UG MA S2 - 01
(DSC/DSE)

FOUR YEAR BACHELOR'S DEGREE COURSE

(CBCS in Accordance with NEP 2020)

SEMESTER II

ABSTRACT ALGEBRA AND DISCRETE MATHEMATICS

MATHEMATICS

Hiranya Chandra Bhuyan School of Science and Technology
KRISHNA KANTA HANDIQUI STATE OPEN UNIVERSITY

Subject Experts

Professor Bipan Hazarika, Dept. of Mathematics, Gauhati University
Dr. Dillip Kumar Sarma, Former Head, Cotton College

Course Coordinator : Harekrishna Deka, KKHSOU

SLM Preparation Team

UNITS	CONTRIBUTORS
1, 2, 3, 4, 5, 6, 7, 8,9,10,11,12,14	Dr Dilip Kumar Sarma Cotton College, Guwahati
13	Harekrishna Deka KKHSOU

Editorial Team

Content : Prof. Biswajit Bhagawati,Former Head, ,Cotton college
Structure & Format : Harekrishna Deka, KKHSOU

First Edition : March, 2023; Reprint : February, 2024 ISBN: .....

© Krishna Kanta Handiqui State Open University

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

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

The University acknowledges with thanks the financial support provided by the **Distance Education Bureau, UGC** for the preparation of this study material.

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

COURSE INTRODUCTION

'Abstract Algebra and Discrete Mathematics' is the second discipline specific minor course of Mathematics. The course consists of fourtheen units.

The first unit deals with relations and functions. After going through this unit, you will be able to know various types of relations and function.In second unit, we will discuss binary operation and its different types.In third unit, we will discuss group and its properties.The fourth unit deals with subgroups and cyclic groups. In this unit, we will also discuss properties of subgroup.The fifth unit consists of group of permutation. In this unit, we define permutation and different type of permutations. Concept of permutation groups will also be discussed in this unit.In sixth unit, we will discuss subgroup of a group and Lagrange's subgroup order theorem.In seventh unit, concept of normal subgroup and quotient group will be discussed.

The eight unit deals with the concept of homomorphism types of groups. In this unit, we will discuss different types of homomorphisms and properties of homomorphisms.In ninth unit, we will discuss ring and its properties.The tenth unit consists of Integral domains and Field. In this unit, you will know about properties of Integral domains and Field.The eleventh unit deals with the concept of vector space. In this unit, we will discuss properties of vector space and subspace of a vector space. We will also discuss linear dependence and independence of a vactor space. Finally, we also define basis and dimension of a vector space in this unit.The twelvth unit deals with the concept of combintorics. After going through this unit, you will be able to know permutations and combinations.In thirteenth unit, we will discuss the concept of Mathematical logic. In this unit, we will discuss the different logical connectives.The concept of Boolean Algebra will be discussed in the fourtheenth unit. In this unit, we will discuss some basic laws of Boolean Algebra and Boolean Expression.

While going through a unit, you wll notice some along side boxes, which have been included to help you know some of the difficult, unseen terms. At the end of each section, you will get "CHECK YOUR PROGRESS" questions. These have been designed to self-check your progress of study. It will be better if you solve the problems put in these boxes immediately after you go through the sections of the units and then match your answers with " ANSWERS TO CHECK YOUR PROGRESS" given the end of each unit.

CONTENTS

UNIT 1: Relations and functions **Page : 7-30**

Relations and Types of relations, equivalence relation, function and types of function.

UNIT 2: Binary operations **Page : 31-40**

Binary Operation, Commutative Binary Operation, Associative Binary Operation, Identity Element, Inverse of an Element.

UNIT 3: Group **Page : 41-51**

Definitions and Examples of groups, Properties of groups.

UNIT 4: Subgroup **Page : 52-61**

Subgroups, cyclic groups.

UNIT 5: Groups of permutation **Page : 62-83**

Definition of Permutation, Examples, Multiplication of Permutation, Different Kinds of Permutation, Permutation Group.

UNIT 6: Cosets **Page : 84-90**

Coset, Lagrange's Subgroup order theorem.

UNIT 7: Normal subgroup & Quetion Group **Page : 91-97**

Normal subgroups, Quotient groups.

UNIT 8: Homomorphism of group **Page : 98-115**

Definition and examples, Types of Homomorphism, Properties of Homomorphism.

UNIT 9: Ring **Page : 116-127**

Definitions and Examples of Rings, Properties of Ring.

UNIT 10: Integral domain & Field **Page : 128-135**

Integral domains, Field and their properties.

UNIT 11: Vector space **Page : 136-161**

Defintion and examples of vector space, Elementary properties, subspace of a vector space, Linear dependence and Independence, Basis and Dimension.

UNIT 12: Cominatorics **Page : 162-178**

The Rule of Sum, The Rule of product, Permutation, Combination.

UNIT 13: Mathematical Logic **Page : 179-196**

Definition of Statements, Examples of Statements, Logical Connectives : Negation, Conjunction, Disjunction Conditional, Biconditional.

UNIT 14: Boolean Algebra **Page : 197-227**

Definition, Properties and Examples, Basic Laws of Boolean Algebra, Boolean Expression.

UNIT1: RELATIONS AND FUNCTIONS

UNIT STRUCTURE

1.1 Learning objectives

1.2 Introduction

1.3 Concept of Relation

1.3.1 Identity Relation

1.3.2 Inverse Relation

1.4 Types of Relation

1.5 Equivalence Relations

1.5.1 Equivalence Class

1.6 Concept of Function

1.6.1 Identity Function

1.6.2 Constant Function

1.7 Types of Function

1.8 Let us Sum Up

1.9 Answers to Check Your Progress

1.10 Further Readings

1.11 Model Questions

1.1 LEARNING OBJECTIVES

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

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

1.2 INTRODUCTION

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

subset of A. Symbolically we denote it by $B \subseteq A$.

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

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

(a, b) is called an ordered pair.

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

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

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

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

$$n(AxB) = n(BxA)=xy$$

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

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

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

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

1.3 CONCEPT OF RELATION

Let us consider the following sentences.

(1) 11 is greater than 10.

(2) 35 is divisible by 7.

(3) New Delhi is the capital of India.

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

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

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

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

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

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

pairs of R is called the range of R.

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

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

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

B={8, 9}

$\therefore$ A x B ={(1, 8), (1, 9), (2, 8), (2, 9), (3, 8), (3, 9)}

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

Clearly $R \subseteq$ AxB

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

Here 1R8, 2R9, 3R9

Domain of R = {1, 2, 3}

Range of R = {8, 9}

Example 2 : Let IR be the set of real numbers.

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

$\therefore$ R is a relation on IR.

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

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

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

Example 3: Let X be the set of odd integers.

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

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

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

$\therefore R = \phi \subseteq X \times X$

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

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

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

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

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

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

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

1.3.1 Identity Relation

Let A be a non-empty set.

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

I_A is called the identity relation on A.

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

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

Clearly I_A is the identity relation on A.

1.3.2 Inverse Relation

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

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

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

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

B = {5, 6}

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

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



CHECK YOUR PROGRESS 1

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

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

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

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

Examine if the following ordered pairs belong to R.

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

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

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

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

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

Write down the identity relation on A.

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

Let R = {(4, 7), (5, 8), (6, 7), (6, 8), (6, 9)}

Write down R^{-1}.

1.4 TYPES OF RELATION

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

1. R is called reflexive if $(a, a) \in R$, i.e; aRa, for all $a \in A$.
2. R is called symmetric if whenever $(a, b) \in R$, then $(b, a) \in R$, i.e, if whenever aRb, then bRa; $a, b \in A$.
3. R is called anti-symmetric if $(a, b) \in R$, $(b, a) \in R \Rightarrow a = b$, i.e., if aRb, bRa $\Rightarrow$ a=b; $a, b \in A$.
4. R is called transitive if whenever (a, b), $(b, c) \in R$, then $(a, c) \in R$, i.e., if whenever aRb, bRc, then aRc; $a, b, c \in A$.

Example 7: Let A = {1, 2, 3}

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

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

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

$\therefore$ R is not reflexive.

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

$\therefore$ R is symmetric.

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

$\therefore$ R is not anti-symmetric.

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

$\therefore$ R is transitive.

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

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

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

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

$\therefore$ R is reflexive.

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

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

$\therefore$ R is not symmetric.

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

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

$\therefore$ R is anti-symmetric.

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

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

$\therefore$ R is transitive.

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

Solution : Let A = {1, 2}

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

Clearly R is a relation on A.

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

$\therefore$ R is not reflexive.

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

$\therefore$ R is not symmetric.

But R is transitive.



CHECK YOUR PROGRESS 2

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

Q 2: Define a relation on the set

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

(i) symmetric, but neither reflexive nor transitive;

(ii) reflexive and transitive, but not symmetric;

(iii) reflexive and symmetric, but not transitive.

1.5 EQUIVALENCE RELATION

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

Example 10: Let Z be the set of integers and

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

Examine if R is an equivalence relation on Z.

Solution : Let $x \in Z$

$\therefore$ x+x is even

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

$\therefore$ R is reflexive.

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

$\Rightarrow$ y+x is even

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

$\therefore$ R is symmetric.

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

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

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

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

$\Rightarrow$ x+z is even

$(x, z) \in R$

$\therefore$ R is transitive

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

Example 11: Let A be the set of all straight lines in a plane.

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

Examine if R is reflexive, symmetric and transitive.

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

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

$\therefore$ R is not reflexive

If a line x is perpendicular to another line y, then y is perpendicular to x,

i.e. $x \perp y \Rightarrow y \perp x$

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

$\therefore$ R is symmetric.

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

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

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

$\therefore$ R is not transitive.

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

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

Examine if R is an equivalence relation on A.

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

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

$\therefore$ R is reflexive.

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

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

$\therefore$ R is symmetric.

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

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

$\therefore$ R is transitive

Thus, R is an equivalence relation on A.

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

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

Solution : We have ab = ba

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

$\therefore$ R is reflexive

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

$\Rightarrow$ cb = da

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

$\therefore$ R is symmetric

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

$\Rightarrow$ ad = bc and cf = de

$\Rightarrow$ adcf = bcde

$\Rightarrow$ af = be

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

$\therefore$ R is transitive.

Thus, R is an equivalence relation on IN x IN.

Example 14: (Congruence modulo n)

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

Let a, b $\in$ Z

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

Symbolically, we write.

a $\equiv$ b (mod n)

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

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

$\therefore$ the relation is reflexive.

Let a $\equiv$ b (mod n)

$\Rightarrow$ a–b is divisible by n.

$\Rightarrow$ b–a is divisible by n.

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

$\therefore$ the relation is symmetric.

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

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

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

$\Rightarrow$ a–c is divisible by n

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

$\therefore$ the relation is transitive.

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

We know that 15-3 is divisible by 4.

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

15 $\equiv$ 3 (mod 4)

15–3 is not divisible by 7

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

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

Example 15: Let Z be the set of integers.

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

Examine if R is an equivalence relation on Z.

Solution : We have aa $\geq$ 0

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

$\therefore R$ is reflexive

Let $(a, b) \in R$

$\therefore ab \geq 0$

$\Rightarrow ba \geq 0$

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

$\therefore$ R is symmetric.

We have

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

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

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

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

$\therefore$ R is not transitive.

Thus, R is not an equivalence relation.

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

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

R is reflexive.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proof. Let A be a non-empty set.

Let R and S be two equivalence relations on A.

R and S are reflexive

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

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

$\therefore R \cap S$ is reflexive.

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

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

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

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

$\therefore R \cap S$ is symmetric.

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

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

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

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

$\therefore R \cap S$ is transitive.

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

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

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

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

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

are two equivalence relations on A.

$R \cup S$ = {(1, 1), (2, 2), (3, 3), (1, 3), (3, 1), (1, 2), (2, 1)}

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

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

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

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

1.5.1 Equivalence Class

Let us consider the set Z of integers

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

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

Clearly R is reflexive, symmetric and transitive.

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

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

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

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

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

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

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

We see that

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

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

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

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

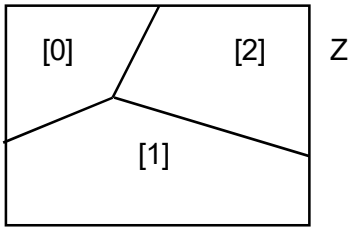
We see that there are 3 distinct equivalence classes, viz, [0], [1], [2].

Also we note that

[0] U [1] U [2] = Z

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

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



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

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

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

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

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

Definition : Let A be a non-empty set.

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

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

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



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

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

Proof. Let [a] = [b]

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

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

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

$\Rightarrow$ aRb

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

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

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

Now, xRa and aRb

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

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

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

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

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

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

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

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

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

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

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

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

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

Let a, b $\in$A.

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

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

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

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

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

$\Rightarrow$ xRa and xRb

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

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

Let y$\in$[a]

$\Rightarrow$ yRa

Now yRa and aRb

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

$\Rightarrow$ y $\in$ [b]

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

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

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

$\therefore$[a] = [b]

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

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



CHECK YOUR PROGRESS 3

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

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

Q 3: Let Z be the set of integers.

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

Examine if R is an equivalence relation on Z ?

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

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

Examine if R is an equivalence relation on A.

Q 5: let Z be the set of integers.

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

Is R an equivalence relation on Z ?

Justify your answer.

1.6 CONCEPT OF FUNCTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Are the following relations from be functions A to B ?

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

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

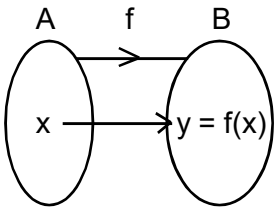
Solution : (i) No. Here two distinct ordered pairs (1, x), (1, w) have the same first component.

(ii) Yes.

Here, each element of A appears as the first component exactly in one of the ordered pairs of f_2.

Thus we see that.

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



We observe that if A and B are two non-empty sets and if each element of A is associated with a unique element of B, then the rule by which this association is made, is called a function from the set A to the set B. The rules are denoted by f, g etc. The sets A, B may be the same.

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

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

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

Clearly, domain of f = IN

codomain of f = Z

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

$\therefore$ range of f = {–1, 1}

1.6.1 Identity Function

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

i is called the identity function.

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

1.6.2 Constant Function

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

f is called a constant function.

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

1.7 TYPES OF FUNCTION

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

1. If there is at least one element in B which is not the image of any

element in A, then f is called an "into" function.

2. If each element in B is the image of at least one element in A, then f is called an "onto" function (or a surjective function or a surjection).

Note : In case of an onto function, range of f = codomain of f.

3. If different elements in A have different images in B, then f is called a one-one function (or an injective function or an injection).

4. If two (or more) different elements in A have the same image in B, then f is called a many-one function.

5. A function is said to be bijective if it is one-one (injective) and onto (surjective).

Note : Identity function is a bijective function.

How to prove that f is one-one?

Let $x_1, x_2, \in A$

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

or,

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

How to prove that f is onto?

Let $y \in B$ (codomain)

Let $y = f(x)$

We find x in terms of y

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

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

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

Examine if f is a bijective function.

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

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

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

$\Rightarrow x_1 = x_2$

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

Let $y \in IN$ (codomain)

Let $y = f(x)$

$\Rightarrow y = 3x + 7$

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

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

$\therefore$ f is not onto

$\therefore$ f is not a bijection.

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

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

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

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

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

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

$\Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

Let $y \in X$ (codomain)

Let y = f(x)

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

$\Rightarrow y(x-1) = x+1$

$\Rightarrow yx-y = x+1$

$\Rightarrow yx - x = y+1$

$\Rightarrow x(y-1) = y+1$

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

$\therefore$ f is onto.

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

Solution :

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

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

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

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

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

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

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

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

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

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

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

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

Now, range of f

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

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

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

$\therefore$ A has n elements,

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

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

$\therefore$ f is one-one.

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

Let IN be the set of natural numbers.

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

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

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

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

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

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

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

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

Let $u \in A$ (codomain).

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

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

$\therefore$ f is onto.

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

Let IN be the set of natural numbers.

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

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



CHECK YOUR PROGRESS 4

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

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

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

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

f : IR$\rightarrow$IR be defined by

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

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

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

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

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

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

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

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



1.8 LET US SUM UP

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

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



1.9 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS – 1

Ans to Q No 1: 2^{12}

Ans to Q No 2: 2^{25}

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

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

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

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

CHECK YOUR PROGRESS – 2

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

CHECK YOUR PROGRESS – 3

Ans to Q No 1: Equivalence relation.

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

Ans to Q No 3: Equivalence relation.

Ans to Q No 4: Equivalence relation.

Ans to Q No 5: Yes.

CHECK YOUR PROGRESS – 4

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

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

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

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

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

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

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



1.10 FURTHER READINGS

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

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

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

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

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



1.11 MODEL QUESTION

Q 1: Let A = {1, 2, 3}, B = {3, 4, 5}.
How many relations are there from A to B ? Write down any four relations from A to B.

Q 2: Let A = {3, 4, 5}, B = {5, 6, 7}
Which of the following relations are functions from A to B ? If it is a function, determine whether it is one-one and whether it is onto ?
(i) {(3, 5), (4, 5), (5, 7)}
(ii) {(3, 7), (4, 5), (5, 6)}
(iii) {(3, 6), (4, 6), (5, 6)}
(iv) {(3, 6), (4, 7), (5, 5)}

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

Q 4: Let A be the set of all triangles in a plane.
Let R = {(x, y) : x, y $\in$ A and x is congruent to y}
Examine if R is an equivalence relation on A.

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

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

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

Show that R is reflexive but neither symmetric nor transitive.

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

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

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

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

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

Show that f is bijective.

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

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

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

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

*** ***** ***

UNIT 2: BINARY OPERATION

UNIT STRUCTURE

2.1 Learning objectives
2.2 Introduction
2.3 Binary Operation
  2.3.1 Commutative Binary Operation
  2.3.2 Associative Binary Operation
  2.3.3 Identity Element
  2.3.4 Inverse of an Element
2.4 Let Us Sum Up
2.5 Answers to Check Your Progress
2.6 Further Reading
2.7 Model Questions

2.1 LEARNING OBJECTIVES

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

- binary operation on a set

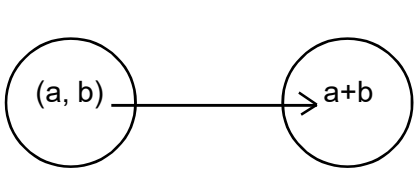
2.2 INTRODUCTION

We have studied relations and functions. In this unit, we will introduce the notion of binary operations and its types.

2.3 BINARY OPERATION

Let us consider the set IN of natural numbers.

For every ordered pair $(a, b) \in IN \times IN$, we get a unique $a+b \in IN$. So we can define a funtion $f : IN \times IN \to IN$, $f(a, b) = a+b$.

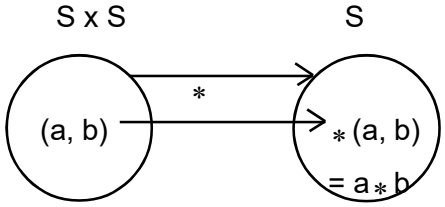


This function is known as a binary operation on IN. Thus, addition is a binary operation on IN.

Similarly, multiplication is a binary operation on IN; for every ordered pair (a, b) $\in$ IN x IN. We get a unique ab $\in$ IN. But subtraction is not a binary operation on IN; for every ordered pair (a, b) $\in$ IN x IN, we do not get a–b $\in$ IN. We have (2, 3) $\in$ IN x IN, but 2–3 = -1 $\notin$ IN.

Definition: A binary operation $*$ on a non-empty set S is a function from S x S to S, i.e.

$* : S \times S \to S$



Here the image of (a, b) $\in$ S x S under the function $*$, i.e $*$ (a, b) is denoted by a $*$ b.

Thus, $*$ is a binary operation on S if a $*$ b $\in$ S, for all a, b $\in$ S.

Definition: Let $*$ be a binary operation on a non-empty set S and H be a subset of S. H is said to be closed under $*$ if for all a, b $\in$ H, we have a $*$ b $\in$ H.In particular,if a $*$ b $\in$ A $\forall$ a, b $\in$ A,then A is said to be closed under the operation $*$.

Number of Binary operations on a finite set

Let A, B be two finite sets, and n (A) = m and n (B) = n.

Then the number of functions from A to B is n^m. [The first element of A can be associated in n ways, the second element in n ways and lastly, the m th element can be associated in n ways.

$\therefore$ the number of functions

= n. n ... ... n (m factors) = n^m]

We know that n (A x A) = mm = m^2

$\therefore$ number of binary operations on A

= number of functions from A x A to A

= m^{m^2}

Examples

1. Addition is a binary operation on IN.
2. Subtraction is not a binary operation on IN.

3. Multiplication is a binary operation on IN.
4. Addition is a binary operation on Z.
5. Addition is not a binary operation on the set S = Z – {0} of non–zero integers, for $3 \in S$, $-3 \in S$, but $3+(-3) = 0 \notin S$.
6. Subtraction is a binary operation on Z.
7. Let S be the collection of all real matrices. Matrix addition is not a binary operation on S. We cannot find the sum of a 2 x 3 matrix and a 3 x 4 matrix.
8. Let M_{mxn} be the collection of all m x n real matrices. Matrix addition is a binary operation on M_{mxn}.
9. Let M_{nxn} be the collection of all nxn real matrices. Matrix multiplication is a binary operation on M_{nxn}.
10. Addition (also multiplication) is a binary operation on the set C of complex numbers.

Example 1: Is $*$ defined by $a * b = a-b+10$ a binary operation on Z ?

