	0.3133
0.9	0.3159	0.3186	0.3212	0.3238	0.3264	0.3289	0.3315	0.3340	0.3365	0.3389
1.0	0.3413	0.3438	0.3461	0.3485	0.3508	0.3531	0.3554	0.3577	0.3599	0.3621
1.1	0.3643	0.3665	0.3686	0.3708	0.3729	0.3749	0.3770	0.3790	0.3810	0.3830
1.2	0.3849	0.3869	0.3888	0.3907	0.3925	0.3944	0.3962	0.3980	0.3997	0.4015
1.3	0.4032	0.4049	0.4066	0.4082	0.4099	0.4115	0.4131	0.4147	0.4162	0.4177
1.4	0.4192	0.4207	0.4222	0.4236	0.4251	0.4265	0.4279	0.4292	0.4306	0.4319
1.5	0.4332	0.4345	0.4357	0.4370	0.4382	0.4394	0.4406	0.4418	0.4429	0.4441
1.6	0.4452	0.4463	0.4474	0.4484	0.4495	0.4505	0.4415	0.4525	0.4535	0.4545
1.7	0.4554	0.4564	0.4573	0.4582	0.4591	0.4599	0.4608	0.4616	0.4625	0.4633
1.8	0.4641	0.4649	0.4656	0.4664	0.4671	0.4678	0.4686	0.4693	0.4699	0.4706
1.9	0.4713	0.4719	0.4726	0.4732	0.4738	0.4744	0.4750	0.4756	0.4761	0.4767
2.0	0.4772	0.4778	0.4783	0.4788	0.4793	0.4798	0.4803	0.4808	0.4812	0.4817
2.1	0.4821	0.4826	0.4830	0.4834	0.4838	0.4842	0.4846	0.4850	0.4854	0.4857
2.2	0.4861	0.4864	0.4868	0.4871	0.4875	0.4878	0.4881	0.4884	0.4887	0.4890
2.3	0.4893	0.4896	0.4898	0.4901	0.4904	0.4906	0.4909	0.4911	0.4913	0.4916
2.4	0.4918	0.4920	0.4922	0.4925	0.4927	0.4929	0.4931	0.4932	0.4934	0.4936
2.5	0.4938	0.4940	0.4941	0.4943	0.4945	0.4946	0.4948	0.4949	0.4951	0.4952
2.6	0.4953	0.4955	0.4956	0.4957	0.4959	0.4960	0.4961	0.4962	0.4963	0.4964
2.7	0.4965	0.4966	0.4967	0.4968	0.4969	0.4970	0.4971	0.4972	0.4973	0.4974
2.8	0.4974	0.4975	0.4976	0.4977	0.4978	0.4978	0.4979	0.4979	0.4980	0.4981
2.9	0.4981	0.4982	0.4982	0.4983	0.4984	0.4984	0.4985	0.4985	0.4986	0.4986
3.0	0.4987	0.4987	0.4987	0.4988	0.4988	0.4989	0.4989	0.4989	0.4990	0.4990

Percentage Points of  $t$ -distribution

## Example

For  $\Phi = 10$  d. o. f.  
 $P(|t| > 1.812) = 0.1$

<b><i>Φ</i></b>	<b><i>P</i></b>	<b>0.20</b>	<b>0.10</b>	<b>0.05</b>	<b>0.02</b>	<b>0.01</b>
1		3.078	6.314	12.706	31.812	63.657
2		1.886	2.920	4.303	6.965	9.925
3		1.638	2.353	3.182	4.541	5.841
4		1.533	2.132	2.776	3.747	4.604
5		1.476	2.015	2.571	3.365	4.032
6		1.440	1.943	2.447	3.143	3.707
7		1.415	1.895	2.365	2.998	3.499
8		1.397	1.860	2.306	2.896	3.355
9		1.383	1.833	2.262	2.821	3.250
10		1.372	1.812	2.228	2.764	3.169
11		1.363	1.796	2.201	2.718	3.106
12		1.356	1.782	2.179	2.681	3.055
13		1.350	1.771	2.160	2.650	3.012
14		1.345	1.761	2.145	2.624	2.977
15		1.341	1.753	2.131	2.602	2.947
16		1.337	1.746	2.120	2.583	2.921
17		1.333	1.740	2.110	2.567	2.898
18		1.330	1.734	2.101	2.552	2.878
19		1.328	1.729	2.093	2.539	2.861
20		1.325	1.725	2.086	2.528	2.845
21		1.323	1.721	2.080	2.518	2.831
22		1.321	1.717	2.074	2.508	2.819
23		1.319	1.714	2.069	2.500	2.807
24		1.318	1.711	2.064	2.492	2.797
25		1.318	1.708	2.060	2.485	2.287
26		1.315	1.706	2.056	2.479	2.779
27		1.314	1.703	2.052	2.473	2.771
28		1.313	1.701	2.048	2.467	2.763
29		1.311	1.699	2.045	2.462	2.756
30		1.310	1.697	2.042	2.457	2.750
40		1.303	1.684	2.021	2.423	2.704
60		1.296	1.671	2.000	2.390	2.660
120		1.289	1.658	1.980	2.358	2.617
$\infty$		1.282	1.645	1.960	2.325	2.576