Solution: Let $a, b \in Z$

Clearly $a-b+10 \in Z, \forall\ a, b \in Z$

i.e., $a * b \in Z, \forall\, a, b \in Z$

$\therefore\ *$ is a binary operation on Z

Example 2: Is $*$ defined by $a * b = \frac{ab}{5}$ a binary operation on Q ?

Solution: Let $a, b \in Q$

$\therefore ab \in Q$ (the product of two rational numbers is a rational number)

$\therefore \frac{ab}{5} \in Q$

i.e. $a * b \in Q, \forall\, a, b \in Q$

$\therefore\ *$ is a binary operation on Q

Example 3: Let P be the set of all subsets of a non-empty set S. Show that union and intersection are two binary operations on P.

Solution: Let $A, B \in P$ i.e. $A \subseteq S, B \subseteq S$

$\therefore A \cup B \subseteq S$ i.e $A \cup B \in P$

$\therefore\ \cup$ is a binary operation on P.

Similarly, $A \cap B \in P, \forall\, A, B \in P$

$\therefore \cap$ is a binary operation on P.

Operation (or composition) Table

Let S be a finite set and the number of elements of S be small. We can construct a table, known as the operation (or composition) table, as follows.

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

We write the elements a_1, a_2, a_3 in a horizontal row as well as in a vertical column and write the binary operation $*$ in the top left corner. Now we enter each of the 9($= 3^2$) entries a_i x a_j (i = 1, 2, 3; j = 1, 2, 3) in the (i, j) th cell as shown in Table 2.1. Each of the 9 entries belongs to A, since $*$ is a binary operation on A.

$*$	a_1	a_2	a_3
a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$
a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$
a_3	$a_3 * a_1$	$a_3 * a_2$	$a_3 * a_3$

Table 2.1

Example 4: Is multiplication a binary operation on {–1, 0, 1} ?

Solution: Each of the 9 entries belongs to A

$\therefore$ multiplication is a binary operation on {–1, 0, 1}.

x	–1	0	1
–1	1	0	–1
0	0	0	0
1	–1	0	1

Table 2.2

Example 5: Is addition a binary operation on {–1, 0, 1} ?

Solution: $-2 \notin \{-1, 0, 1\}$

$2 \notin \{-1, 0, 1\}$

$\therefore$ addition is not a binary operation on {–1, 0, 1}.

+	–1	0	1
–1	–2	–1	0
0	–1	0	1
1	0	1	2

Table 2.3

Example 6: Is $*$ defined by $a * b=|a-b|$ a binary operation on {0, 1, 2} ?

$*$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

Table 2.4

Solution: $0 * 0 = |0-0|=0$,

$0 * 1 = |0-1|=1$,

$0 * 2 = |0-2|=2$;

$1 * 0 = |1-0|=1$, $1 * 1 = |1-1|=0$,

$1 * 2 = |1-2|=1$;

$2 * 0 = |2-0|=2$, $2 * 1 = |2-1|=1$, $2 * 2 = |2-2|=0$,

From the table we see that $*$ is a binary operation on {0, 1, 2}.

2.3.1 Commutative Binary Operation

A binary operation $*$ on a non-empty set S is commutative if $a * b = b * a, \forall a, b \in S$.

Note : For a finite set, a binary operation is commutative if and only if the entries in the operation table are symmetric with respect to the principal diagonal.

For example, the entries in Table 2.3 are symmetric with respect to the principal diagonal 0, 0, 0. Therefore, $*$, defined in Example 6, is commutative on {0, 1, 2}.

Example 7: Is the binary operation $*$ defined by $a * b = a-b+5$ commutative on Z ?

Solution: We have $a * b = a-b+5$

$b * a = b-a+5, \forall a, b \in Z$

Clearly $a * b \neq b * a$

$\therefore *$ is not commutative on Z.

Example 8: Let Q be the set of rational numbers. Let $*$ be a binary operation on Q defined by $a * b = ab^2, \forall a, b \in Q$. Is $*$ commutative?

Solution: $a * b = ab^2$, $b * a = ba^2$, $\forall$ $a, b \in Q$

$\therefore a * b \neq b * a$

$\therefore *$ is not commutative.

2.3.2 Associative Binary Operation

A binary operation $*$ on a non-empty set S is associative if $(a * b) * c = a * (b * c)$, $\forall a, b, c \in S$.

Example 9: Is the binary operation $*$ defined by $a * b = a–b+5$ associative on Z ?

Solution: Let $a, b, c \in Z$.

$(a * b) * c = (a–b+5) * c$

$= (a–b+5) – c+5$

$= a–b–c+10$

$a * (b * c) = a * (b–c+5)$

$= a – (b–c+5)+ 5$

$= a – b + c – 5 + 5$

$= a – b + c$

$\therefore (a * b) * c \neq a * (b * c)$

$\therefore *$ is not associative.

Example 10: Let X be the set of rational numbers excluding 1. We define $*$ on X as follows.

$a * b = a + b – ab$, $\forall a, b \in X$.

Show that $*$ is a binary operation on X. Examine if $*$ is (i) commutative, (ii) associative.

Solution: Let $a, b \in X$

$\therefore$ a, b are two rational numbers and $a \neq 1$, $b \neq 1$.

Now $a + b – ab$ is a rational number and $a+b–ab \neq 1$, for if $a+b–ab=1$, then

$a+b–ab–1=0$

i.e. $(a–1)–b(a–1)=0$

i.e. $(a–1)(1–b)=0$

i.e. $a–1=0$ or $1–b=0$

i.e. a = 1 or b = 1, which is a contradiction.

$\therefore a+b–ab \in X$

i.e $a * b \in X$, $\forall a, b \in X$

$\therefore *$ is a binary operation on X

Second Part

$a * b = a+b-ab$

$= b+a-ba$

$= b * a$

$\therefore *$ is commutative on X.

Again $(a * b) * c$

$= (a+b-ab) * c$

$= (a+b-ab) + c - (a+b-ab)c$

$= a+b-ab+c - ac-bc+abc$

$= a+b+c-ab-bc-ca+abc$

$a*(b*c) = a * (b+c-bc)$

$= a+(b+c-bc) - a(b+c-bc)$

$= a+b+c-ab-bc-ca+abc$

$\therefore (a*b) * c = a * (b*c)$

$\therefore *$ is associative.

2.3.3 Identity Element

Let S be a non-empty set equipped with a binary operation $*$. An element $e \in S$ is called an identity element for $*$ if

$$a * e = a = e * a, \forall a \in S.$$

Note: Identity element for a binary operation if it exists, is unique.

Examples

1. Multiplication is a binary operation on IN. There exists $1 \in$ IN such that

$$a\ 1 = a = 1\ a, \forall\ a \in \text{IN}$$

$\therefore$ 1 is the identity for multiplication in IN.

2. Addition is a binary operation on Z.

There exists $0 \in Z$ such that

$$a + 0 = a = 0+a, \forall a \in Z$$

$\therefore$ 0 is the identity for addition in Z.We say that 0 is the additive identity in Z.

3. Addition is a binary operation on IN. But there does not exist identity

element for addition in IN.

4. Matrix addition is a binary operation on M_{mxn}, the set of all m x n real matrices. The m x n null matrix 0 is the identity for matrix addition in M_{mxn}.

2.3.4 Inverse of an Element

Let S be a non-empty set equipped with a binary operation $*$, and with identity element e. An element $b \in S$ is called inverse of a under $*$ if

$$a * b = e = b * a$$

Note : 1. Inverse of an element under a binary operation, if it exists, is unique.

2. Generally inverse of a is denoted by a^{-1}. In case of real numbers, inverse of a under addition (i. e. additive inverse) is denoted by –a, whereas inverse of a ($a \neq 0$) under multiplication (i.e. multiplicative inverse) is denoted by $\frac{1}{a}$.

Examples

1. Multiplication is a binary operation on IN and $1 \in$ IN is the identity for multiplication. But no element of IN, except 1, possesses inverse under multiplication in IN.
2. Addition is a binary operation on Z and $0 \in Z$ is the identity for addition. For every $a \in Z$, there exists $-a \in Z$ such that
   $a+(-a) = 0=(-a) + a$.
   $\therefore$ –a is the inverse of a under addition.



CHECK YOUR PROGRESS

Q 1: Let A be a finite set having 4 elements. What is the number of binary operations on A?

Q 2: Is $*$ defined by $a * b = \frac{a}{b}$, a binary operation on IR ?

Q 3: Is multiplication a binary operation on {–1, 1, i, –i} ? where $i = \sqrt{-1}$.

Q 4: Let Q be the set of rational numbers. Show that $*$ defined by

$a * b = a + ab$, is a binary operation on Q.

Examine if $*$ is (i) commutative, (ii) associative.



2.4 LET US SUM UP

- A binary operation $*$ on a non-empty set S is a function from S x S to S.
- If S is a finite set having m elements, the number of binary operations on S is m^{m^2}.
- A binary operation $*$ on a non-empty set S is commutative if $a * b = b * a$, $\forall$ a, b$\in$S.
- A binary operation $*$ on a non-empty set S is associative if $(a * b) * c = a * (b * c)$, $\forall$ a, b, c $\in$ S
- An element e in a non-empty set S equipped with a binary operation $*$ is called an identity element for x if $a * e = a = e * a$, $\forall$ a $\in$ S.
- An element b in a non-empty set S equipped with a binary operation $*$ is called an inverse element of a $\in$ S if $a * b = e = b * a$.



2.5 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS

Ans to Q No 1: $4^{4^2} = 4^{16}$

Ans to Q No 2: No.

Ans to Q No 3: Yes

Ans to Q No 4: Not commutative, not associative.



2.6 FURTHER READING

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.



2.7 MODEL QUESTION

Q 1: Let IR be the set of real numbers. Examine if the binary operation $*$ defined by $a * b = a+5b$; $a, b \in IR$ is (i) commutative, (ii) associative.

Q 2: Let S be a set having 3 elements. How many binary operations can be defined on S?

*** ***** ***

UNIT 3: GROUP

UNIT STRUCTURE

3.1 Learning objectives

3.2 Introduction

3.3 Group

3.4 Properties of group

3.5 Let us Sum Up

3.6 Answers to Check Your Progress

3.7 Further Reading

3.8 Model Questions

3.1 LEARNING OBJECTIVES

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

- define groups
- know properties of group.

3.2 INTRODUCTION

In unit-2, we have studied binary operation in a set. In this unit we will introduce the notion of groups. Group is an algebraic structure, i.e, a non-empty set equipped with a binary operation satisfying certain postulates. Group theory occupies an important position in the study of abstract algebra.

3.3 GROUP

A non-empty set G, equipped with a binary operation $*$ is called a group if the following postulates are satisfied.

(i) Associativity

$(a * b) * c = a * (b * c), \forall a, b, c \in G$

(ii) Existence of Identity

There exists $e \in G$ such that

$a * e = a = e * a, \forall a \in G$.

e is called identity.

(iii) Existence of Inverse

For every $a \in G$, there exists $b \in G$ such that

$a * b = e = b * a$

b is called inverse of a and it is denoted by a^{-1}.

Furthermore, if $*$ is commutative, G is called an Abelian group, after the name of the celebrated Norwegian mathematician Niels Henrik Abel (1802–1829).

Note : 1. In order to be a group, there must be a non-empty set equipped with a binary operation satisfying the postulates mentioned above. Later on, we will simply write 'Let G be a group'. It should be borne in mind that there is a binary operation on G.

2. We will drop the binary operation symbol and simply write ab. It should be borne in mind that this is not our usual multiplication.

3. A non-empty set G equipped with a binary operation is called a semigroup if the binary operation is associative.

Finite and Infinite Groups

A group G is finite if the set G is finite; otherwise it is infinite group.

Order of a group

The number of elements of a finite group G is called the order of G. Symbolically it is denoted by 0(G) or |G|.

Example 1 : Let G = {1}

Clearly multiplication is a binary operation on G.

Moreover, all the postulates for a group are satisfied.

$\therefore$ G is a group under multiplication.

Furthermore, G is an Abelian group.

Example 2: Let G = {–1, 1}, the set consisting of the square roots of unity.

(i) From the table, we see that multiplication is a binary operation on G.

(ii) We know that multiplication of real numbers is associative.

(iii) 1 is the identity under multiplication.

(iv) Every element G possesses inverse in G.

1 is the inverse of 1,

–1 is the inverse of –1.

$\therefore$ G is a group under multiplication.

(v) Moreover, multiplication of real numbers is commutative.

∴ G is an Abelian group.

×	–1	1
–1	1	–1
1	–1	1

Table 3.1

Example 3: Let G = {z : z is complex and $z^n=1$}, i.e. G is the set consisting of the n the roots of unity. ($n \in IN$)

(i) Let $z_1, z_2 \in G$

∴ $z_1^n=1$, $z_2^n=1$

Now $(z_1 z_2)^n = 1$ ∴ $z_1 z_2 \in G$

∴ multiplication is a binary operation on G.

(ii) We know that multiplication of complex numbers is associative.

(iii) There exists $1 \in G$ such that

$1z = z = z1, \forall z \in G$

∴1 is the identity element.

(iv) Let $z \in G$. ∴$z^n = 1$

Now $\frac{1}{z}$ is a complex number and $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1$

$\therefore \frac{1}{z} \in G$

Thus, for every $z \in G$, there exists $\frac{1}{z} \in G$ such that $z \frac{1}{z}=1=\frac{1}{z} z$

∴ $\frac{1}{z}$ is the inverse of z.

∴ G is a group under multiplication of complex numbers.

(v) Moreover, multiplication of complex numbers is commutative.

∴ G is an Abelian group.

Note : We have seen that, for every positive integer n, there exists an Abelian group of order n.

Example 4: Let Z be the set of integers

(i) Let $a, b \in Z$

∴ $a+b \in Z, \forall a, b \in Z$

i.e. addition is a binary operation on Z.

(ii) We know that multiplication of integers is associative.

(iii) We have $0 \in Z$ and $a+0 = a = 0+a, \forall a \in Z$

∴ 0 is the identity.

(iv) For every a $\in$ Z, there exists –a $\in$ Z such that a+(–a) = 0 = (–a) +a.

$\therefore$ Z is a group under addition.

(v) Moreover, addition of real numbers is commutative.

$\therefore$ Z is an Abelian group under addition.

Note : Z is an infinite group.

Some other examples are the following.

- Q is an Abelian group under addition.
- IR is an Abelian group under addition.
- Q_0, the set of non-zero rational numbers is an Abelian group under multiplication.
- IR_0, the set of non-zero real numbers is an Abelian group under multiplication.
- C is an Abelian group under addition.
- C_0, the set of non-zero complex numbers is an Abelian group under multiplication.

Example 5: Let G = $\left\{\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix} : \alpha \in IR\right\}$

(i) Let $A_\alpha = \begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix} \in G,$

$$A_\beta = \begin{pmatrix}\cos\beta & -\sin\beta\\ \sin\beta & \cos\beta\end{pmatrix} \in G;\ \ \alpha, \beta \in IR$$

Now $A_\alpha A_\beta$ = $\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}\begin{pmatrix}\cos\beta & -\sin\beta\\ \sin\beta & \cos\beta\end{pmatrix}$

$$= \begin{pmatrix}\cos(\alpha+\beta) & -\sin(\alpha+\beta)\\ \sin(\alpha+\beta) & \cos(\alpha+\beta)\end{pmatrix} = A_{\alpha+\beta} \in G$$

i.e. matrix multiplication is a binary operation on G.

(ii) We know that matrix multiplication is associative.

(iii) We have $I = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

$$= \begin{pmatrix}\cos 0 & -\sin 0\\ \sin 0 & \cos 0\end{pmatrix} \in G$$

and $A_\alpha I = A_\alpha = IA_\alpha, \forall A_\alpha \in G$.

$\therefore$ I is the identity element

(iv) We have $|A_\alpha| = \begin{vmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{vmatrix}$

$= \cos^2\alpha + \sin^2\alpha = 1 \neq 0$

$\therefore A_\alpha^{-1}$ exists.

$\therefore \text{adj} A_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$

$\therefore A_\alpha^{-1} = \frac{1}{|A_\alpha|} adj\ A_\alpha$

$= \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} \in G$

$\therefore$G is a group under matrix multiplication.

(v) Moreover, $A_\alpha A_\beta = A_{\alpha+\beta} = A_{\beta+\alpha} = A_\beta A_\alpha$

$\therefore$ G is an Abelian group.

Example 6: Let G = $\left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} : x \in IR,\ x \neq 0 \right\}$

(i) Let $\begin{pmatrix} x & x \\ x & x \end{pmatrix} \in G,\ \begin{pmatrix} y & y \\ y & y \end{pmatrix} \in G$

x, y $\in$ IR, $x \neq 0,\ y \neq 0$

Now $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in G,$ xy $\in$ IR, xy $\neq 0$

(ii) We know that matrix multiplication is associative.

(iii) We have $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \in G$

and $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{x}{2}+\frac{x}{2} & \frac{x}{2}+\frac{x}{2} \\ \frac{x}{2}+\frac{x}{2} & \frac{x}{2}+\frac{x}{2} \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$\therefore \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ is the identity element

(iv) For every $\begin{pmatrix} x & x \\ x & x \end{pmatrix} \in G$ we have $\begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} \in G$

such that $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$\therefore \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix}$ is the inverse of $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$.

$\therefore$ G is a group under matrix multiplication.

(v) Moreover, $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix}$

$$= \begin{pmatrix} 2yx & 2yx \\ 2yx & 2yx \end{pmatrix}$$

$$= \begin{pmatrix} y & y \\ y & y \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

$\therefore$ G is an Abelian group.

Note : In the above example, the identity element is $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$.

Example 7: Let G be the set of rational numbers excluding 1. We define $*$ on G as follows.

$$a * b = a+b-ab, \ \forall \ a, b \in G$$

(i) $*$ is a binary operation on G

[Ref : Example 10 in [unit 2]

(ii) $*$ is associative on G

[Ref : Example 10 in [unit 2]

(iii) We have $0 \in$ G and

$a * 0 = a + 0 - a0 = a$

$0 * a = 0 + a - 0a = a$

$\therefore$ 0 is the identity under $*$.

(iv) For every $a \in G$, there exists $\frac{a}{a-1} \in G$ such that.

$$a * \frac{a}{a-1} = 0 = \frac{a}{a-1} * a$$

$\therefore \frac{a}{a-1}$ is the inverse of a under $*$.

$\therefore$ G is a group commutative.

[Ref : Example 10 in [unit 2]

$\therefore$ G is an Abelian group.

3.4 PROPERTIES OF GROUP

Theorem 1: Let G be a group. Then

(i) identity element is unique;

(ii) inverse of each element in G is unique;

(iii) $(a^{-1})^{-1} = a$, for all $a \in G$, where a^{-1} denotes the inverse of a,

(iv) $(ab)^{-1} = b^{-1}a^{-1}$, for all $a, b \in G$

(v) $ab = ac \Rightarrow b = c$, (left cancellation law)

$ba = ca \Rightarrow b = c$, (right cancellation law) for all $a, b, c \in G$.

Proof (i) If possible, let e, f be two identities of G.

$\therefore ef = e = fe$ [$\because$ f is identity]

Again $ef = f = fe$ [$\because$ e is identity]

$\therefore e = f$

Thus, identity element is unique.

Note : In view of the above theorem, we write the identity, not 'an identity'.

(ii) Let $a \in G$ and e be the identity of G.

If possible, let b and c be two inverses of a.

$\therefore ab = e = ba$ [$\because$ b is inverse of a]

$ac = e = ca$ [$\because$ c is inverse of a]

Now $b = be$ [$\because$ e is the identity}

$= b(ac)$ [$\because$ $e = ac$]

$= (ba)c$ [by associativity]

$= ec$ [$\because$ e is the identity]

$= c$

Thus, inverse of a is unique.

Note : In view of the above theorem, we write 'the inverse of a', not ' an inverse of a'.

(iii) We have $aa^{-1} = e = a^{-1}a$

$\therefore$ a^{-1} is the inverse of a, and vice versa, a is the inverse of a^{-1} i.e. $(a^{-1})^{-1} = a$

(iv) Let e be the identity of G and $a, b \in G$

Now $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$

$= a\ e\ a^{-1}$

$= aa^{-1}$

$= e$

$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b$

$= b^{-1}\ eb$

$= b^{-1}\ b$

$= e$

$\therefore$ $b^{-1}a^{-1}$ is the inverse of ab, i.e. $(ab)^{-1} = b^{-1}a^{-1}$

(v) We have $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b=(a^{-1}a)c$, [by associativity]

$\Rightarrow eb = ec$

$\Rightarrow b = c$, [$\because$ e is the identity]

Again $ba = ca$

$\Rightarrow (ba)a^{-1} = (ca)\ a^{-1}$

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$ [by associativity]

$\Rightarrow be = ce$

$\Rightarrow b = c$ [$\because$ e is the identity]

Example 8: If, in a group G, every element is its own inverse, prove that G is Abelian.

Solution: Let G be a group. Let $a, b \in G$

$\therefore$ $a^{-1} = a$, $b^{-1} = b$ (given)

Now $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ [Theorem 1 (iv)]

$\therefore$ G is Abelian

Example 9: Prove that a group G is Abelian if and only if $(ab)^2 = a^2b^2$, for all $a, b \in G$.

Solution: $(ab)^2 = a^2 b^2$

$\Leftrightarrow$ (ab) (ab) = (aa) (bb)

$\Leftrightarrow$ a(ba)b = a(ab)b

$\Leftrightarrow$ (ba)b = (ab)b, [by left cancellation law]

$\Leftrightarrow$ ba = ab, [by right cancellation law]

$\Leftrightarrow$ G is Abelian.



CHECK YOUR PROGRESS

Q 1: Show that the set G = {1, ω, ω^2} consisting of the cube roots of unity is a group under usual multiplication. (ω is a complex cube root of unity).

Q 2: Show that the set G consisting of all 2 x 2 non-singular matrices over reals is a group under matrix multiplication.

Q 3: Let G = $\left\{\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in IR,\ x \neq 0\right\}$

Show that G is an Abelian group under matrix multiplication.

Q 4: If for every element a in a group G, $a^2 = e$; prove that G is Abelian. (e is the identity of G).



3.5 LET US SUM UP

- A group is an algebraic structure i.e., a non-empty set equipped with a binary operation satisfying certain postulates.
- Elementary Properties of a group are discussed



3.6 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS

Ans to Q No 1: Left as an exercise

Ans to Q No 2: Left as an exercise

Ans to Q No 3: Left as an exercise

Ans to Q No 4: Left as an exercise



3.7 FURTHER READING

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

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

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

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

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



3.8 MODEL QUESTION

Q 1: Let G be the set of odd integers. A binary operation $*$ on G is defined as follows $a * b = a+b-1$; $a, b \in G$.
Show that G is an Abelian group under $*$.

Q 2: Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$, for all $a, b \in G$.

*** ***** ***

UNIT 4: SUBGROUP

UNIT STRUCTURE

4.1 Learning objectives

4.2 Introduction

4.3 Sub group

4.4 Cyclic Group

4.5 Let us Sum Up

4.6 Answers to Check Your Progress

4.7 Further Reading

4.8 Model Questions

4.1 LEARNING OBJECTIVES

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

- subgroups
- cyclic groups

4.2 INTRODUCTION

In unit 3,we discussed the concept of group and its properties.In this unit,we will discuss subgroup and its properties.In this unit, We will also discuss cyclic group.

4.3 SUBGROUP

Let us consider the set Z of integers.

We know that Z is a group under addition.

Let $2Z = \{0, \pm 2, \pm 4, ...\}$ be the set of even integers.

Clearly 2Z is a non-empty subset of Z.

Moreover, 2Z is also a group under addition.

In this case, 2Z is said to be a subgroup of Z.

Definition : A non-empty subset H of a group G is a subgroup of G if H is also a group under the same binary operation of G. Symbolically, we write $H \leq G$.

Note : (1) If e is the identity of G, {e} is also a subgroup of G, called the trivial subgroup of G. All other subgroups are nontrivial.

(2) G itself is a subgroup of G, called the improper subgroup of G. All other subgroups are proper. [John B. Fraleigh, A First Course in Abstract Algebra (First Indian Reprint, 2003)]

Example 1: Let us consider G = {–1, 1, –i, i}, i = $\sqrt{-1}$

We know that G is a group under multiplication,

Let H = {–1, 1}.

We have H $\subseteq$ G.

Also H is group under multiplication

$\therefore$ H $\leq$ G.It is a proper subgroup of G.

Note : The set of real numbers IR is a group under addition. The set IR_+ of positive real numbers is a group under multiplication. IR_+ is a subset of IR, but not a subgroup of IR. Binary operations are different.

Theorem 3: Let H be a subgroup of a group G. Then

(i) the identity element of H is the identity element of G;

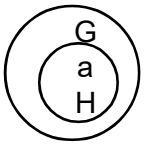
(ii) the inverse of any element of H is the same as the inverse of the element of G.

Proof : Let G be a group and H$\leq$G.

(i) If possible, let e be the identity of G, and f be the identity of H.

Let a $\in$ H.

$\therefore$ af = a = fa [$\because$ f is the identity of H]



Again a $\in$ H $\Rightarrow$ a $\in$ G.

$\therefore$ ae = a = ea [$\because$ e is the identity of G]

$\therefore$ af = ae

$\Rightarrow$ f = e [by left cancellation law]

(ii) Let e be the identity of G

$\therefore$ e is also the identity of H.

Let a $\in$ H.

If possible, let b be the inverse of a in H, and c be the inverse of a in G.

$\therefore$ ab = e = ba

ac = e = ca

$\therefore$ ab = ac$\Rightarrow$ b = c [by left cancellation law]

Note : If H, K are two subgroups of a group G and e is the identity of G, then e is also the identity of H as well as of K. So, H and K have at least one common element, viz., the identity element. Thus, we can conclude that there cannot be two disjoint subgroups of a group.

Theorem 1 : A non-empty subset H of a group G is a subgroup of G if and only if a, b $\in$ H $\Rightarrow$ $ab^{-1} \in H$.

Proof : Let H $\leq$ G and a, b $\in$ H.

b $\in$ H $\Rightarrow$ $b^{-1} \in$ H [$\because$ H is a group]

Now a $\in$ H, $b^{-1} \in$ H

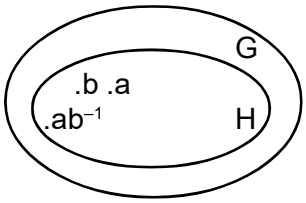
$\therefore$ $ab^{-1} \in$ H

Conversely, let H $\subseteq$ G such that a, b $\in$ H $\Rightarrow$ $ab^{-1} \in$ H

(i) Now a, a $\in$ H $\Rightarrow$ $aa^{-1} \in$ H (by the given condition)

$\Rightarrow$ e $\in$ H,

where e is the identity of G.



(ii) e $\in$ H, a $\in$ H $\Rightarrow$ $ea^{-1} \in$ H

$\Rightarrow$ $a^{-1} \in$ H

$\therefore$ every element of H has inverse in H.

(iii) b $\in$ H $\Rightarrow$ $b^{-1} \in$ H by (ii)

Now a $\in$ H, $b^{-1} \in$ H $\Rightarrow$ $a(b^{-1})^{-1} \in$H (Since $(b^{-1})^{-1} \in$H)

$\Rightarrow$ ab $\in$ H

(iv) The binary operation is associative in H as it is associative in G.

$\therefore$ H is a group under the same binary operation in G. Also H $\subseteq$ G.

$\therefore$ H $\leq$ G.

Note : If G is an additive group, i.e., if G is a group under addition, then a non-empty subset H of G is a subgroup of G if and only if a, b $\in$ H $\Rightarrow$ a–b $\in$H.

Theorem 2 : The intersection of two subgroups of a group is again a subgroup of the group.

Proof : Let G be a group and e be the identity of G.

Let H $\leq$ G, K $\leq$ G.

We note that H $\cap$ K $\neq \phi$,

for at least the identity element e $\in$ H $\cap$ K

Let $a, b \in H \cap K$

$a \in H \cap K \Rightarrow a \in H$ and $a \in K$

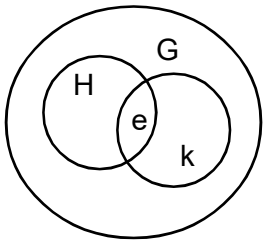
$b \in H \cap K \Rightarrow b \in H$ and $b \in K$

Now $a, b \in H$ and $H \leq G$. $\therefore ab^{-1} \in H$

$a, b \in K$ and $K \leq G$. $\therefore ab^{-1} \in K$

$ab^{-1} \in H$ and $ab^{-1} \in K \Rightarrow ab^{-1} \in H \cap K$

$\therefore H \cap K \leq G$



Note : The union of two subgroups is not necessarity a subgroup.

Let $Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$ be the additive group of integers.

Let $2Z = \{0, \pm 2, \pm 4, \pm 6, ...\}$

$3Z = \{0, \pm 3, \pm 6, \pm 9, ...\}$

Clearly $2Z \leq Z$, $3Z \leq Z$

Now $2 \in 2Z \cup 3Z$, $3 \in 2Z \cup 3Z$

But $2+3 = 5 \notin 2Z \cup 3Z$

$\therefore$ addition is not a binary operation on $2Z \cup 3Z$.

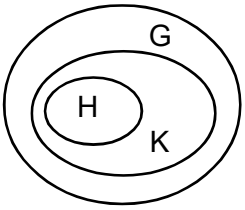
$\therefore 2Z \cup 3Z$ cannot be a group.

Theorem 4 : The union of two subgroups is a subgroup if and only if one of them is contained in the other.

Proof : Let G be a group and $H \leq G$, $K \leq G$.

Let $H \subseteq K$. Then $H \cup K = K$.

$\because K \leq G$, $\therefore H \cup K \leq G$



Conversely, let $H \leq G$, $K \leq G$ such that $H \cup K \leq G$.

Let e be the identity of G.

We are to prove that either $H \subseteq K$ or $K \subseteq H$

If possible, let it not be true.

$\therefore H \not\subseteq K$ and $K \not\subseteq H$

$\therefore$ there exists $a \in H$ such that $a \notin K$

Also, there exists $b \in K$ such that $b \notin H$

Now $a \in H \Rightarrow a \in H \cup K$

$b \in K \Rightarrow b \in H \cup K$

$\because H \cup K \leq G, \therefore ab \in H \cup K$

This $\Rightarrow ab \in H$ or $ab \in K$

If $ab \in H$, then $a \in H$, $ab \in H \Rightarrow a^{-1}(ab) \in H$

$\Rightarrow (a^{-1}a)b \in H$

$\Rightarrow eb \in H$

$\Rightarrow b \in H,$

which is a contradiction.

Similarly, if $ab \in K$, then $ab \in K, b \in K \Rightarrow (ab)b^{-1} \in K$

$\Rightarrow a(bb^{-1}) \in K$

$\Rightarrow ae \in K$

$\Rightarrow a \in K$

which is a contradiction.

So, our assumption is wrong.

$\therefore$ either $H \subseteq K$ or $K \subseteq H$.



CHECK YOUR PROGRESS 1

Q 1: Is the multiplicative group IR_+ of positive real numbers a subgroup of the additive group IR of real numbers? Justify your answer.

Q 2: Can there be two disjoint subgroups of a group? Justify your answer.

Q 3: Can an Abelian group have a non-Abelian subgroup ?

Q 4: Let Z be the additive group of integers. Let m be a fixed integer. Show that the set.

$m Z = \{0, \pm m, \pm 2m, \pm 3m, ...\}$ is a subgroup of Z.

Q 5: Let G be the group consisting of all 2 x 2 non-singular real matrices under matrix multiplication. Let

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in IR \text{ and } ad - bc = 1 \right\}$$

Show that H is a subgroup of G.

Q 6: Give an example to show that a group cannot be expressed as the union of two of its proper subgroups.

4.4 CYCLIC GROUPS

Definition : A group G is said to be cyclic if there exists an element a in G such that every element of G can be expressed in the form a^n, $n \in Z$. a is said to be a generator of G. Symbolically we write G = <a>, i.e., G is a

cyclic group generated by a.We can also write, $G = \{a^n : a \in G, n \in Z\}$

Note : If the group G is additive, every element of G is expressed in the form na.

Examples

(1) We know that G = {–1, 1} is a group under multiplication.

We have $(-1)^1 = -1$, $(-1)^2 = 1$

$\because$ G is a cyclic group generated by –1, i.e. G = <–1>

(2) We know that G = {1, ω, ω^2} is a group under multiplication ; ω is a complex cube root of unity.

We have, $\omega^1 = \omega, \omega^2 = \omega^2, \omega^3 = 1$

.. G is cyclic group generated by ω i.e., G = <ω>

Similarly G = <ω^2>

(3) We know that G = {–1, 1, –i, i} is a group under multiplication.

We have $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$

$\therefore$ G is a cyclic group generated by i , i.e. G = < i >

Similarly G = < – i >

(4) Let Z be the additive group of integers.

Let x $\in$ Z Then x = 1x

$\therefore$ G is a cyclic group generated by 1, i.e. G = < 1 >

Similarly G = < –1 >.

Theorem 5 : Every cyclic group is Abelian.

Proof : Let G = < a > be a cyclic group.

Let x, y $\in$ G.

Then there exist integers m, n such that $x = a^m$, $y = a^n$

Now $xy = a^m a^n$

$= a^{m+n}$

$= a^{n+m}$

$= a^n a^m$

= yx

$\therefore$ G is Abelian.

Theorem 6 : If a is a generator of a cyclic group G, a^{-1} is also a generator of G.

Proof : Let G = < a > be a cyclic group.

Let x, y $\in$ G.

Then there exists integer m such that $x = a^m$

$= (a^{-1})^{-m}$

$\therefore$ G = $< a^{-1} >$.

Division Algorithm for Z

If b is a positive integer and a is any integer, then there exist unique integers q and r such that $a = bq+r$, $0 \leq r < b$

Theorem 7 : A subgroup of a cyclic group is cyclic.

Proof : Let G = <a> be a cyclic group.

Let H $\leq$ G.

Let e be the identity of G.

Case 1. If H = {e}, there is nothing to prove.

Case 2. If H = G, then also the result is obvious,

Case 3. Let H $\neq$ G, H $\neq$ {e}

Each element of H is a power of a.

Let m be the least positive integer such that $a^m \in$ H.

Let x $\in$ H.

Then $x = a^p$ for some p.

Now, by Division Algerithm, there exist unique integers q and r such that

p = mq + r, where $0 \leq r <$m

$\therefore r = p - mq$

$\therefore a^r = a^{p-mq} = a^p (a^m)^{-q} = x(a^m)^{-q}$

Now $x (a^m)^{-q} \in$ H. $\therefore a^r \in$ H.

But m is the least positive integer such that $a^m \in$ H. $\therefore$ r must be 0.

$\therefore$ p = mq

$\Rightarrow x = a^p = a^{mq} = (a^m)^q$

$\therefore$ H = $<a^m>$ is a cyclic group.

Theorem 8 : A group of prime order is cyclic.

Proof : Let G be a finite group, and O (G) = p, where p is a prime number.

Let e be the identity of G.

Let a $\in$ G such that a $\neq$ e

Let H = $\{a^n : n$ is an integer$\}$

Clearly, H is a cyclic subgroup of G.

$\therefore$ by Lagrange's subgroup order theorem, [see unit 6.4]

O (H) divides O (G)

i.e. O(H) divides p

This $\Rightarrow$ O(H) = 1 or p

But O(H) $\neq$ 1, $\because$ a $\neq$ e.

$\therefore$ O (H) = p = O(G)

$\therefore$ H = G

$\therefore$ G is a cyclic group generated by a.

Example 2: Prove that a group of order $\leq$ 5 is Abelian.

Solution: Obviously, a group of order one is Abelian. We know that every group of prime order is cyclic and every cyclic group is Abelian.

$\therefore$ groups of orders 2, 3, 5 are Abelian.

Let us consider group of order 4.

Let G = {e, a, b, c}, where all the elements are distinct, and e is the identity of G.

Clearly, e is its own inverse. Similarly if each of the remaining three elements is its own inverse, then G is Abelian. (Ref. Example 18)

If not, let $b^{-1} = c$, $c^{-1} = b$. Then $a^{-1} = a$

Now let us complete the operation table

$\because$ $a^{-1} = a$ $\therefore$ aa = e

Again, each element of G must appear exactly once in every row or column of the operation table.

$\therefore$ ab = b or ab = c.

Now ab = b $\Rightarrow$ ab = eb $\Rightarrow$ a = e (by right cancellation law), which is a contradiction.

$\therefore$ ab = c, and $\therefore$ ac = b

$\therefore$ b = c^{-1}, $\therefore$ bc = e

$\therefore$ ba = a or ba = c

ba = a $\Rightarrow$ b = e, which is a contradiction

$\therefore$ ba = c, and bb = a

Again, $\because$ c = b^{-1} $\therefore$ cb = e

$\therefore$ ca = a or ca = b

●	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Table 4.1

ca = a $\Rightarrow$ c = e, which is a contradiction.

$\therefore$ ca = b, and $\therefore$ cc = a

We see that the operation table is symmetrical about the principal diagonal.

$\therefore$ G is Abelian.



CHECK YOUR PROGRESS 2

Q 1: How many generators are there of the cyclic group G of order 10?

Q 2: Which of the following groups are cyclic? For each cyclic group list all the generators of the group.

(a) G = <Z, + >

(b) G = < Q, + >

(c) G = < Q^+, + >

(d) G = {6^n : n $\in$ z} under multiplication



4.5 LET US SUM UP

- A non-empty subset H of a group G is a subgroup of G if H is also a group under the same binary operation of G.
- A group G is said to be cyclic if there exists an element a in G such that every element of G can be expressed in the form a^n; n $\in$ Z



4.6 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS – 1

Ans to Q No 1: No,Binary operations are different.

Ans to Q No 2: No. Two subgroups of a group have at least one common element, viz., the identity element.

Ans to Q No 3: No.

Ans to Q No 4: Left as an exercise

Ans to Q No 5: Left as an enexise

Ans to Q No 6: $Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$ is an additive group.

$2Z = \{0, \pm 2, \pm 4, \pm 6, ...\}$

and $3Z = \{0, \pm 3, \pm 6, \pm 9, ...\}$

are two subgroups of Z

$Z \neq 2Z \cup 3Z$.

CHECK YOUR PROGRESS – 2

Ans to Q No 1: Since 1, 3, 7, 9 are relatively prime to 10. Thus, a, a^3, a^7 and a^9 are generators of G.

Ans to Q No 2: Left as an exercise



4.7 FURTHER READING

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.



4.8 MODEL QUESTION

Q 1: Let G be an Abelian group. Prove that the set $H = \{x \in G : x = x^{-1}\}$ is a sub group of G.

Q 2: Show that a group of order 4 is always Abelian.

Q 3: Let g be a group and e be the identity of G. Prove that G is Abelian if $b^{-1}a^{-1}ba = e$, for all $a, b \in G$.

*** ***** ***

UNIT 5 : GROUP OF PERMUTATIONS

UNIT STRUCTURE

5.1 Learning Objectives

5.2 Introduction

5.3 Definition of Permutation, Examples

5.4 Multiplication of Permutation

5.5 Different Kinds of Permutation

5.6 Permutation Group

5.7 Let Us Sum Up

5.8 Answers To Check Your Progress

5.9 Further Reading

5.10 Model Questions

5.1 LEARNING OBJECTIVES

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

- permutation and its examples
- multiplication of permutations
- different kinds of permutation
- permutation group

5.2 INTRODUCTION

The word permutation is used in two different ways. Firstly, it is an ordered arrangement of the elements of a finite set of distinct elements. Secondly, a permutation is a one-one and onto mapping from a non-empty set to itself. In Group theory, permutation is taken as a one-one and onto mapping from a non-empty set to itself. In this unit, we will define a permutation, give examples and obtain the number of permutations from a finite set to itself. We will prove that the collection of permutations on a finite set is a group under multiplication of permutations. This group is called permutation group (or symmetric group).

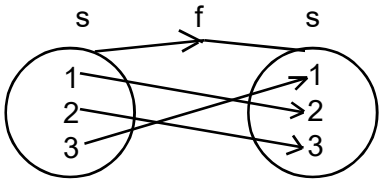
5.3 DEFINITION OF PERMUTATION, EXAMPLES

A bijective mapping (i.e. a one-one and onto mapping) from a non-empty set to itself is called a permutation on the set.

Example 1 : Let us consider the set S = {1, 2, 3}. Let f ; S $\rightarrow$ S be a mapping such that f(1) = 2, f(2) = 3, f(3) = 1

Clearly, f is a one-one and onto mapping from S to itself.

$\therefore$ f is a permutation on S.



Notation for permutation

Let us consider the permutation given above.

S = {1, 2, 3}

f : S $\rightarrow$ S, f(1) = 2, f(2) = 3, f(3) = 1

The above permutation is, generally, written as

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

We write the elements of the set S in the first row. In the second row, we write their respective images. The image of 1 under f is 2. We write 2 just below 1. Similarly the image of 2 is 3. We write 3 just below 2. Similarly, we write 1 just below 3. In this way, a permutation is written.

Number of permutations on S = {1, 2, 3}.

Here S has 3 distinct elements.

Now 1 can be associated in 3 ways. It can be associated with 1 or with 2 or with 3.

2 can be associated in 2 ways.

3 can be associated in 1 way.

$\therefore$ the number of permutations = $3 \times 2 \times 1 = 3!$

Number of permutations on a finite set having n elements

Let us consider a set S having n distinct elements.

The first element can be associated in a ways.

The second element can be associated in (n-1) ways.

The third element can be associated in (n-2) ways.

In this way (n-1)th element can be associated in 2 ways, and the nth element can be associated in 1 way.

$\therefore$ the number of permutations

= n(n-1)(n-2) . . . . . 2.1 = n!

Example 2 : Let S = {1, 2}. Write down all the permutations on S.

Solution : The number of elements of S is 2.

$\therefore$ there are 2!, i.e. 2 permutations on S. They are

$$i = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \qquad f = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Note : The permutation i is called the identity permutation. Here the image of 1 is 1, the image of 2 is 2.

Example 3 : Let S = {1, 2, 3}. Write down all the permutations on S.

Solution : The number of elements of S is 3.

$\therefore$ there are 3!, i.e. 6 permutations on S.

They are

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Note : In this case $i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

is the identity permutation.

Identity permutation

Let S = {a_1, a_2, ..., a_n} where all the a_i's are distinct.