Percentage Points of  $\chi^2$  - Distribution

## Example

For  $\Phi = 10$  d. o. f.  
 $P(\chi^2 > 15.99) = 0.10$

$\Phi \backslash P$	0 = .99	0.95	0.50	0.10	0.05	0.02	0.01
1	0.00157	0.0393	4.55	2.706	3.841	5.214	6.635
2	.0201	.103	1.386	4.605	5.991	7.824	9.210
3	.115	.352	2.366	6.251	7.815	9.837	11.341
4	.297	.711	3.357	7.779	9.488	11.668	13.277
5	.554	1.145	4.351	9.236	11.070	13.388	15.086
6	.872	1.635	5.348	10.645	12.592	15.033	16.812
7	1.339	2.167	6.346	12.017	14.067	16.622	18.475
8	1.646	2.733	7.344	13.362	15.507	18.168	20.090
9	2.088	3.325	8.343	14.684	16.919	19.679	21.666
10	2.558	3.940	9.340	15.987	18.307	21.161	23.209
11	3.053	4.575	10.341	17.275	19.875	22.618	24.725
12	3.571	5.226	11.340	18.549	21.026	24.054	26.217
13	4.107	5.892	12.340	19.812	22.362	25.472	27.688
14	4.660	6.571	13.339	21.064	23.685	26.873	29.141
15	4.229	7.261	14.339	22.307	24.996	28.259	30.578
16	5.812	7.962	15.338	23.542	26.296	29.633	32.000
17	6.408	8.672	16.338	24.769	27.587	30.995	33.409
18	7.015	9.390	17.338	25.989	28.869	32.346	34.805
19	7.633	10.117	18.338	27.204	30.144	33.687	36.191
20	8.260	10.851	19.337	28.412	31.410	35.020	37.566
21	8.897	11.591	20.337	29.615	32.671	36.349	38.932
22	9.542	12.338	21.337	30.813	33.924	37.659	40.289
23	10.196	13.091	22.337	32.007	35.172	38.968	41.638
24	10.856	13.848	23.337	32.196	36.415	40.270	42.980
25	11.524	14.611	24.337	34.382	37.652	41.566	44.314
26	12.198	15.379	25.336	35.363	38.885	41.856	45.642
27	12.879	16.151	26.336	36.741	40.113	44.140	46.963
28	13.565	16.928	27.336	37.916	41.337	45.419	48.278
29	14.256	17.708	28.336	39.087	42.557	46.693	49.588
30	14.953	18.493	29.336	40.256	43.773	47.962	50.892

## A List of Primes

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	181	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531

## Applied Mathematics - IV

(B)

2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2967	2963	2969	2971	2999
3001	3011	3019	3023	3037	3041	3049	3061	3087	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331
3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511
3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
3581	3583	3593	3607	3613	3617	3623	3631	3637	3643
3659	3671	3673	3677	3691	3697	3701	3709	3719	3727
3733	3739	3761	3767	3769	3779	3793	3797	3803	3821
3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989
4001	4003	4007	4013	4019	4021	4027	4049	4051	4057
4073	4079	4091	4093	4099	4111	4127	4129	4133	4139
4153	4157	4159	4177	4201	4211	4217	4219	4229	4231
4241	4243	4253	4259	4261	4271	4273	4283	4289	4297
4327	4337	4339	4349	4357	4363	4373	4391	4397	4409
4421	4423	4441	4447	4451	4457	4463	4481	4483	4493
4507	4513	4517	4519	4523	4547	4549	4561	4567	4583
4591	4597	4603	4621	4637	4639	4643	4649	4651	4657
4663	4673	4679	4691	4703	4721	4723	4729	4733	4751
4759	4783	4787	4789	4793	4799	4801	4813	4817	4831
4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999	5003
5009	5011	5021	5023	5039	5051	5059	5077	5081	5087
5099	5101	5107	5113	5119	5147	5153	5167	5171	5179
5189	5197	5209	5227	5231	5233	5237	5261	5273	5279
5281	5297	5303	5309	5323	5333	5347	5351	5381	5387
5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
5449	5471	5477	5479	5483	5501	5503	5507	5519	5521
5527	5531	5557	5563	5569	5573	5581	5591	5623	5639
5641	5647	5651	5653	5657	5659	5669	5683	5689	5693

Statistical Tables

## Applied Mathematics - IV

## Values of Euler's Phi-Function

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	35	24	69	44
2	2	36	24	70	24
3	2	38	26	71	24
4	4	39	24	72	36
5	2	40	40	73	72
6	6	42	12	74	24
7	4	43	42	75	40
8	6	44	20	76	36
9	4	45	24	77	24
10	10	46	22	78	78
11	4	47	46	79	32
12	12	48	16	80	54
13	6	49	42	81	40
14	8	50	20	82	64
15	8	51	32	83	42
16	16	52	24	84	56
17	6	53	52	85	82
18	8	54	18	86	40
19	8	55	40	87	88
20	8	56	24	88	24
21	12	57	36	89	72
22	10	58	28	90	44
23	22	59	58	91	60
24	8	60	16	92	46
25	20	61	60	93	72
26	12	62	30	94	32
27	18	63	36	95	96
28	12	64	32	96	32
29	28	65	48	97	96
30	8	66	98	98	42
31	30	67	100	99	60
32	16	68	20	100	40
33	20	69	66		
34	16	70	32		