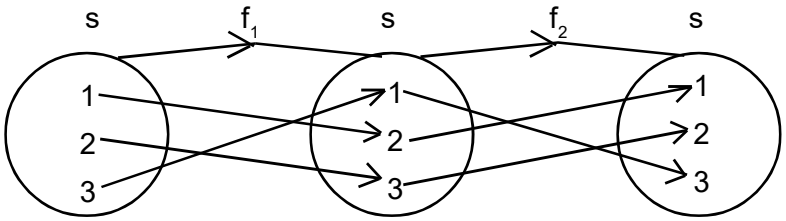
The identity permutation i on S is defined by

$$i = \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ a_1 & a_2 & a_3 .....a_n \end{pmatrix}$$

5.4 MULTIPLICATION OF PERMUTATION

Let S = {1, 2, 3}. Let us consider the following two permutations on S

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$



Then we get the composite mapping

$f_2of_1 : S \to S$, such that

$(f_2of_1)(1) = f_2(f_1(1)) = f_2(2) = 1$

$(f_2of_1)(2) = f_2(f_1(2)) = f_2(3) = 2$

$(f_2of_1)(3) = f_2(f_1(3)) = f_2(1) = 3$

Clearly, f_2of_1 is a permulation on S, and $f_2of_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

Similarly f_1of_2 is also a permutation on S.

The product f_2f_1 of permutations is defined by the composite mapping f_2of_1. Thus

$$f_2 f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Note : 1. We know that the composite mapping of two one-one and onto functions is also a one-one and onto function. Therefore, the product of two permutations is always a permutation.

2. We know that the composition of mappings is associative. Therefore, the multiplication of permutations is associative.

3. We know that the composition of mappings is not, in general, commutative. Therefore, the multiplication of permutations is not, in general, commutative.

Let $$f = \begin{pmatrix} a_1 & a_2 & a_3 & .....a_n \\ f(a_1) & f(a_2) & f(a_3).....f(a_n) \end{pmatrix}$$

$$g = \begin{pmatrix} a_1 & a_2 & a_3 & .....a_n \\ g(a_1) & g(a_2) & g(a_3).....g(a_n) \end{pmatrix}$$

be two permutations on S.

Then $$fg = \begin{pmatrix} a_1 & a_2 & a_3 & ..... a_n \\ f(g(a_1)) & f(g(a_2)) & f(g(a_3)).....f(g(a_n)) \end{pmatrix}$$

Similarly

$$gf = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots\ldots\ldots\ldots & a_n \\ g(f(a_1)) & g(f(a_2)) & g(f(a_3)) & \ldots\ldots & g(f(a_n)) \end{pmatrix}$$

Example 4 : Let S ={1, 2, 3, 4}. Consider the following permutations f and g on S.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},\ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

Find fg and gf

Solution : $fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ f(g(1) & f(g(2) & f(g(3) & f(g(4) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ f(4) & f(2) & f(1) & f(3) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$gf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ g(f(1) & g(f(2) & g(f(3) & g(f(4) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ g(2) & g(3) & g(4) & g(1) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Clearly fg $\neq$ gf [Recall the definition of equality of two functions.]

Example 5 : Let S= {1, 2, 3, 4}. Consider the following permutations on S.

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},\ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

Find $\phi\psi$ and $\psi\phi$

Solution : $\phi\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\psi\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

In this case $\phi\psi = \psi\phi$

Example 6: Let S = {1, 2, 3, 4}. Consider the following permutations on S.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \; h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Find fh and hf

Solution : $fh = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = i$$

$$hf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = i$$

Here fh = hf = i

Note : In the above example fh=hf = i, the identity permutation f is called the inverse of h, and vice versa, h is the inverse of f. We write $f = h^{-1}$ or $h = f^{-1}$

Inverse of a permutation

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

Let $f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ f(a_1) & f(a_2) & f(a_3) \ldots & & f(a_n) \end{pmatrix}$ be a permutation on f.

Then the inverse of f, denoted by f^{-1}, is given by

$$f^{-1} = \begin{pmatrix} f(a_1) & f(a_2) & f(a_2) \ldots & & f(a_n) \\ a_1 & a_2 & a_3 & \ldots & a_n \end{pmatrix}$$

We note that $ff^{-1} = f^{-1}f = i$



CHECK YOUR PROGRESS

Q 1: Let S = $\{a_1, a_2, a_3\}$, where all the a_i's are distinct. How many permutations are there on S? Write down all the permutations on S.

Q 2: Let S = {1, 2, 3, 4}. How many permutations are there on S ? Write down any five permutations on S.

Q 3: Let S = {1, 2, 3, 4, 5}. Consider the following permutations on S.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}, \quad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$$

(i) Find $fg,\ f\phi,\ f\psi,\ g\psi$

(ii) Find $g\phi,\ \phi g$. Are they equal ?

(iii) Find $\phi\psi,\ \psi\phi$. Are they equal?

Q 4: Let S = {1, 2, 3, 4, 5, 6, 7}. Write down the inverse of each of the following permutations on S.

(i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$

(ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

(iii) $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix}$

5.5 DIFFERENT KINDS OF PERMUTATION

Cyclic Permutation

Let S be a finite set. Let f be a permutation on S. f is called a cyclic permutation if there exist elements $a_1, a_2, a_3, \ldots, a_{n-1}, a_n$ in S such that $f(a_1) = a_2$, $f(a_2) = a_3$, $f(a_3) = a_4$, ..., $f(a_{n-1}) = a_n$, $f(a_n) = a_1$, and all other elements, if any, remain fixed under f, i.e., f(a) = a, for all other $a \in S$.

In this case we denote f by $(a_1, a_2, a_3 \ldots . a_n)$.

f is called a cyclic permutation of length n.

Note : A cyclic permutation is also called a cycle. A cyclic permutation of length n is called an n-cycle.

Transposition

A cyclic permutation of length 2 is called a transposition.

Example 7: Let S ={1, 2, 3}

Let $f=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ be a permutation on S.

Here f(1) = 2, f(2) = 3, f(3) = 1

$1\to 2\to 3\to 1$

Thus, $f=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=(1 \quad 2 \quad 3)$

f is a cyclic permutation of length 3 or a 3-cycle.

Example 8 : Let S = {1, 2, 3, 4, 5}. Let

$f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 4 & 2 & 5\end{pmatrix}$ be a permutation on S.

Here f(2) = 3, f(3) = 4, f(4) = 2

$2\to 3\to 4\to 2$

And f(1) = 1, f(5) = 5

i.e, 1, 5 remain fixed under f, i.e. f(1) = 1, f(5) = 5

Thus, $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 4 & 2 & 5\end{pmatrix}=(2 \quad 3 \quad 4)$

f is a cyclic permutation of length 3 or a 3-cycle.

Example 9 : Let S = {1, 2, 3, 4}. Let

$f=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 2 & 4\end{pmatrix}$ be a permutation on S

Here f(2) = 3, f(3) = 2

$2\to 3\to 2$

And f(1) = 1, f(4) = 4

Thus, $f=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 2 & 4\end{pmatrix}=(2 \quad 3)$

f is a cyclic permutation of length 2, i.e. f is a transposition.

Note : Let S = {1, 2, 3}

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3) \qquad (1)$$

is a cyclic permutation on S = (1, 2, 3}.

Now, we consider

S = {1, 2, 3, 4, 5}

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1 \quad 2 \quad 3) \qquad (2)$$

is a cyclic permutation on S = {1, 2, 3, 4, 5}.

We note that (1) and (2) are different permutations. In (2), (1 2 3) means the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

Cycles of a permutations

Let S = {1, 2, 3}

Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3)$

be a permutation of S = {1, 2, 3}

Now $(1 \quad 3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $(1 \quad 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$$(1 \quad 3)(1 \quad 2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3)$$

Thus, we see that

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3) = (1 \quad 3)(1 \quad 2)$$

Again, we consider S = {1, 2, 3, 4, 5}

Let $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1 \quad 2 \quad 3 \quad 4 \quad 5)$

be a permutation on S = {1, 2, 3, 4, 5}

Now, it can be shown that

$g = (1 \quad 2 \quad 3 \quad 4 \quad 5)$

$= (1 \quad 5)(1 \quad 4)(1 \quad 3)(1 \quad 2)$

Again, we consider S = {1, 2, 3, 4, 5, 6}

Let $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}$

be a permutation on S = {1, 2, 3, 4, 5, 6}

Now h can be expressed as

$h = (1 \quad 2 \quad 3)(4 \quad 5 \quad 6)$

Here $(1 \quad 2 \quad 3), (4 \quad 5 \quad 6)$ are called the cycles of the permutation h. Here $(1 \quad 2 \quad 3)$ and $(4 \quad 5 \quad 6)$ have no common elements. They are called disjoint cycles.

Disjoint Permutations

Let S = {1, 2, 3, 4, 5, 6}

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix}$

$= (1 \quad 2 \quad 3)$

and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix}$

$= (4 \quad 5 \quad 6)$

be two permutations on S = {1, 2, 3, 4, 5, 6}

We note that $(1, \quad 2, \quad 3)$, and $(4, \quad 5, \quad 6)$ have no common elements. In this case, the permutations f, and g are said to be disjoint.

Again, consider the permutations

$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix} = (1 \quad 2 \quad 3 \quad 4)$

$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 6 & 3 \end{pmatrix} = (3 \quad 4 \quad 5 \quad 6)$

on S = {1, 2, 3, 4, 5, 6}

Here $(1 \quad 2 \quad 3 \quad 4)$ and $(3 \quad 4 \quad 5 \quad 6)$ have common elements. So, the permutations ϕ and ψ are not disjoint.

Thus, we define disjoint permutations as follows.

Two permutations f and g on a finite set S are said to be disjoint if

(i) $f(a) \neq a \Rightarrow g(a) = a,$ for any $a \in S$.

and (ii) $g(a) \neq a \Rightarrow f(a) = a$, for any $a \in S$.

It can be proved that multiplication of two disjoint cycles, as well as of two disjoint permutations is commutative.

Even and odd permutations

Let S = {1, 2, 3}

$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ is a permutation on S = {1, 2, 3}

Again $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3) = (1 \quad 3) = (1 \quad 2)$

Again, consider the set S = {1, 2, 3, 4}

Let $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ be a permutation on S = {1, 2, 3, 4}

Now $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1 \quad 2 \quad 3 \quad 4) = (1 \quad 4)(1 \quad 3)(1 \quad 2)$

Thus, we see that f has been expressed as the product of even number of transpositions (two), whereas g has been expressed as the product of odd number of transpositions (three).

If a permutation can be expressed as the product of even number of transpositions, then it is said to be even. On the other hand, if a permutation can be expressed as the product of odd number of transpositions, then it is said to be odd.

The permutation f, given above, is even, whereas the permutation g is odd.

We note the following results without proof.

1. The product of two even permutations is an even permutation.
2. The product of two odd permutation is an even permutation.
3. The product of an even permutation and an odd permutation is an odd permutation.
4. Identity permutation is an even permutation.
5. The inverse of an even permutation is even.
6. The inverse of an odd permutation is odd.



CHECK YOUR PROGRESS

Q 5: Write down all the permutations on the set S = {1, 2, 3}, and pick out the even permutations and the odd permutations.

Q 6: Let S = {1, 2, 3, 4, 5, 6}. Determine whether the following permutations on S are even or odd.

(i) $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 6 & 1 \end{pmatrix}$

(ii) $f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 1 & 4 \end{pmatrix}$

(iii) $f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

(iv) $f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 6 & 3 \end{pmatrix}$

(v) $f_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 2 & 3 & 6 \end{pmatrix}$

Number of even permutations and odd permutations on S = {1, 2, 3, . . . , n}, $n \geq 2$

Let S = {1, 2, 3, ..., n}

Let S_n be the set of all permutations on S. Then number of elements of S_n is n!. Of these n! permutations, some are even and some are odd.

Let the number of even permutations be m, and the number of odd permutations be k.

Clearly, m+k = n!

Let the even permutations be $e_1, e_2, \ldots, e_m$; where the e_i's are distinct.

Let f be any transposition

Then $fe_1, fe_2, \ldots, fe_m$ are odd permutations, and are distinct, for if $fe_i = fe_j$, then $e_i = e_j$, which is a contradiction.

Since the number of odd permutations is k,

$\therefore\ m \leq k$

Interchanging the roles of m, k, we get

$k \le m$

$\therefore \ m = k$

$\because \ m + k = n!, \quad \therefore \ m = k = \frac{n!}{2}$

$\therefore$ Number of even permutations on $S = \frac{n!}{2}$, and number of odd permutations on $S = \frac{n!}{2}$, where S = {1, 2, 3, ..., n}, $m \ge 2$.

5.6 PERMUTATION GROUP

Let S = {1, 2, 3, 4, ... , n}, and let S_n be the set of all permutations on S.

(i) Let $f, g \in S_n$.

We know that the product fg is defined by the composite mapping fog.

Also we know that the composite mapping of two one-one and onto function is also one-one and onto.

Therefore, the product of two permutations is always a permutation .

$\therefore \ fg \in S_n$

(ii) We know that the composition of mappings is associative. Therefore, the multiplication of permutations is associative.

(iii) The identity permutation

$$i = \begin{pmatrix} 1 & 2 & 3 & ..... & n \\ 1 & 2 & 3 & ..... & n \end{pmatrix} \in S_n$$

Also if = f = fi, $\forall f \in S_n$

i is the identity element of S_n.

(iv) Let $f = \begin{pmatrix} 1 & 2 & 3 & ..... & n \\ f(1) & f(2) & f(3) & ..... & f(n) \end{pmatrix} \in S_n$

Now

and fg = i = gf

g is the inverse of f.

We denote g by f^{-1}

i.e., $ff^{-1} = i = f^{-1} f$.

Thus S_n is a group under multiplication of permutations, called the permutation group (or symmetric group) of degree n.

Note : 1) The group

2) The number of elements of S_n is n!, i.e, the order of

Example 10 : Let S = {1, 2, 3}. Let S_3 be the set of all permutations on S. Show that S_3 is a group under product of permutations. Is the group Abelian?

Solution : Let $S_n = \{i, f_1, f_2, f_3, f_4, f_5\}$, where

We construct the operation table as follows :

(i) From the table we see that S_3 is closed under multiplication of permutations.

(ii) We know that multiplication of permutations is associative.

(iii) The identity permutations , and if = f = fi,

(iv) Every element of S_3 possesses inverse in S_3.

The inverse of i is i.

The inverse of f_1 is f_2.

The inverse of f_2 is f_1.

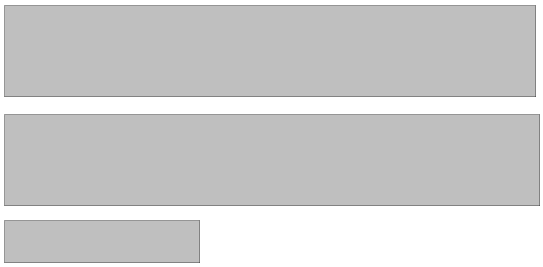
The inverse of f_3 is f_3.

The inverse of f_4 is f_4.

The inverse of f_5 is f_5.

Thus, S_3 is a group under multiplication of permutations.

2nd Part : The group S_3 is not Abelian.



Alternating Group

Let $S = \{1, 2, 3, \ldots, n\}$

Let  $_n$is a group under multiplication of permutations, called the **alternating group** of degree n.

Number of elements of A_n is  $_n$ is 

Clearly A_n is a subgroup of S_n.

Example 11 : Let $S = \{1, 2, 3\}$. Let A_3 be the set of all even permutations on S. Show that A_3 is a group under multiplication of permutations. Is the group Abelian ?

Solution : Let $S = \{1, 2, 3\}$.

Let A_3 be the set of all even permutations.

Let $A_3 = \{i, f_1, f_2\}$, where



i, f_1, f_2 are even permutations.

We construct the operation table as follows.

(i) From the table, we see that A_3, is closed under multiplication of permutations.

(ii) We know that multiplications of permutations is associative.

(iii) The identity permutation , and if = f = fi,

(iv) Every element of A_3 possesses inverse in A_3.

Th inverse of i is i.

The inverse of f_1 is f_2.

The inverse of f_2 is f_1.

Thus, A_3 is a group under multiplication of permutations.

2nd Part : From the table we see that multiplication is commutative.

A_3 is an Abelian group

Note : We have seen that S_3 is a non-Abelian group, whereas A_3 is an Abelian group.

Moreover, A_3 is a subgroup of S_3.

Thus, we can conclude that a non-Abelian group can have an Abelian subgroup.



CHECK YOUR PROGRESS

Q 7: Let S = {1, 2, 3, ..., n}. Is the set of all odd permutations on S a group? Justify.

Q 8: Let S = {1, 2, 3, 4}

Let V = {1, f_1, f_2, f_3}, where

Show that V is group under multiplication of permutations. Is the group Abelion ?

Q 9: Give an example of a finite non-Abelian group.



5.7 LET US SUM UP

- A bijiective mapping (i. e., a one-one and onto mapping) from a non-empty set to itself is called a permutation on the set.
- The number of permutations on a finite set S having n elements is n!.
- Let S be a finite set. Let f be a permutation on S. f is said to be a cyclic permutation of length n if there exist elements $a_1, a_2, a_3, \ldots a_{n-1}, a_n$ in S such that $f(a_1) = a_2$, $f(a_2) = a_3, \ldots ., f(a_{n-1}) = a_n$, $f(a_n) = a_1$, and all other elements, if any, remain fixed under f, i.e., f(a) = a, for all this case f is denoted by $(a_1\ a_2\ a_3 \ldots a_n)$.
- A cyclic permutation of length 2 is called a transposition.
- If a permutation can be expressed as the product of even number of transpositions, then it is said to be even.
- If a permutation can be expressed as the product of odd number of transpositions, then it is said to be odd.
- Let S = {1, 2, 3, ..., n}, and let S_n be the set of all permutations on S. S_n is a group under multiplications of permutations called the permutation group (or symmetric group) of degree n, and of order n!. If A_n is the set of all even permutations on S, then A_n is a group under multiplications of permutations, called the alternating group of degree and of order



5.8 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Here S = $(a_1, a_2, a_3\}$, where all the a_i1s are distinct.

there are 3!, i.e., 3 2



Ans to Q No 2: S = {1, 2, 3, 4}

The number of permutations on S is 4!, i.e., 4 3 2

Any five permutations on S :





Ans to Q No 3: (i) 















(ii) 







Clearly 

(iii) 







Clearly 

Ans to Q No 4: (i) 



(ii) 



(iii) 



Ans to Q No 5: Here S = {1, 2, 3}

The permutations on S are







Even permutations : i, f_1, f_2

Odd permutations : f_3, f_4, f_5.

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

(i)

f_1 is an even permutations.

(ii)

f_2 is an even permutation.

(iii)

f_3 is an odd permutation.

(iv)

f_4 is an odd permutation.

(v)

f_5 is an odd permutation.

Ans to Q No 7: Here S = {1, 2, 3, ..., n}

Let O_n be the set of odd permutations on S.

Let f. g $_n$

We know that the product of two odd permutations is an even permutation.

[redacted]

O_n cannot be a group.

Ans to Q No 8: Here S = {1, 2, 3, 4}

V = {i, f_1, f_2, f_3}, where

[redacted]

(i) From the table we see that V is closed under multiplication of permutations.

(ii) We know that multiplications of permutations is associative.

(iii) We have [redacted]

and if = f = f_1, [redacted].

i is the identity

(iv) Every element of V has inverse in V.

i is the inverse of i.

f_1 is the inverse of f_1.

f_2 is the inverse of f_2.

f_3 is the inverse of f_3.

[Here every element is its own inverse]

V is a group under multiplication of permutations.

2nd Part: From the table we see that multiplication is commutative.

V is an Abelian group

Ans to Q No 9: Let S = {1, 2, 3}

Let S_3 be the set of all permutations on S. Then S_3 is a group under multiplication of permutations.

Clearly S_3 is a finite group of order 3! i.e. 6.

S_3 is not an Abelian group.

5.9 FURTHER READING

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.

5.10 MODEL QUESTIONS

Q 1: Let S = {1, 2, 3}. Show that the set S_2 of all permutations on S is an Abelian group under multiplication of permutations.

Q 2: Let S = {1, 2, 3, 4, 5, 6, 7, 8}.
Express the following permutations on S as product of trenspositions.

(i)

(ii)

Q 3: Let S = {1, 2, 3, 4}
Let V = {1, f_1, f_2, f_3}, where

are permutations on V.
Examine if V is an Abelian group under multiplication of permutations.

Q 4: Prove that the set S_n of all permutations on S = {1, 2, 3, 4, ..., n} is a group under multiplication of permutations.

*** ***** ***

UNIT 6: COSETS

UNIT STRUCTURE

6.1 Learning objectives

6.2 Introduction

6.3 Coset

6.4 Lagrange's Subgroup order theorem

6.5 Let us Sum Up

6.6 Answers to Check Your Progress

6.7 Further Reading

6.8 Model Questions

6.1 LEARNING OBJECTIVES

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

- cosets of a subgroup
- Lagrange's subgroup order theorem

6.2 INTRODUCTION

We have already discussed group ,subgroup and their properties in unit 3 and unit 4.In this unit,we will discuss cosets of a subgroup of a group.

We will also discuss Lagrange's subgroup order theorem in this unit.

6.3 COSET

Let G be a group and H □

Let a□

The set Ha = {ha : h □ .

Similarly, the set aH = {ah : h□ .

Note : (1) Right (or left) coset cannot be empty ,we have e□

□ ea = a □ □ Ha □□

Similarly ae = a □ □ aH □□

(2) H .

(3) If H is a subgroup of the additive group G and a G, the right coset of H in G is given by H+a = {h+a : h

Similarly, the left coset of H in G is given by a+H={a+h : h

(4) If G is abelian,then every left coset is a right coset.

Example : Let us consider the additive group of integers Z.

We know that 2 Z = {0, 2, 4, 6,.....}

We have

0+2 Z = {0, 2, 4,

1+2Z = { 1, 3, 5,

2+2Z = {0, 2, 4,

3+2Z = { 1, 3, 5,

Thus, we see that

2Z = 2+2Z = 4+2Z = ...

1+2Z = 3+2Z = 5+2Z = ...

2Z has two distinct left cosets viz. 2Z and 1+2Z such that

2Z

2Z (1+2Z) =

Similarly, 2Z has two distinct right cosets 2Z and 2Z + 1 such that

2Z

2Z (2Z+1) =

Theorem 1 : Let G be a group and H

(i) aH = H a H; Ha = H a

(ii) aH = bH $^{-1}$b H ; Ha = Hb $^{-1}$ H, where a, b

Proof : (i) Let aH = H

We have ae

ae H [

a

Conversely, let a

Let x

This x = ah, for some h

Now a H, h ah H x

Thus, x x

aH

Again, let y

a H, $^{-1}$

$a^{-1}y$

$a^{-1}y = h_1$, for some h_1 H

$a(a^{-1}y) = ah_1$

$(aa^{-1})y = ah_1$

$ey = ah_1$

$y = ah_1$

Thus, y H y

H

From (1) and (2), aH = H

Similarly Ha = H a

(ii) aH = bH

$a^{-1}(aH) = a^{-1}(bH)$

$(a^{-1}a)H = (a^{-1}b)H$

$eH = (a^{-1}b)H$

$H = (a^{-1}b)H$

$a^{-1}b$

Similarly, Ha = Hb $^{-1}$

Theorem 2 : (i) Any two left (or right) cosets of a subgroup are either disjoint or identical.

(ii) A group G is union of all its right (or left) cosets of a subgroup H of G.

Proof :(i) Let G be a group and H .

Let a, b .

Then aH, bH are two left cosets of H in G.

Clearly aH, bH are either disjoint or not disjoint.

Let aH, bH be not disjoint, i.e, aH bH

Let x aH

x aH and x

Now x aH $_1$ for some h_1

x bH $_2$ for some h_2 H

$ah_1 = bh_2$

$(ah_1)h_1^{-1} = (bh_2)h_1^{-1}$

$a\ h_1h_1^{-1} = b\ h_2h_1^{-1}$

$ae = bh_2h_1^{-1}$, where e is the identity of G

$a = bh_2h_1^{-1}$

Similarly $b = ah_1h_2^{-1}$

Let p aH $_3$ for some h_3

$= bh_2h_1^{-1}h_3$

$_2h_1^{-1}h_3$

Thus, p aH p aH

Again, let q bH $_4$ for some h_4

q $= ah_1h_2^{-1}h_4$

aH, $h_1h_2^{-1}h_4$ H

Thus q q bH

From (1) and (2), aH = bH

Thus, aH, bH are either disjoint or identical.

(ii) Let be a group and let

subgroup of G.Let

Clearly

Also

From (1) and (2),we get

or

6.4 LAGRANGE'S SUBGROUP ORDER THEOREM

Theorem 3 : (Lagrange's subgroup Order Theorem) The order of a subgroup of a finite group divides the order of the group.

Proof : Let G be a finite group, and let O(G) = n

and H G.

Let e be the identity of G.

Case 1 : Let H = {e},

There is nothing to prove. O(H) =1, and 1 divides n.

Case 2 : Let H = G. Hence O(H) = O(G).

There is nothing to prove.

Case 3 : Let H $\subset$ {e}, H $\subset$.

Let O(H) = m, m < n.

Let H = $\{h_1, h_2, h_3, \ldots h_m\}$, where the h_i's are distinct.

Let a $\in$ G, a $\notin$

Let us consider the left coset.

aH = $\{ah_1, ah_2, ah_3, \ldots, ah_m\}$

We claim that all the elements in aH are distinct, for if $ah_i = ah_j$, 1 $\leq$ i $\leq$ m, 1 $\leq$ j $\leq$ m, i $\neq$ $_i=h_j$, (by left cancellation law), which is a contradiction.

Again, no element of H is equal to any element of aH, for if $h_i = ah_j$, then $h_i h_j^{-1} = a$ i.e. $a = h_i h_j^{-1}$ $\in$ H

i.e. a $\in$ H

Thus, we have listed m+m = 2m elements of G. If this exhausts all the elements of G, then 2m = n. $\Rightarrow$ m divides n.

If not, let b $\in$ G, b $\notin$ H, b $\notin$

Let us consider $bH = \{bh_1, bh_2, \ldots, bh_m\}$

Clearly, all the elements in bH are distinct. No element of H is equal to any element of bH.

Again, no element of aH is equal to any element of bH, for if $ah_i = bh_j$, then $ah_i h_j^{-1} = bh_j h_j^{-1}$ i.e $ah_i h_j^{-1} = b$ i.e $b = ah_i h_j^{-1} \in$ aH, ($\in$ $_i h_j^{-1} \in$ H) i.e. b $\in$ H

Thus, we have listed m+m+m = 3m elements of G. If this exhausts all the elements of G, then 3m = n. $\Rightarrow$ m divides n.

If not, we proceed as above. Since G is finite, we must stop somewhere, say, after k times. $\Rightarrow$ mk = n $\Rightarrow$ m divides n.

Note : Joseph Louis Lagrange (1736 – 1813) was a famous mathematician, ''born at Turin of once prosperous parents with French and Italian backgrounds".

Remark : The converse of Lagrange's theorem is not true.



CHECK YOUR PROGRESS

Q 1: Find all cosets of the subgroup 4Z of 2Z.

Q 2: Find all cosets of the subgroup 6Z of 2Z.



6.5 LET US SUM UP

- If H is a subgroup of a group G, the set Ha = {ha : h ∈ H}, a∈ called a right coset of H in G. Similarly, a left coset is defined.
- Any two left (or right) cosets of a subgroup are either disjoint or identical.
- Lagrange's subgroup Order Theorem state that the order of a subgroup of a finite group divides the order of the group.

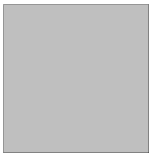


6.6 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS

Ans to Q No 1: Since 2Z is abelian,the left cosets and the right cosets are the same.The left coset containing the integer 0 is [redacted] and left coset containing the integer 2 is [redacted].

Ans to Q No 2: Left as an exercise



6.7 FURTHER READING

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

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

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

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

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

6.8 MODEL QUESTION

Q 1: Let G be a group and H be a subgroup of G. Let a, b G. Show that the two right cosets Ha, Hb are equal if and only if the two left cosets $a^{-1}H$, $b^{-1}H$ are equal.

Q 2 : Find all cosets of the subgroup 4Z of Z.

Q 3: Index of a subgroup. Let G be a group and H be a subgroup of G. The number of distinct left (or right) cosets of H in G is called the index of H in G. Generally it is denoted by [G : H]

If G is a finite group, show that [G : H] =

*** ***** ***

UNIT 7: NORMAL SUBGROUP& QUOTIENT GROUP

UNIT STRUCTURE

7.1 Learning objectives

7.2 Introduction

7.3 Normal Subgroup

7.4 Quotient Group

7.5 Let us Sum Up

7.6 Answers to Check Your Progress

7.7 Further Reading

7.8 Model Questions

7.1 LEARNING OBJECTIVES

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

- normal subgroups
- quotient groups.

7.2 INTRODUCTION

We have already discussed group ,subgroup and their properties in unit 3 and unit 4.In this unit,we will discuss normal subgroup of a group.In this unit,we will also discuss quotient group.

7.3 NORMAL SUBGROUP

Definition : A subgroup H of a group G is said to be a normal subgroup of G if aH = Ha, for all a

Symbolically We write H .

Note : A group G has at least two normal subgroups, viz., G and {e}. A group, having no normal subgroups other than G and {e}, is called a simple group.

Example : Let G ={ –1, 1, –i, i}

We know that G is a group under multiplication.

Let H = {–1, 1}, and H

Now 1H = {–1, 1} = H1

(–1)H = {1, –1} = H (–1)

iH = {–i, i} = Hi

(–i)H = {i, –i} = H (–i)

Thus, aH = Ha, for all a

H .

Note : In the above example, H has two distinct left (or right) cosets, viz H, iH. We note that iH is not a subgroup of G.

Theorem 1 : Every subgroup of an Abelian group is normal.

Proof : Let G be an Abelian group.

Let H .

Let a

Now aH = {ah : h

= {ha : h H} [

= Ha

H .

Theorem 2 : A subgroup H of a group G is a normal subgroup of G if and only if ghg^{-1} H, for all g G, h

Proof : Let H .

aH = Ha, for all a

Let g G, h

gh

gh Hg [

gh = h_1g, for some h_1

$ghg^{-1} = h_1 gg^{-1}$

$ghg^{-1} = h_1$

i.e. ghg^{-1}

Conversely, let H $^{-1}$ H, for all g G, h

Let a G ah

aha^{-1} H, by the given condition

$(aha^{-1})a$

$ah(a^{-1}a)$

ah

aH

Now ha

We take $a^{-1} = b$.

$bhb^{-1} \in H$

$a^{-1}h(a^{-1})^{-1}$

$a^{-1}ha$

$a(a^{-1}ha)$

$(aa^{-1})ha$

ha

Ha

From (1) and (2), aH = Ha

$H \triangleleft G$.

Theorem 3 : The intersection of any two normal subgroup of a group is again a normal subgroup of the group.

Proof : Let G be a group, an $H \triangleleft G$, $K \triangleleft G$.

$H \triangleleft G$, $K \triangleleft G$ and so $H \cap K \triangleleft G$.

Let $g \in G$, $h \in H \cap K$

$h \in H \cap K \Rightarrow h \in H$ and $h \in K$

Now $g \in G$, $h \in H$ and $H \triangleleft G$

ghg^{-1}

Again $g \in G$, $h \in K$ and $K \triangleleft G$

$ghg^{-1} \in K$

Thus, $ghg^{-1} \in H$ and $ghg^{-1} \in K$.

$ghg^{-1} \in H \cap K$

$H \cap K \triangleleft G$.

Note : The union of two normal subgroups is not necessarily a normal subgroup.For example But subgroup of Z.

7.4 QUOTIENT GROUPS

Let G be a group and H be a normal subgroup G.

H is normal in G, therefore, there is no distinction between a left coset and

its corresponding right coset. So, by a coset we mean left coset (or right coset).

Let G/H denote the collection of all cosets of H in G.

Let a, b aH, bH G/H.

We define a binary operation in G/H by the rule (aH)(bH) = abH, ab .

We show that the binary operation is well defined.

Let aH = cH,

bH = dH; a, b, c, d

Now aH = cH a^{-1}(aH) = a^{-1}(cH)

$(a^{-1}a)H = a^{-1}cH$

$H = a^{-1}cH$

$a^{-1}c$

$a^{-1}c = h_1$, for some h_1 H

Similarly bH = dH $^{-1}$d $^{-1}$d = h_2, for some h_2

Now $(ab)^{-1}(cd) = (b^{-1}a^{-1})(cd)$

$= b^{-1}(a^{-1}c)d$

$= b^{-1}h_1d$

$= b^{-1}dh_1$ [

$= h_2h_1$ H

$(ab)^{-1}(cd)H = H$

abH = cdH

Thus,

the binary operation defined above is well defined.

Theorem : Let G be a group and H be a normal subgroup G. The set G/H consisting of all the cosets of H in G is a group under the binary operation defined by

(aH)(bH) = abH ; a, b .

Proof : (i) It is given that the binary operation is (aH)(bH) = abH ; a, b

(ii) Let a, b, c

aH, bH, cH G/H

Now ((aH)(bH)) (cH) = (abH) (cH)

= (ab)c H

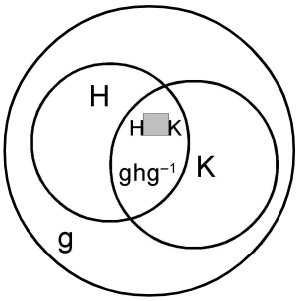
= a(bc)H [

= (aH)((bc)H)

= (aH) ((bH)(cH))

(iii) let e be the identity of G.

eH = H G/H



Now (aH)H = (aH) (eH) = aeH = aH

H (aH) = (eH) (aH) = eaH = aH.

H is the identity.

(iv) a G $^{-1}$ G

$(aH)(a^{-1}H) = (aa^{-1})H = eH = H$

$(a^{-1}H)(aH) = (a^{-1}a)H = eH = H$

$a^{-1}H$ is the inverse of aH.

G/H is a group under the binary operation defined above.

Note : This group is known as the quotient group (or factor group) of G by H.

Theorem 5 : Every quotient group of an Abelian group is Abelian.

Proof : Let G be an Abelian group, and H .

G is Abelian, .

So, we can construct the quotient group G/H.

Let a, b . aH, bH G/H.

Now (aH)(bH) = abH

= baH [

= (bH)(aH)

G/H is Abelian.

Theorem 7 : Every quotient group of a cyclic group is cyclic.

Proof : Let G = <a> be a cyclic group.

Let H

G is cyclic, .

So, we can construct the quotient group G/H.

Let x , xH G/H.

Now $x = a^m$ for some integer m.

Let m > 0

Now $xH = a^m H$

$= (a\ a\ a \ldots\ a)H$

$= (aH)(aH)(aH) \ldots (aH)$

$= (aH)^m$

G/H is a cyclic group generated by aH.

We can prove the result immediately for m = 0 or m < 0.



CHECK YOUR PROGRESS

Q 1: Can a non-Abelian group be cyclic?

Q 2: Show that a non-Abelian group must contain at least six elements.

Q 3: Let G = {1, , } be the multiplicative group; being a complex cube root of unity. Is the group simple?

Q 4: Can a group of order seven be non-Abelian?

Q 5: Let Z be the additive group of integers. The set 3 Z = {0, 3, 6, ...} is a subgroup of Z. Write down the number of elements of the quotient group $Z/3Z$.



7.5 LET US SUM UP

- A subgroup H of a group G is a normal subgroup of G if aH = Ha, for all a .
- If G is a group and H is a normal subgroup of G, the set G/H consisting of all the cosets of H in G is a group, called the quotient group (or the factor group).



7.6 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS

Ans to Q No 1: Every cyclic group is Abelian. Therefore, every non-Abelian group is non-cyclic.

Ans to Q No 3: Yes. It has no normal subgroups other than G, {1}.

Ans to Q No 4: No. Every group of prime order is cyclic and every cyclic group is Abelian.

Ans to Q No 5: Three.

7.7 FURTHER READING

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.

7.8 MODEL QUESTIONS

Q 1: If   is also a normal subgroup of G.

Q 2: Let G = 

Show that G is a non-Abelian group under matrix multiplication.

Let H = 

Show that H is a normal subgroup of G.

Q 3: Show that a group of prime order is simple.

*** ***** ***

UNIT 8 : HOMOMORPHISM OF GROUPS

UNIT STRUCTURE

8.1 Learning Objectives

8.2 Introduction

8.3 Homomorphism of Groups : Definition and examples

8.4 Types of Homomorphism

8.5 Properties of Homomorphism

8.6 Let Us Sum Up

8.7 Answers To Check Your Progress

8.8 Further Reading

8.9 Model Questions

8.1 LEARNING OBJECTIVES

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

- the concept of homomorphism of groups
- different types of homomorphism
- properties of homomorphism, and related theorems.

8.2 INTRODUCTION

The word homomorphism has been derived from two Greek words homos (meaning 'same') and morphe (meaning 'form' or 'shape'). Thus, homomorphism means 'of the same form or shape'.

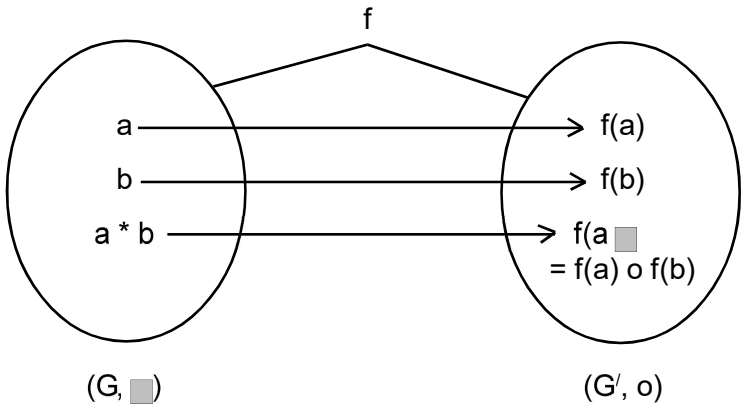
A homomorphism is a structure-preserving mapping between two algebraic structures. Thus, a group homomorphism is a homomorphism that preserves the group structure.

8.3 HOMOMORPHISM OF GROUPS

Definition : Let G be a group under the binary operation' / be a group under the binary operation '

Let f : G -/ be a mapping. f is said to be a homomorphism if

f(a b) = f(a) o f(b),



Note : 1. Here a is related to f(a), b is related f(b). Moreover, a to f(a) o f(b). Thus, the mapping f not only relates two elements of G with two unique elements of G/, but also relates a /. Thus, the mapping f preserves the algebraic structure of the systems.

2. In our subsequent discussions, we will drop the symbols for binary operations. Simply we will write f(ab) = f(a) f(b).

It should be borne in mind that the binary operations in the two groups are not necessarily the same.

Example 1: Let

Let

Now f(a+b) = –(a+b), by definition of f

= – a – b

= (–a) + (–b)

= f(a) + f(b)

f is a homomorphism.

Note : In the above example the binary operation is "+". Moreover, both the groups are the same with same binary operation.

Example 2 : Let R be the additive group of real numbers, and R_+ be the multiplicative group of positive real numbers. We define

f: R $_+$, $f(x) = e^x$

We are to examine whether f is a homomorphism or not. Now, the

binary operation in R is " + ", and the binary operation in R_+ is " . ". So, we are to examine if f(a+b) = f(a) f(b),

Now $f(a+b) = e^{a+b}$, by definition of f

$= e^a e^b$

= f(a) f(b)

f is a homomorphism.

Example 3: Let

Let

Now f(a+b) = (a+b) + 5

f(a) + f(b) = (a+5) + (b+5)

= (a+b) +10

f(a+b)

f is not a homomorphism.

Example 4: Let

multiplicative group. We define

Let

Case I: Let a be even, b be even.

f(a) = 1, f(b) = 1

Also, a + b is even

f (a + b) = 1

= 1 x 1

= f(a) f(b)

Case 2: Let a be odd, b be odd

f(a) = –1, f(b) = –1

a, b are odd, a + b is even

f (a + b) = 1

= (–1) x (–1)

= f(a) f(b)

Case 3: Let a be even, be be odd a + b is odd.

f(a) = 1, f(b) = –1

a is even and b is odd, a + b is odd

f(a + b) = –1

= 1 x (–1)

= f(a) f(b)

Similarly, if a is odd, and b is even, then f(a + b) = f(a) f(b)

Thus, in all the cases

f(a + b) = f(a) f(b)

f is a homomorphism.

Example 5: Let G be a group, and e be the identity of G. We define

such that f(x) = e,

Let

Now f(a) = e, f(b) = e

Also f(ab) = e

= e e (

= f(a) f(b)

f is a homomorphism



CHECK YOUR PROGRESS

Q 1: Let be the additive group of integers.

Define

Examine if f is a homomorphism.

Q 2: Let be the additive group of integers.

Define

Examine if f is a homomorphism.

Q 3: Let be the multiplicative group of positive reals. Define

Examine if f is a homomorphism.

Q 4: Let be the multiplicative group of positive real numbers,

and be the additive group of real numbers. Define

Examine if f is a homomorphism.

Q 5: Let S = {1, 2, 3}, and let S_3 be the group of all permutations of S. Let G = {–1, 1} be the multiplicative group. Define

Examine if f is a homomorphism.

8.4 TYPES OF HOMOMERPHISM

Let f : G / be a homomorphism from a group G to a group G/.

1. A homomorphism f is said to be a monomorphism if f is one-one (i.e. if f is injective).
2. A homomorphism f is said to be an epimorphism if f is onto (i.e. if f is surjective).
3. A homomorphism from a group to itself is called an endomorphism.
4. A homomorphism f is said to be an isomorphism if f is one-one and onto (i.e. if f is bijective).

   The word 'isomorphism' has also been derived from two Greek words "isos" (meaning "equal"). If there exists an isomorphism between two groups, they can be called "abstractly identical". They can be treated as one group, and not as two different groups.
5. An isomorphism from a group to itself is called an automorphism

Example 6: Let

f : , f(x) = – x,

(i) We have proved that f is a homomorphism (Example 1)

(ii) Let

f(a) = f(b)

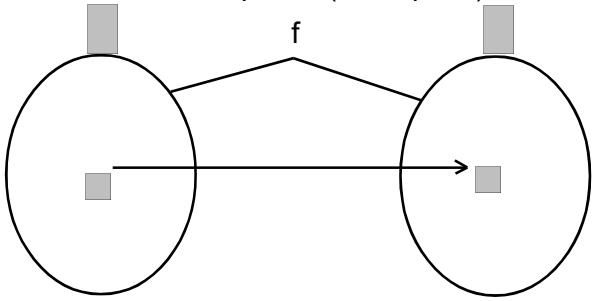
–a = – b

a = b

f is one-one

(iii) Let

Then there exists



(domain) such that

f is onto.

Thus, f is a homomorphism, f is one-one, and f is onto.

f is an isomorphism. Moreover, f is an automorphism, for f is an isomorphism from

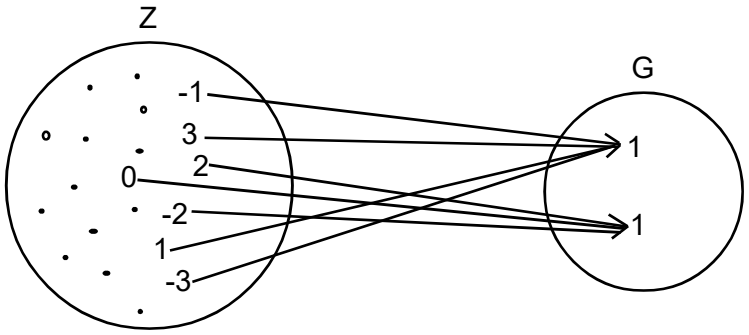
Example 7: Let

multiplicative group. We define

(i) We have proved that f is a homomorphism (Example 4).

(ii) Clearly f is not one-one.

(iii) Clearly f is onto.



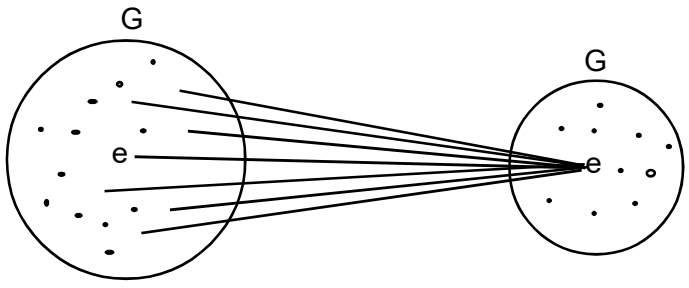
1 is the image of all even integers, and –1 is the image of all odd integers.

Thus, f is an epimorphism, but not an isomorphism.

Example 8: Let G be a group, and e be the identity of G. We define

(i) We have proved that f is a homomorphism (Example 5).

(ii) Clearly f is not one-one. All the elements are related to e.



(iii) f is not onto. e is the only image.

f is not an isomorphism. It is neither a monomorphism nor an epimorphism.

f is a homomorphism from G to itself, it is an endomorphism.



CHECK YOUR PROGRESS

Q 6: Let C be the additive group of complex numbers.Define

Examine if f is an automorphism.

Q 7: Let be the additive group of real numbers, and $_+$ be the multiplicative group of positive real numbers.

Define

Examine if f is an isomorphism

Q 8: Let be the additive group of integers, and be the additive group of even integers. Define

Examine if f is an isomorphism.

Q 9: Let

and are additive groups.

Define , f(2x)=3x where x is an integer.

Examine if f is an isomorphism.

Q 10: Let be the multiplicative group of positive real numbers, and be the additive group of real numbers. Define

Examine if f is an isomorphism.

8.5 PROPERTIES OF HOMOMORPHISM

Theorem : Let G, G/ be two groups. Let e, e/ be the identities of G, G/ respectively. Let f : G / be a homomorphism. Then

(i) $f(e) = e'$

(ii) $f(x^{-1}) = (f(x))^{-1}$,

(iii) $f(x^n) = (f(x))^n$, .

Proof: (i) We have

$e\ e = e$

$f(e\ e) = f(e)$

$f(e)\ f(e) = f(e)$, f is a homomerphism

$f(e)\ f(e) = f(e)e'$, $f(e)$ $'$, and e' is the identity of G'

$f(e) = e'$, by left cancellation.

(ii) We have

This

i.e.

(iii) Let n be a positive integer :

Then

=

=

Let n = 0 :

Then $x^0 = e$

$f(x^0) = f(e)$

$= e'$

$= (f(x))^0$

Let n be a negative integer :

Let n = –m, where m is a positive integer.

Now $f(x^n) = f(x^{-m})$

$= f(x^{-1})^m)$

$= ((f(x))^{-1})^m$

$= (f(x))^{-m}$

$= (f(x))^n$

Thus, $f(x^n) = (f(x))^n$, for any integer n.

Theorem : Let $f : G$ $'$ be an epimorphism from a group G to a group G'. If G is Abelian, then G' is also Abelian

Proof : Here f : G / is an epimorphism.

 f is a homomorphism and f is onto.

Let

 f is onto, there exist a, b

Now

= f(ab), f is a homomorphism

= f(ba), G is Abelion

= f(b) f(a), f is a homomorphism

=

Thus,

 G is Abelian

Note : The converse of the above theorem is not true.

Let us consider the group S_3 of all permutntions of S = {1, 2, 3}.

Let G = {–1, 1} be the multiplicative group.

We define

f is a homomorphism. Moreover f is onto, i.e, f is an epimorphism.

Now G is Abelian, but S_3 is not Abelian.

Theorem : Let f : G / be an epimorphism from a group G to a group G/. If G is cyclic, then G/ is also cyclic.

Proof : Here f : G / is an epimorphism.

 f is a homomorphism and f is onto. Let the cyclic group G be generated by

Let

Then there exists

u = f(p)

= $f(a^m)$, p = a^m, for some integer m

= $(f(a))^m$

This / is a cyclic group generated by f(a).

Note : The converse of the above theorem is not true.

Let us consider the example given in the previous theorem.

Here G = {–1, 1} is cyclie,

but S_3 is not cyclic.

Theorem : Let f : G / be a homomorphism from a group G to a group G/

.

(i) If H is a subgroup G, f(H) is a subgroup of G/.

(ii) If K is a subgroup of G/, $f^{-1}(K)$ is a subgroup of G.

[f(H) = {f(h) : h

$f^{-1}(K)$ = {a G : f(a)

It should be borne in mind that f^{-1} may not be a homomorphism, though f is a homomorphism]

Proof : Let e be the identity of G, and e/ be the identity of G/.

f(e) = e/

(i) We have e/ = f(e)

Let

there exist a, b

Now $^{-1}$

= f(a) f(b^{-1})

= f(ab^{-1})

H is a subgroup of G, $^{-1}$H

f(ab^{-1})

Thus,

f(H) is a subgroup of G/

(ii) We have

Let a, b $^{-1}$(K)

f(a) K, f(b)

f(a) (f(b))$^{-1}$ K, K is a subgroup of G/

f(a) f(b^{-1})

$f(ab^{-1})$

$ab^{-1} f^{-1}(K)$

Thus, $a, b \in f^{-1}(K) \Rightarrow ab^{-1} \in f^{-1}(K)$

$f^{-1}(K)$ is a subgroup of G'.

Example 9 : Let G be a group. Let the mapping $f : G \to G$ be defined by $f(x) = x^{-1}$ be a homomorphism. Show that G is Abelian.

Solution : Let $a, b \in G$.

Now $f(ab) = f(a) f(b)$, $\because$ f is a homomorphism by definition of f

$\Rightarrow (ab)^{-1} = a^{-1} b^{-1}$

$\Rightarrow ((ab)^{-1})^{-1} = (a^{-1}b^{-1})^{-1}$

$\Rightarrow ab = (b^{-1})^{-1}(a^{-1})^{-1}$

$\Rightarrow ab = ba$

$\Rightarrow$ G is Abelian



CHECK YOUR PROGRESS

Q 11: Let $f : G \to G$, $f(x) = x$ be a mapping from group G to itself. Show that f is an automorphism.

Q 12: Let G be an Abelian group. Show that the mapping.

$f : G \to G$, $f(x) = x^{-1}$ is an automorphism.



8.6 LET US SUM UP

Let G be a group under the binary operation $*$ G' be a group under the binary operation o. The mapping $f : G \to G'$ is said to be a homomorphism if $f(a$

- A homomorphism if said to be a monomorphism if it is one-one.
- A homomorphism is said to be an epimorphism if it is onto.
- A homomorphism is said to be an isomorphism if it is one-one and onto.
- A homomorphism from a group to itself is called an endomorphism.
- An isomorphism from a group to itself is called an automorphism.

- Let f : G / be a homomorphism from a group G to a grant G/. Let e, e/ be the identities of G, G/ respectively. Then
  (i) f(e) = e/
  (ii) $f(x^{-1}) = (f(x))^{-1}$,
  (iii) $f(x^n) = (f(x))^n$, n is an integer.
- Let f G / be an epimorphism from a group G to a group G/.
  (i) If G is Abelian, then G/ is Abelian.
  (ii) If G is cyclic, then G/ is cyclic.
  The converse of each of (i) and (ii) is not true.
- Let f : G / be a homomorphism from a group G to a group G/.
  (i) If H is a subgroup of G, f(H) is a subgroup of G/.
  (ii) If K is a subgroup of G/, $f^{-1}(K)$ is a subgroup of G.

8.8 FURTHER READING

1) Fraleigh, Johu B : *A First Course in Abetract Algebra* (2003), Pearson Education (Singapure) Pvt. Ltd, Indian Branch, Delhi 110092.
2) Mapa, S.K. : *Higher Algebra* (Abstract and Linear) (1994), Asoke Prakasan, Calcutta 700007.
3) Khanna, V. K. and Bhambri, S. K. : *A Course in Abstract Algebra* (2006), Vikas Publishing House Pvt. Ltd. New Delhi 110014.

8.7 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1:

Let

Now f(a+b) = 5(a+b)

=5a+ 5b

= f(a) + f(b)

f is a homomorphism.

Ans to Q No 2:

Let

f(a+b) = (a+b) + 3 = a+b+3

f(a) +f(b) = (a+3) + (b+3)

= a + b + 6

f(a+b)

f is not a homomorphism

Ans to Q No 3:

Let

Now

= f(a)f(b)

f is a homomerphism.

Ans to Q No 4:

Let

Now f(ab) = $\log_e$ ab

= $\log_e$a + $\log_e$b

= f(a) + f(b)

f is a homomorphism

Ans to Q No 5: f : S_3 G = {–1, 1}, where

Case I : Let

We know that the product of two even permutations is an even permutation.

Case 2: Let

We know that the product of two odd permutations is an even permutation.

Case 3 : Let be an even permutation, and

We know that the product of an even permutation and an odd permutation is an odd permutation.

Similarly, if is an odd permutation and

also

Thus, in all the cases,

f is a homomorphism.

Ans to Q No 6:

Let

Now

f is a homomorphism.

Let f(z) = f(w)

f is one-one.

Let

Then, there exists

f is onto.

f is an isomorphism.

f is an isomorphism from

f is an automorphism.

Ans to Q No 7:

Let

Now $f(a+b) = e^{a+b}$

$= e^a e^b$

$= f(a) f(b)$

Let $f(a) = f(b)$

$e^a = e^b$

$a = b$

f is one-one

Let

$e^c = u$

$e = \log_e u$

Thus, corresponding to every $_e u$ in

$f(\log_e u) = u$

f is onto.

f is an isomorphism.

Ans to Q No 8:

Let

Now $f(a+b) = 2(a+b)$

$= 2a + 2b$

$= f(a) + f(b)$

f is a homomorphism.

Let $f(a) = f(b)$

$2a = 2b$

a = b

f is one-one

Let

Then there exists such that

f is onto.

f is an isomorphism.

Ans to Q No 9: , where x is an integer.

Let a, b be integers.

2a, 2b

Now f (2a+2b) = f(2(a+b))

= 3(a+b)

= 3a + 3b

= f(2a)+ f(2b)

f is a homomorphism.

Let f(2a) = f(2b)

3a = 3b

a = b

2a = 2b

f is one-one

Let .

Then, there exists

f is onto

f is an isomorphism

Ans to Q No 10:

Let

Now f(ab) = $\log_{10}$ ab

= $\log_{10}a + \log_{10}b$

= f(a) + f(b)

f is a homomorphism

Let f(a) = f(b)

$\log_{10}a = \log_{10}b$

a = b

f is one-one

Let

Then there exists

f is onto.

f is an isomorphism.

Ans to Q No 11:

Let

Now f(ab) = ab

= f(a) f(b)

f is a homomorphism

f(a) = f(b)

a = b

f is one-one

For every

f is onto

f is an isomorphism from G to itself

f is an authomorphism.

Ans to Q No 12:

Let

Now $f(ab) = (ab)^{-1}$

$= b^{-1} a^{-1}$

$= a^{-1}b^{-1}$, G is Abelion

= f(a) f(b)

f is a homomorphism

Let f(a) = f(b)

a = b

f is one-one

Let

Then there exists

f is onto

f is an isomorphism from G to itself.

f is an automorphism.

8.9 MODEL QUESTIONS

Q 1: Let

be a mapping.

Examine if f is a homomorphism.

Q 2: Let

={. . ., –20, –15, –10, –5, 0, 5, 10, 15, 20, ...}

, and

Let .

Examine if f is a homomorphism.

Q 3: Give an example of a homomorphism from an infinite group to a finite group.

Q 4: Let /. If G/ is Abelian, prove that G is also Abelian.

Q 5: Let /. If G/ is cyclic, prove that G is also cyclic.

*** ***** ***

UNIT 9: RING

UNIT STRUCTURE

9.1 Learning objectives

9.2 Introduction

9.3 Ring

9.4 Properties of Ring

9.5 Let us Sum up

9.6 Answers to ‘‘Check Your Progress’’

9.7 Further Reading

9.8 Model Questions

9.1 LEARNING OBJECTIVES

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

- ring
- properties of ring.

9.2 INTRODUCTION

We have discussed group and its various properties, sub group, coset, cyclic group, normal sub groups and quotient group. In this unit we will study ring. Ring is an algebraic structure, i,e., a non-empty set equipped with two binary operations and satisfying certain postulates.

9.3 RING

A non-empty set R, equipped with two binary operations, called addition (+) and multiplication (·) is called a ring if the following postulates are satisfied.

(1) R is an additive Abelian group,

(2) R is an multiplicative semigroup

(3) The two distributive laws hold good, viz

a. (b + c) =a.b + a.c. (left distributive law)

(a + b). c = a.c + b.c, (right distributive law) for all a, b, c

Note : 1. In order to be a ring, there must be a non-empty set equipped with two binary operations, viz, + and , satisfying the postulates mentioned above. Later on we will simply write ‘‘Let R be a ring’’. It should be borne in mind that there are two binary operations, viz, + and

2. It should also be borne in mind that the binary operations + and not be known usual addition and multiplication.

3. Since R is an additive Abelian group, the additive identity, denoted by 0, belongs to R. It is called the zero element of R. Here 0 is a symbol. It should not be confused with the real number zero.

4. If a , b R, then - b R (R is an additive group). a+ (– b) is, generally, denoted by a – b.

5. a.b is, generally, written as ab.

Commutative Ring: A ring R is said to be commutative if ab = ba, for all a, b

Ring with unity : A ring R is said to be a ring with unity (or identity) if there exists an element e

ae = a = ea, for all a

Note 1. A ring may or may not have a unity.

2. If R is a ring with unity, unity may be same as the zero element. For example, {0} is a commutative ring with unity . Here 0 is the additive as well as the multiplicative identity. It is known as the zero ring.

Theorem 1 : If R is a ring with unity, then unity is unique.

Proof Let R be a ring with unity. If possible, let e and f be two identities of R.

ef = e = fe [

ef = f = fe [

∴ e = f

Note: In view of the above theorem, we write ‘‘the unity”.

Example 1. Let R = {

I (i) Let R,

a, b, c, d

Now

Matrix addition is a binary operation on R.

(ii) We know that matrix addition is associative.

(iii) We have 0 =

and

(iv) For every R, we have

∴ is the additive inverse of

(v) We know that matrix additive is commutative.

∴ R is an Abelian group under matrix addition.

II. (i) We have

∴ matrix multiplication is a binary operation on R

(ii) We know that matrix multiplication is associative.

∴ R is a semigroup under matrix multiplication.

III. We know that matrix multiplication is distributive over matrix addition.

The two distributive laws are satisfied.

∴ R is a ring under matrix addition and matrix multiplication.

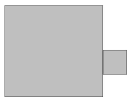
We have R,





∴ R is a non- commutative ring.

Again, there does not exist any element X 

, for all 

∴ R is a ring without unity.

Example 2 Let R be the set of all 2 x 2 matrices over integers.

I. Clearly R is an Abelian group under matrix addition.

II. R is a semigroup under matrix multiplication.

III. The two distributive laws are satisfied.

∴ R is a ring under matrix addition and matrix multiplication.

We know that matrix multiplication is not, in general, commutative.

∴ R is a non-commutative ring.

We have I = 

AI = A = IA, for all A

∴ R is a ring with unity.

Example 3: Let 2Z be the set of all even integers

I. 2Z is an Abelian group under usual addition.

II. 2Z is a multiplicative semigroup.

III. The two distributive laws are satisfied.

∴2Z is a ring under usual addition and multiplication.

Moreover, 2Z is a commutative ring.

2Z is a ring without unity, for 1 

Example 4: Let Z be the set of integers.

I. Z is an Abelian group under usual addition.

II. Z is a multiplicative semigroup.

III. The two distributive laws are satisfied.

∴ Z is a ring under usual addition and scalar multiplication.

Moreover, Z is a commutative ring . It is also a ring with unity, 1 

Other examples of commutative rings with unity are

- the ring Q of rational numbers
- the ring IR of real numbers.
- the ring C of complex numbers.

Example 5: Let C [a, b] denote the set of all real-valued continuous functions defined on [a, b] ; a, b

Let f, g

We define $(f + g)(x) = f(x) + g(x)$

$(fg)(x) = f(x)\, g(x)$, x

I. (i) We have $(f + g)(x) = f(x) + g(x)$

Also, the sum of two continuous functions is continuous.

f + g is continuous and so f + g

(ii) Let f, g, h C [a, b], x

(f + g) + h = f + (g + h)

(iii) We have 0 : [a, b] R, 0 (x) = 0, x

Clearly 0

0 + f = f = f + 0

(iv) For every f

– f : [a, b]

Clearly –f

f + (–f) = 0

Similarly (–f) + f = 0

(v) $(f + g)(x) = f(x) + g(x)$

$= g(x) + f(x)$

$= (g + f)(x)$, x

f + g = g + f

C [a, b] is an Abelian group under addition of functions.

II. (i) (fg) (x) = f (x) g (x)

Also, the product of two continous functions is continuous.

fg is continuous and so fg

Multiplication of functions is a binary operation on C [a, b]

(ii) ((fg) h) (x) = (fg) (x) h (x)

= (f (x) g (x)) h (x)

= f (x) (g (x) h (x))

= f (x) (gh) (x)

= (f (gh)) (x),

(fg)h = f (gh)

C [a, b] is a semigroup under multiplication of functions.

III. ((f+g) h) (x) = (f + g) (x) h (x)

= (f (x) + g (x)) h (x)

= f (x) h (x) + g (x) h(x)

= (f h) (x) + (gh) (x)

= (fh + gh)(x)

(f + g) h = fh + gh

Similarly f (g + h) = fg + fh

C [a , b] is a ring under addition and multiplication of functions.



CHECK YOUR PROGRESS - 1

Q 1: Give an example of a commutative ring with unity having only one element.

Q 2: Give an example of a non-commutative ring without unity.

Q 3: Give an example of a commutative ring without unity.

Q 4: Give an example of a non-commutative ring with unity.

Q 5: Give an example of an infinite commutative ring with unity.

Q 6: Let $IR^2 = \{(a, b) : a, b \text{ are reals}\}$

We define

(a, b) + (c, d) = (a + c, b + d),

(a, b) (c, d) = (ac, bd);

a, b, c, d are reals.

Show that IR^2 is a commutative ring with unity.

9.4 PROPERTIES OF RING

Let R be a ring. Then

(i) a0 = 0a = 0; for all a

(ii) a (–b) = (–a)b = –(ab); for all a, b

(iii) (–a) (–b) = ab; for all a , b

(iv) a (b – c) = ab – ac; for all a, b, c

Proof (i) we have

a0 = a (0 + 0)

= a0 + a0, by left distributive law

a0 + 0 = a0 + a0

0 = a0, by left cancellation law in the additive group R

i. e a0 = 0

Similarly 0a = 0

(ii) We have a0 = 0

This a ((–b) + b) = 0, [(–b) + b = 0]

a (–b) + ab = 0, by left distributive law

a (–b) is the additive inverse of ab

i.e., a(–b) = –(ab)

Similarly (–a)b = – (ab)

(iii) We have (–a) (–b) = l (– b), taking l = –a

= – (lb), using (ii)

= – ((– a) b)

= – (– (ab)), using (ii)

= ab

(iv) a (b – c) = a (b + (–c))

= ab + a (– c), by left distributive law

= ab – ac, by (ii)

Boolean Ring: Let R be a ring and a

a is called an idempotent element of R if $a^2 = a$.

A ring R is called a Boolean ring, if every element of it is idempotent.

Note: George Boole (1815-1864) of the nineteenth century was ‘‘an essentially self-taught Britisher’’. He is famous for his epoch - making book The Laws of Thought.

Theroem 3: Let R be a Boolean ring. Then

(i) $a + a = 0$, for all a

i. e. every element of R is its own additive inverse

(ii) $a + b = 0$ $a = b$, for all a, b

(iii) R is a commutative ring.

Proof : (i) Let a $\therefore a^2 = a$

Also $a + a$

$\therefore (a + a)^2 = a + a$ [

$(a + a)(a + a) = a + a$

$(a + a)a + (a + a)a = a + a$, By left distributive law

$(a^2 + a^2) + (a^2 + a^2) = a + a$, by right distributive law

$(a + a) + (a + a) = (a + a) + 0$

$a + a = 0$, by left cancellation law in the additive group R

(ii) We have $a + a = 0$

$\therefore a + b = a + a$, by (i)

$b = a$, by left cancellation law in the additive group R

i.e. $a = b$

(iii) Let a, b $\therefore a^2 = a, b^2 = b$

Also $a + b$

$\therefore (a + b)^2 = a + b$

$(a + b)(a + b) = a + b$

$(a + b)a + (a + b)b = a + b$, by left distributive law

$(a^2 + ba) + (ab + b^2) = a + b$

$(a + ba) + (ab + b) = a + b$

$(a + b) + ba + ab = (a + b) + 0$, by associative and commutative law of addition.

$ba + ab = 0$, by left cancellation law in the additive group R.

$ab = ba$, by (ii)

$\therefore$ R is a commutative ring.



CHECK YOUR PROGRESS - 2

Q 1: Let [redacted].Show that R is a commutative ring with unity under usual operations of addition and multiplication.

Q 2: If in a ring R, $a^2 = a$ for all a [redacted] R, show that 2a = 0 and a + b = 0 [redacted] a = b

Q 3: In z,define [redacted] and [redacted] as [redacted], [redacted]. Show that Z is a commutative ring under the operations [redacted] and [redacted].Is it a ring with unity ?



9.5 LET US SUM UP

- A non-empty set R, equipped with two binary operations, called addition (+) and multiplication (·), is called a ring if the following postulates are satisfied.

(i) R is an additive Abelian group

(ii) R is a multiplicative semigroup

(iii) The two distributive laws hold good, viz.,

a . (b + c) = a.b + a.c, (left distributive law)

(a + b).c = a.c + b.c, (right distributive law)

for all a, b, c [redacted]

- A ring R is said to be commutative if ab = ba, for all a, b [redacted]
- A ring R is said to be a ring with unity (or identity) if there exists an element e [redacted]

ae = a = ea, for all a [redacted]

9.6 ANSWERS TO "CHECK YOUR PROGRESS"

CHECK YOUR PROGRESS-1

Ans to Q No1: {0} is a commutative ring with unity. It should be noted that, in this ring, 0 is the additive as well as the multiplicative identity.

Ans to Q No 2: The ring R = { : a, b are integers} is a non-commutative ring without unity.

Ans to Q No 3: The ring 2Z of even integers is a commutative ring without unity.

Ans to Q No 4: The ring R of all 2 x 2 matrices over integers is a non-commutative ring with unity.

Ans to Q No 5: The ring Z of integers is an infinite commutative ring with unity.

Ans to Q No 6: IR^2 = {(a, b) : a, b are reals}

I. (i) Let (a, b), (c, d) $\in$ IR^2, where a, b, c, d are reals

Now (a, b) + (c, d) = (a + c, b + d) $\in$ IR^2

(ii) Let (a, b), (c, d), (e, f) $\in$ IR^2

((a, b) + (c, d)) + (e, f) = (a + c, b + d) + (e, f)

= ((a + c) + e, (b + d) + f)

= (a + (c + e), b + (d + f))

= (a, b) + (c + e, d + f)

= (a, b) + ((c, d) + (e, f))

$\therefore$ addition is associative.

(iii) We have (0, 0) $\in$ IR^2,

and (0, 0) + (a, b) = (a, b) = (a, b) + (0, 0)

$\therefore$ (0, 0) is the additive identity.

(iv) For every (a, b) $\in$ IR^2, we have (–a, –b) $\in$ IR^2 such that (a, b) + (–a, –b) = (0, 0) = (–a, –b) + (a, b)

$\therefore$ (–a, – b) is the additive inverse of (a, b).

(v) (a, b) + (c, d) = (a + c, b + d)

= (c + a, d + b)

= (c, d) + (a, b)

$\therefore$ addition is commutative.

$\therefore$ IR^2 is an additive Abelian group.

II. (i) (a, b) (c, d) = (ac, bd) $\square$ ^{2}

(ii) ((a, b) (c, d)) (e, f) = (ac, bd) (e, f)

= ((ac) e, (bd) f)

= (a (ce), b (df))

= (a, b) (ce, df)

= (a, b) ((c, d) (e, f))

$\therefore$ multiplication is associative.

$\therefore$ IR^2 is a multiplicative semigroup.

III. (a, b) ((c, d) + (e, f)) = (a, b) (c + e ,d + f)

= (a (c + e), b (d + f))

= (ac + ae, bd + bf)

= (ac, bd) + (ae, bf)

= (a, b) (c, d) + (a, b) (e, f)

Similarly ((a, b) + (c, d)) (e, f) = (a, b) (e, f) + (c, d) (e, f)

$\therefore$ IR^2 is a ring

Furthermore, (a, b) (c, d) = (ac, bd)

= (ca, db)

= (c, d) (a, b)

$\therefore$ IR^2 is a commutative ring.

Again, (1, 1) $\square$ ^{2}, and

(a, b) (1, 1) = (a1, b1) = (a, b) = (1, 1) (a, b)

$\therefore$ (1, 1) is the unity.

$\therefore$ IR^2 is a ring with unity.

Thus, IR^2 is a commutative ring with unity

CHECK YOUR PROGRESS - 2

Ans to Q No 1: It can be easily verified that R is a commutative ring with

as additive identity and

unity R.

Ans to Q No 2: Properties of Rings ((i), (ii))

Ans to Q No 3: It can be easily verified that Z is a commutative ring under the given operations.Also

with unity 0.

9.7 FURTHER READING

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.

9.8 MODEL QUESTIONS

Q 1: Let Z be the set of integers, We define (+) and (·) on Z as follows

a (+) b = a + b – 1,

a (·) b = a + b – ab, for all a, b

Examine Z is a commutative ring with unity under (+), (·).

Q 2: Prove that a ring R is commutative if and only if

$(a + b)^2 = a^2 + 2ab + b^2$, for all a, b

[Here a^2 means aa]

*** ***** ***

UNIT 10: INTEGAL DOMAIN & FIELD

UNIT STRUCTURE

10.1 Learning objectives

10.2 Introduction

10.3 Integral Domain

10.4 Field

10.5 Let us Sum up

10.6 Answers to ‘‘Check Your Progress’’

10.7 Further Reading

10.8 Model Questions

10.1 LEARNING OBJECTIVES

After going through this unit you will be able to know

- Integral domain and its properties
- Field and their properties.

10.2 INTRODUCTION

In Unit 9, we have discussed ring and its various properties. In this unit we will study Integral domain and Field. Integral domain and Field are also a Ring satisfying certain postulates.

10.3 INTEGRAL DOMAIN

Let us consider the ring R of all 2 x 2 matrices over integers.

Let A = and B =

Here A is not a null matrix, B is not a null matrix, i.e. A 0, B

But AB =

=

i.e, AB is a null matrix.

Thus, we see that A 0, B

Again, let us consider the ring Z of integers. If a, b

a 0, b 0, then ab

Definition: An element a (_____ if there exists an element b (

We see that the ring R of all 2 x 2 matrices over integers has zero divisors whereas the ring Z of integers has no zero divisors, for if a b Z, a 0, b 0, then ab 0, ba

Concellation Laws: Let R be a ring. The additive cancellation laws hold good in R, since R is an additive Abelian group.

So, by cancellation laws in a ring, we mean multiplication laws (cancellation of non zero elements).

The cancellation laws hold good in R if ab = ac b = c, ba = ca b = c; where a, b, c R, a

Theorem 1: The cancellation laws hold good in a ring R if and only if R has no zero divisors.

Proof: Let the cancellation laws hold good in a ring R.

Let a, b

If a 0, ab = 0 ab = a0 .

Similarly, if b 0, ab = 0 ab = 0b

So there can be no zero divisor.

Conversely, let there be no zero divisors in R.

Let a, b, c R and ab = ac, a

ab – ac = 0

a (b – c) = 0

a

b – c = 0

Thus, if a 0, ab = ac

similarly, if a 0, ba = ca

Thus, the cancellation laws hold good in R.

Definition A commutative ring with unity e 0 and containing no zero divisors is called an Integral Domain.

The simplest example of an integral domain is the ring Z of integers. It is a commutative ring, has unity and is without zero divisors.

Note: An integral domain may be considered as a generalisation of Z.

Example 1: Let us consider the set R = {a + bi : a, b are integers, of Gaussian integers, after the name of C. F. Gauss (1777-1855).

I. (i) Let a + bi, c + di

a, b, c, d are integers, i =

(a + bi) + (c + di) = (a + c) + (b + d)i

(ii) Addition of complex numbers is associative.

(iii) We have 0 = 0 + 0i

and 0 + (a + bi) = a + bi = (a + bi) + 0

(iv) For every a + bi R, we have (–a) + (–b)i

(a + bi) + ((–a) + (–b)i) = 0 =((–a) + (–b)i) + (a + bi)

(v) Addition of complex numbers is commutative.

R is an Abelian group under addition of complex numbers.

II. (i) (a + bi) (c + di) = (ac – bd) + (ad + bc)i

(ii) Multiplication of complex numbers is associative

R is a semigroup under multiplication of complex numbers.

III. Clearly the two distributive laws hold good.

Furthermore, multiplication of complex numbers is commutative.

R is a commutative ring.

Also R possesses 1 (1=1 + oi)

R is a ring with unity.

Again we know that the product of two non-zero complex numbers cannot be zero.

R is without zero divisors.

Thus, R is an integral domain.

10.4 FIELD

Definition: Let R be a ring with unity e

has multiplicative inverse in R, then R is called a Division Ring (or a Skew

Field).

A commutative division ring is called a field.

The simplest example of a field is the ring IR of real numbers.

It is commutative, has unity and every non-zero element has multiplicative inverse in IR.

Therefore, IR is a field.

Similarly, the ring C of complex numbers is also a field.

Note: The ring z of integers is not a field. (why?)

Example 2: Examine if the ring

R = {a + bi : a, b, are integers, i =

of Gaussian integers is a field.

Solution: We know that R is a commutative ring with unity.

(Ref. Example 6)

Let a + bi R such that a + bi

Now the multiplicative inverse of a + bi is which is

not an element of R.

R is not a field.

Theorem 2: Every field is an integral domain.

Proof: Let F be a field.

Let a, bF such that a

a $^{-1}$

Now ab = 0

a^{-1} (ab) = a^{-1} 0

(a^{-1} a) b = 0

b = 0

Similarly, if b

F has no zero divisors.

Thus, F is a commutative ring with unity and containing no zero divisors.

F is an integral domain.

Note: The converse of the above theorem is not true, i.e, every integral domain is not a field.

Let us consider the ring Z of integers. We know that Z is an integral domain. But only two elements, viz, –1 and 1 have multiplicative inverses in Z.

However we have the following

Theorem 3: A non-zero finite integral domain is a field.

Proof: Let R = {a_1, a_2, a_3, ...

where all the

Let

Let us consider the non zero elements a_2, a_3, ...,

Let be not the unity of R (p 1),i.e.,

Let us consider the products

2, 3, ...,

All these elements belong to R. Also all the elements are distinct, for if

=, , ,

then –

(–

– = 0, [

=

Now one of $a_p a_2$, $a_p a_3$, ..., $a_p a_n$ must be unity, Let $a_p a_q$ = e, where e is the unity of R

Then $a_p a_q = e = a_q a_p$.

a_p has multiplicative inverse in R. If a_p is the unity of R, then a_p has multiplicative inverse in R.

Thus, every non-zero element of R has multiplicative inverse in R.

R is a field.

Theorem 4: A division ring has no zero divisors.

Proof: Let R be a division ring.

Let a, b R such that a

a $^{-1}$ R (

Now ab = 0

a^{-1} (ab) = a^{-1} 0

$\square$ $(a^{-1}a)b = 0$

$\square$ $b = 0$

Similarly, if $b\square$

$\therefore$ R is without zero divisors



CHECK YOUR PROGRESS

Q 1: Does the ring Q of rational numbers contain zero divisors?

Q 2: Let R be the ring of all 2 x 2 matrices over integers, Does the cancellation laws hold good in R?

Q 3: Is the ring 2Z of even integers an integral domain?

Q 4: Give an example of an integral domain which is not a field.

Q 5: Does the ring $IR^2 = \{(a, b) : a, b \square IR\}$ contain zero divisiors?



10.5 LET US SUM UP

- An element a($\square$
  element b ($\square$
- A commutative ring with unity e$\square$
  called an integral domain
- Let R be a ring with unity e$\square$
  If every non-zero element of R has multiplicative inverse in R, then R is called a division ring (or a skew field).
  A commutative division ring is called a field.
- Every field is an integral domain, but every integral domain is not a field.
- A non-zero finite integral domain is a field.

10.6 ANSWERS TO "CHECK YOUR PROGRESS"

CHECK YOUR PROGRESS

Ans to Q No 1: No. If a, b Q and a 0, b 0, then ab

Ans to Q No 2: No. Cancellation laws hold good in a ring if and only if it has no zero divisors. The ring of all 2 x 2 matrices over integers contains zero divisors. So cancellation laws do not hold good in the ring of all 2 x 2 matrices over integers.

For example





i. e. 

i. e. AB = AC, but B

where 

Ans to Q No 3: The ring 2Z of even integers is not an integral domain, since it does not contain the multiplicative identity.

Ans to Q No 4: The ring Z of integers is an integral domain, but not a field. Only –1 and 1 have multiplicative inverses in Z,

Ans to Q No 5: Yes.

(7, 0) ^{2}, (0, 13) ^{2} ,(7, 0) (0, 0), (0, 13)

But (7, 0) (0, 13) = (0, 0).

10.7 FURTHER READING

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

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

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

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

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

10.8 MODEL QUESTIONS

Q 1: Let R = {(a, b) : a, b are reals}. We define

(a, b) + (c, d) = (a + c, b + d)

(a, b) (c, d) = (ac – bd, bc + ad)

Prove that R is a field.

Q 2: Let R = {a + b

under usual addition and multiplication.

Q 3: Let R be a commutative ring with unity and is without zero divisors. Show that the only idempotent elements are the zero element and the unity element.

*** ***** ***

UNIT 11: VECTOR SPACE

UNIT STRUCTURE

11.1 Learning objectives

11.2 Introduction

11.3 Defintion and examples of vector space

11.4 Elementary properties

11.5 Subspace of a vector space

11.6 Linear dependence and Independence

11.7 Basis and Dimension

11.8 Let us Sum Up

11.9 Answers to Check Your Progress

11.10 Further Reading

11.11 Model Questions

11.1 LEARNING OBJECTIVES

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

- definition and examples of vector space
- elementary properties of vector space
- subspace of a vector space
- linear dependence and independence of vectors
- basis and dimension of a vector space

11.2 INTRODUCTION

We know the notion of a vector. The concept of a vector space comes from the notion of a vector.In vectors, we have addition of vectors, multiplication of a vector by a scalar, and the scalar product of vectors.In vector space also, we find the addition of vectors,multiplication of a vector by a scalar and the scalar product of vectors.Thus a vector space may be regarded as a generalisation of a vector that is found in mechanics or Analytical geometry.

11.3 DEFINITION AND EXAMPLES OF VECTOR SPACE

Definition : Let V be an Abelian group under " + ". Let F be a field under "+,

For each element , ,we have multiplication.

Then V is said to be a vector space over the field F if the following conditions are satisfied.

1.
2.
3.
4.

where , .

We write "

Note

1. The element of V are called vectors, and the elements of F are called scalars.
2. denotes the "addition " (+) of two vectors , whereas denotes "addition " (+) of two scalars borne in mind that these two additions are different, though they are denoted by the same symbol.
3. denotes the "multiplication" of a vector by a scalar ;whereas . It should be borne in mind that these two multiplication are also different ,though they are denoted by the same symbol.
4. is an Abelian group under " + ". So,we have the operation " + "in .F is a field under "+, by a scalar.Thus ,we have altogether four operations in a vector space.
5. is an Abelian group under " + ".So,we have the additive identity 0 under +,called the zero element.Again F is a field.So,we have the zero element they are dented by the same symbol.Again F contains the unit element 1.It should be borne in mind that 1 is not necessarily the real number 1.

6. If ,i.e., if is the field of real numbers,then is called a real vector space.

   If ,i.e., if is the field of complex numbers,then called a complex vector space.

7. We define the "subtraction"in as follows ,where is the additive inverse of ;

Example 1 : Let

numbers.We define addition and scalar multiplication in

where , ,

Then is a vector space over R,i.e.

Solution : I.First we prove that

(1)

(i)

(ii) Let ,

Now

(iii) We have

and

Similarly,

i.e.,

[Note that in ,

(iv) For every , there exists

Similarly,

i.e.

(v)

is an abelian group under

II. we have ,

III. (i)

(ii)

,

(iii)

(iv) We have

is a vector space over R,i.e.,

Example 2 : Let

of real numbers.

and

where and

It can be shown as in the previous example.

Example 3 : Let V be the set of all real-valued continuous functions defined on

multiplication as follows

where , and

I. First we prove that V is an Abelian group under addition.

(i) Let

and are real valued continuous functions defined on

is also a real valued continous function defined on

(ii) Let and

Now,

,

,

(iii) Let , ,

Clearly

Now

Similarly,

This shows that .

(iv) For every , we define

,

Clearly,

,

Similarly,

(v)

,

V is an abelian group under addition.

II.Let , ,

Since f is continuous ,

III. (i)

,

,

(ii)

,

(iii)

,

(iv)

V is a vector space over R,i.e.,V is a real vector space.



CHECK YOUR PROGRESS 1

Q 1: Show that the field of real numbers R is a vector space over R.

Q 2: Show that the field of complex numbers C is a vector space over C.

Q 3: Show that the field of complex numbers C is a vector space over R. Is R is a vector space over C?

Q 4: Let V be the set of all matrices over reals. Show that V is a vector space over R.

Q 5: Let , and . Define addition and scalar multiplication in V as follows

where , ,

Show that V is not a vector space.

11.4 ELEMENTARY PROPERTIES

Let V be a vector space over a field F.Let ,

(i) (This"0" is the zero element of the Abelian group V)

(ii) (The "0" on the left is the zero element of the field F,and the"0" on the right is the zero element of V.)

(iii) if ,then or

(iv)

(v)

(vi)

Proof : (i) We have

We note that this

Now

i.e.

(ii) We have

We note that this

Now

i.e.

(iii) Here

If

Let ,

Now

(iv) We have

Now,

Again

Thus,

(v) We have

Also,we have

Now

(vi) Proceed as above.

Example 4 : Let V be a vector space over the field F.Show that

,

Solution : we have



CHECK YOUR PROGRESS 2

Q 1: Let V be a vector space over the field F.Let and . Show that (i) if , Then ,

(ii) if , then ,

(iii) if , and , then

(iv) if , and , then

(v) if , then or .

11.5 SUBSPACE OF A VECTOR SPACE

Let V be a vector space over a field F.Let W be a nonempty subset of V.W is called a subspace of V if W itself is a vector space over F under the same addition and scalar multiplication in V.

Note: 1. V itself is a subspace of V.

2. The set

is a vector space,called the null space. .

Theorem : A non-empty subset W of a vector space V(F) is a subspace of V if and only if W is closed under addition and scalar multiplication.

Proof : Let W be a subspace of V(F).Then,by definition,W is closed under addition and scalar multiplication.

Conversely, let W be closed under addition and scalar multiplication.

Let

Now

Now

i.e.

Thus,

.

All the other conditions for a vector space are satisfied in W, as they are satisfied in V.

.

Theorem : A non-empty subset W of a vector space V(F) is a subspace of V if and only if ,for all

Proof : Let W be a subspace of V.

Let ,

,

Conversely, let W be a non-empty subset of V such that for all ;, ,

Now

i.e.,

W is closed under addition.

Again ,

i.e.,

W is closed under scalar multiplication.

Example 5 : Let us consider the vector space

Let

Clearly ,and

Let ;

W is a subspace of

Example 6 : Let us consider the vector space

Let

Clearly,

Let ;

Now,

Now,

.

Theorem : Intersection of two subspaces of a vector space is a subspace.

Proof : Let V be a vector space over a field F.

Let and .

, since at least the zero element 0 of W is in

Let

and

and

Now ; and .

Again ; and .

Thus, and

is a subspace of V.

Note : Union of two subspaces may not be a subspace.

We know

componentwise scalar multiplication.

Let

Clearly, is a subspace of , is a subspace of

Now ,

But

i.e., ,

but

is not a subspace of

Theorem: Union of two subspaces is a subspace if and only if one of them is contained in the other.

Proof : Let V be a vector spae over a field F.

Let .

Let .Then

,

.

Conversely, let be a subspace of V such that subspace of V.

We are to prove that or

If possible,let it not be the true.

and

there exists such that .Also, there exists .

Now

is a subspace of V.

This or

Let

Now ,

which is a contradiction.

Similarly,let

Now ,

which is a contradiction.

So,our assumption is wrong.

either or



CHECK YOUR PROGRESS 3

Q 1: Let be the vector space under componentwise addition and componentwise scalar multiplication.

(i) Let . Show that W is a subspace of .

(ii) Let . Show that W is a subspace of .

(iii) Let . Show that W is not a subspace of .

Q 2: Let be the vector space under componentwise addition and componentwise scalar multiplication.

Let .Show that W is not a subspace of .

11.6 LINEAR DEPENDENCE AND INDEPENDENCE

Let V be a vector space over a field F. Vectors are said to be linearly dependent over F if there exist scalars

(not all of them zero) such that .

Thus,the vectors

at least one of

If

;

the vectors

A finite set is said to be linearly dependent or linearly independent according as its

independent.

A subset W of V is called linearly independent if the elements of W are linearly independent .Otherwise it is said to be linearly dependent.

Note

1. Let ,and

   Let

   Now

   ,[if

   is linearly independent i.e.a non-zero vector is always linearly independent.

2. We have ,but .

zero vetor is always lineraly dependent.

3. A superset of a linearly dependent set of vectors is linearly dependent.
4. A subset of a linearly independent set of vectors is linearly independent.

Example 7 : Let us consider the vector space over componentwise addition and componentwise scalar multiplication.

Let us consider the vectors in

Let

Now,

the vectors

Example 8 : Let us consider the vector space over componentwise addition and componentwise scalar multiplication.

Let us consider the vectors in

Let

Now

... (1)

i.e.

... (3)

Now

the only solution of the equations (1),(2),(3) is

the vectors

Example 9: Let us consider the vector space

vectors in

Let

Now

... (1)

Now

the system of equations possesses non zero solution.

From (1) and (2)

From (3),

Thus,

the vectors

Example 10 : Let us consider the vector space R over Q.

We have

Let such that

If possible, let

Now

, which is a contradiction.

This

Proposition : If two vectors of a vector space are linearly dependent,one of them is a scalar multiple of the other.

Proof : Let V be a vector space over a field F.

Let such that

Then there exist scalars

Let ,

Now

,taking

Thus, is a scalar multiple of

Similarly,if ,y is a scalar multiple of

CHECK YOUR PROGRESS 4

Q 1: Show that the vectors

dependent in .

Q 2: Show that the vectors are linearly dependent in

Q 3: Show that the vectors independent in .

Q 4: Show that the vectors independent in .

11.7 BASIS AND DIMENSION

Definition : Let V be a vector space over a field F.Let

Any vector ;where

linear combination of the vectors

Definition : Let V be a vector space over a field F.A subset S of V is called a basis of V if

(i) any finite number of elements in S are linearly independent,

(ii) each vector in V is a linear combination of a finite number of elements of S.

Example 11 : Let us consider the vector space

subset of ,where

Let

S is linearly independent.

Let

Now

Thus, each vector in

S is a basis of

Example 12 : is the standard basis of

, ,

Example 13 : is the standard basis

, ,

Example 14 : Let us consider the vector space

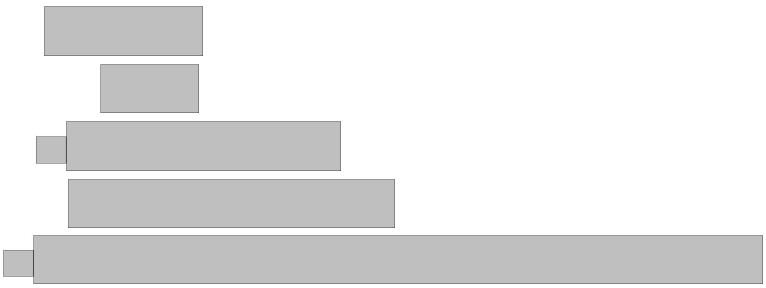
Let be a subset of

, , .

Let

Let

, where



Thus, each vector in .

T is a basis of

Note : From Example 12 and Example 14,we see that a vector may have more than one basis.

Example 15 : Show that the set .

Solution : We have already proved that the set linearly dependent. (Example 9)

the given set is not a basis of

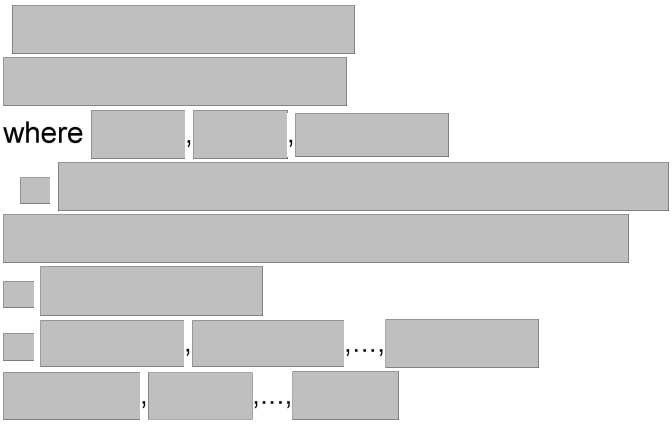
Theorem : Let V be a vector space over the field F. If basis of V, then each element of V can be uniquely expressed as a linear combination of

Proof : By definition of basis, we know that each element of V can be expressed as a linear combination of

We show that the expression is unique.

Let

If possible, let



where , ,

Thus, the expression is unique.

Definition : Let V be a vector space over a field F.

If the number of elements in a basis of V is finite, then V is said to be a finite dimensional vector space.It is said to be a of finite dimension.Other vector spaces are said to be infinite dimensional.We note that any two bases of finite dimensional vector space have the same number of elements.

The number of elements in a basis of a vector space V is said to be the dimension of V.Generally it is denoted by dimV.THe null space is said to be of 0 dimension.

Example 16 : We know that the standard basis

space

dim

Example 17: Dimension of

Example 16: Dimension of is

Example 19 : Show that forms a basis of

of

Solution : Let

is linearly independent.

Now

Thus, each vector in C is a linear combination of the elements of

Number of elements of

dimension of

Example 20 : If are elements in a vector space

;Show that the set

Solution : We have

Hence



11.8 LET US SUM UP

- Let V be an Abelian group under " + ". Let F be a field under "+, each element , , we have multiplication.

  Then V is said to be a vector space over the field F if the following conditions are satisfied.

  1.
  2.
  3.
  4.

  where , .
- The set

  vector space,called the null space.
- Let V be a vector space over a field F.Let W be a nonempty subset of V.W is called a subspace of V if W itself is a vector space over F under the same addition and scalar multiplication in V.

  V itself is a subspace of V.

  .
- Intersection of two subspaces of a vector space is a subspace, whereas union of two subspaces may not be a subspace.
- The vectors

  linearly dependent over F if

  at least one of

  If

  ;

  The vectors
- A non-zero vector is always linearly independent.
- Zero vector is always linearly dependent.
- Let V be a vector space over a field F.Let

Any vector ;where

called a linear combination of the vectors

- Let V be a vector space over a field F.A subset S of V is called a basis of V if

  (i) any finite number of elements in S are linearly independent,

  (ii) each vector in V is a linear combination of a finite number of elements of S.

- The number of elements in a basis of a vector space V is said to be the dimension of V.Generally it is denoted by dimV.The null space is said to be of 0 dimension.



11.9 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS – 1

Ans to Q No 1: I. We know that R is an abelian additive group.

II. If , then

III. (i).

(ii).

(iii).

(iv).

where ,

R is a vector space over R.

Ans to Q No 2: Left as an exercise.As above.

Ans to Q No 3: First part : Left as an exercise.

Second Part : R is not a vector space over C

,

But , i.e. R is not closed with repect to scalar multiplication.

Ans to Q No 4: I. We know that V be an Abelian group under matrix addition.

II.If ,then .

III.(i).

(ii).

(iii).

(iv).

where ;

Ans to Q No 5 : Let ,

Now

CHECK YOUR PROGRESS – 2

Ans to Q No 1: (i)

(ii)

(iii)

(iv)

(v)

or

or

CHECK YOUR PROGRESS – 3

Ans to Q No 1: (i) Let , and ,

Now

. is a subspace of

(ii) Left as an exercise.

(iii) Left as an exercise.

Ans to Q No 2: Let

Now

Now

, if

, if

W is not a subspace of

CHECK YOUR PROGRESS – 4

1. Left as an exercise.
2. Left as an exercise.
3. Left as an exercise.
4. Left as an exercise.

11.10 FURTHER READING

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society.
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd. Hyderabad 500029.

11.11 MODEL QUESTION

Q 1: Prove that a field F is a vector space over any subfield K of F.

Q 2: Let componentwise scalar multiplication.

Let

Define

Show that W is a subspace of

Q 3: Let

componentwise scalar multiplication.

Let

Examine if W is a subspace of

Q 4: Let R(R) be the vector space of real numbers.Let

that the set is linearly dependent if the set

is linearly dependent.

[is linearly dependent,there exist scalar

all zero such that

This

If , then clearly

If , then at least one of

; , .

at least one of ,

the set

Q 5: Consider the vector space

componentwise scalar multiplication.

Examine if the set is a basis of

Q 6: Consider the vector space

componentwise scalar multiplication.

Show that is a basis of

, , , .

*** ***** ***

UNIT 12 : COMBINATORICS

UNIT STRUCTURE

12.1 Learning Objectives

12.2 Introduction

12.3 The Rule of Sum

12.4 The Rule of product

12.5 Permutation

12.6 Combination

12.7 Let Us Sum Up

12.8 Answers To Check Your Progress

12.9 Further Reading

12.10 Model Questions

12.1 LEARNING OBJECTIVES

After going through this unit, you will able to know

- the rule of sum
- the rule of product
- permutation
- combination

12.2 INTRODUCTION

Combinatorics is an important branch of discrete mathematics. It deals with counting the number of ways of arranging or selecting objects from a finite collection under specified rules, i.e. it deals with problems of permutation and combinations. Combinatorics is widely applied in computer science.

12.3 THE RULE OF SUM

If there are n_1 ways to do a work A and distinct from them, n_2 ways to do work B,then the number of ways to do A or B is n_1+n_2. Here the two works cannot be done at the same time.

Note : The rule can be extended to any finite number of works. Thus, if r works can be done in n_1, n_2, ...,n_r ways and if they cannot be done simultaneously, then any one of the r works can be performed in $n_1+n_2+n_3$ . . . . .+ n_r ways.

Example 1 : There are 26 boys and 28 girls in a class. Find the number of ways of selecting one student as class representative.

Solution : One boy can be selected in 26 ways (we can select any one of these 26 boys). One girl can be selected in 28 ways.

$\square$ One student (a boy or a girl, not both of them) can be selected in 26+28 i.e. 54 ways.

Example 2 : There are 30 mathematics books and 25 science books in a library. In how many ways a mathematics book or a science book can be selected ?

Solution : We are to select one book, a mathematics book or a science book.

One mathematics book can be selected in 30 ways. One science book can be selected in 25 ways.

$\square$ a mathematics book or a science book can be selected in 30+25 i.e. 55 ways.

Example 3 : In how many ways a heart or a club can be selected from a pack of cards ?

Solution : A pack of cards contains 52 cards out of which there are 13 hearts, 13 diamonds, 13 clubs, 13 spades.

$\square$ One heart can be selected in 13 ways, one club can be selected in 13 ways.

$\square$ a heart or a club can be selected in 13+13 i.e, 26 ways.

12.4 THE RULE OF PRODUCT (OR SEQUENTIAL RULE)

If a work can be done in two successive steps, and the first step can be done in n_1 ways, the second step can be done in n_2 ways, then the work can be done in $n_1 \square n_2$ ways.

Note : The rule can be extended to any finite number of works. Thus, if a work can be done in r successive steps, and the first step can be done in n_1

ways, the second step can be done in n_2 ways, and in this way, the r th step can be done in n_r ways, then the work can be done in $n_1 \square n_2 \square \ldots\ldots\ldots \square_r$ ways.

Example 4 : There are 25 boys and 20 girls in a class. A teacher wants to select one boy and one girl. In how many ways can this be done ?

Solution : One boy can be selected in 25 ways. One girl can be selected in 20 ways. Thus, the first step (i.e. to select one boy) can be done in 25 ways, the second step (i.e. to select one girl) can be done in 20 ways.

$\square$ One boy and one girl can be selected in $25\square$

Example 5 : What is the number of two-digit odd positive integers ?

Solution : Ones place can be filled up in 5 ways (any one of the five digits 1, 3, 5, 7, 9). Tens place can be filled up in 9 ways (any one of the nine digits 1, 2, 3, 4, 5, 6, 7, 8, 9). Thus, the first step can be done in 5 ways, the second step can be done in 9 ways.

$\square$ the work can be done in $5\square$

$\square$ the number of two odd-digit positive integers = 45



CHECK YOUR PROGRESS 1

Q 1: One man or a woman is to be selected from 24 men and 12 women. In how many ways can this be done ?

Q 2: There are 24 boys and 12 girls in a class. A teacher wants to select one boy and one girl. In how many ways can this be done ?

Q 3: Find the number of two-digit even positive integers.

Q 4: Find the number of three-digit odd positive integers.

Q 5: Find the number of three-digit even positive integers.

Q 6: Find the number of four-digit odd positive integers.

Q 7: Find the number of four-digit even positive integers.

Q 8: There are 40 mathematics books and 28 science books in a library. In how many ways one mathematics book or one science book can be selected ?

Q 9: There are 40 mathematics books and 28 science books in a library. In how many ways one mathematics book and one science book can be selected ?

Q 10: A big hall has 12 doors. In how many ways can a person enter the hall by one door and come out by a different door ?

Q 11: There are 15 buses plying between Guwahati and Dibrugarh. In how many ways can a man go from Guwahati to Dibrugarh and return by a different bus ?

Q 12: In how many ways can 7 students stand in a queue ?

Q 13: A man has six letters and there are three latter boxes. In how many ways can he post the letters ?

Q 14: In how many ways can three prizes be distributed among six students, if each of the students is eligible for each of the prizes ?

Q 15: Find the number of license plates that can be made where each plate contains two distinct English letters followed by four distinct digits.

Q 16: In how many ways a condidate can answer all the questions of a true-false test consisting of 10 question ?

Q 17: How many functions are there from a set with 5 elements to a set with 7 elements ?

Q 18: How many functions are there from a set with 7 elements to a set with 5 elements ?

Q 19: How many one-one functions are there from a set with 5 elements to a set with 7 elements ?

Q 20: How many one-one functions are there from a set with m elements to a set with n elements ?

Q 21: Find the number of seven-character palindromes that can be formed using the letters of the English alphabet such that no letter appears more than twice in each of them.

12.5 PERMUTATION

Let there be a set containing n distinct elements. An ordered arrangement of r elements of the set is called a permutation (or an r-permutation of n elements), r

Symbolically it is denoted by ${}^nP_r$, or P(n, r), or $P(n_r)$.

Theorem : (Number of r-permutations without repetition) The number of r-permutations of n distinct objects is

P(n, r) = n(n-1) n(-2) . . . . . (n-r+1)



Proof : The first object can be closen in n different ways. So, we are left with (n-1) objects. Therefore, the second object can be chosen in (n-1) ways. Similarly, the third object can be chosen in (n-2) ways. In this way, the last object, i.e. the rth object can be chosen in (n-r+1) ways .Consequently, by the product rule, there are n(n-1)(n-2) . . . . (n-r+1) way of ordered arrangment Thus,

P(n, r) = n(n-1)(n-2) . . . . . (n-r+1)





Note : 

Example 6: Find the value of n if P(n, 4) = 360

Solution : P (n, 4) = 360

or, 

or, 

or, n(n-1)(n-2)(n-3) = 6 x 5 x 4 x 3

n = 6

Note : Left hand side is the product of 4 consecutive positive integers.

Therefore, the right hand side has also been expressed as the product of 4 consecutive positive integers.

Example 7 : How many four-digit numbers can be formed from the six digits 1, 2, 3, 5, 7, 8, if repetitions of digits are not allowed ?

Solution : The number of 4 digit numbers.

= the number of 4-permutations of 6 objects (digits)

= P (6, 4)

=

Example 8: In how many ways can 10 different examination answer scripts be arranged so that the best and the worst always come together ?

Solution : The best and the worst come together. So, we can consider the best script and the worst script as a single script. Thus, we can consider 10 objects to be '9' objects. So, these '9' objects can be arranged in ${}^{9}P_{9}$ i.e. 9! ways.

Again, the best script and the worst script can be arranged among themselves in 2! ways.

the required number of ways

= 9!

= 725760.



CHECK YOUR PROGRESS 2

Q 1: Three persons enter a railway carriage, where there are 6 vacant seats. In how many ways can they seat themselves ?

Q 2: A gentleman has 6 friends to invite. In how many ways can he send invitation cards to them, if he has three bearers to carry the cards ?

Q 3: There are 20 candidates in an examination for awarding 5 prizes. In how many ways can the prizes be distributed, each candidate being eligible for one prize ?

Q 4: How many numbers lying between 100 and 1000 can be formed with the digits 1, 2, 3, 4, 5 if the digits in the same number are

not repeated ? Fund also the number of numbers lying between 100 and 10,000.

Q 5: How many four-digits even numbers cab be formed from the digits 1, 2, 3, 5, 7, 8 if repetition of digits are not allowed ?

Q 6: How many four-digit odd numbers can be formed from the digits 1, 2, 3, 5, 7, 8 if repetition of digits are not allowed ?

Q 7: How many four-digit numbers divigible by 5 can be formed from the digits 1, 2, 3, 5, 7, 8 if repetition of digits are not allowed ?

Q 8: In how many ways can 10 different examination answer scripts be arranged so that the best and the worst never come together ?

Q 9: Mr X has 4 mathematics books, 3 statistics book and 5 economics books. In how many ways can he arrange them on a shelf of books if books of each subject are placed together, and in the following order : mathematics, statistics, economics ?

Q 10: Find the number of ways in which letters of the word TRIANGLE can be arranged among themselves, if each arrangement begins with T and ends with E.

12.6 COMBINATION

Let there be a set containing n distinct elements. An unordered selection of r elements of the set is called a combination (or an r-combination of n elements),

Symblically it is denoted by ${}^{n}C_{r}$, or C(n, r), or $C(n_{r})$

Theorem : (Number of r-combinations without repetition) The number of r-combinations of n distinct objects is

Proof : By r-combination we mean an unerdered selection of r-objects from n distinct objects. Each r-combination contains r objects. These r objects can be ananged among themseleves in ${}^{r}P_{r}$, i.e., r! ways.

Therefore, each r-combination yields r! permutations.

C(n, r) combinations will yoeld C(n, r) r! permutations.

We know that the number of r-permutations of n distinct objects is given by P(n, r)

C (n, r) r ! = P (n, r)

or, C(n, r) =

Note :

Theorem : C(n, r) = C(n, n-r),

Proof : If r objects are chosen from n objects, then (n-r) objects are left.

Thus, selection of r objects from n objects is the same as leaving (n-r) objects.

Thus, to each r-combination there corresponds an (n-r) combination.

C(n, r) = C(n, n-r)

Theorem : (Pascal's Identity)

C(n+1, r) = C(n, r) + C(n, r-1),

Proof : Let us counsider a finite set A having (n+1) elements.

Let B be a subset of A, and let the number of elements of A be n.

Let such that

Clearly

Every r-element subset of A is either an r-element subset of B or the union of an (r-1) element subset of B and the singleton set {p}.

In the first case, the number of subsets is C(n, r); whereas in the second case, the number of subsets is C(n, r-1).

the total number of r-element subsets of A is C(n, r) + C(n, r-1).

But we know that the total number of r-element subsets of A is C(n+1, r).

C(n+1, r) = C(n, r) + C(n, r-1).

Note : Blaise pascal was a famous french mathematician of the seventeenth century.

Example 9 : In how many ways can a committee of 6 gentlemen and 3 ladies be formed out of 9 gentlemen and 6 ladies?

Solution : 6 gentlemen can be selected from 9 gentlement in ${}^9C_6$ ways. 3 ladies can be selected from 6 ladies can be selected in ${}^6C_3$ ways.

$\therefore$ by the product rule, the number of committees = ${}^9C_6 \cdot {}^6C_3$

$= 3 \cdot 4 \cdot 7 \cdot 5 \cdot$

$= 1680$

Example 10 : A question paper contains 3 different sections A, B and C containing 4, 5 and 6 questions respectively. In how many ways a caudidate can make a selection of 7 questions, selecting at least 2 questions from each sections ?

Solution : There are three possibilities.

I 2 questions from A, 2 from B, 3 from C

II 2 from A, 3 from B, 2 from C

III 3 from A, 2 from B, 2 from C

The number of ways in I

$= {}^4C_2 \cdot {}^5C_2 \cdot {}^6C_3 = 6 \cdot 10 \cdot$

The number of ways in II

${}^4C_2 \cdot {}^5C_3 \cdot {}^6C_2 = 6 \cdot 10 \cdot$

The number of ways in III

${}^4C_3 \cdot {}^5C_2 \cdot {}^6C_2 = 4 \cdot 10 \cdot$

$\therefore$ the required number of ways

$= 1200 + 900 + 800$

$= 2900$



CHECK YOUR PROGRESS 3

Q 1: There are 6 men and 7 women working in an office. In how many ways can a committee of 3 men and 4 women be selected ?

Q 2: There are 6 men and 7 women working in an office. In how many ways can a committee of 4 persons which has at least one woman be selected ?

Q 3: There are 6 men and 7 women working in an office. In how many ways can a committee of 4 persons which has at most one man be selected ?

Q 4: From 8 gentlemen and 4 ladies, a team of 5 is to be formed. In how many ways can this be done so as to include at least one lady?

Q 5: A man has 7 friends, 4 of them are ladies and 3 men. His wife has also 7 friends, 3 of them are ladies and 4 men. In how many ways can they invite a dinner party of 3 ladies and 3 men so that there are 3 of man's friends and 3 of wife's friends ?



12.7 LET US SUM UP

- If there are n_1 ways to do a work A and distinct from them, n_2 ways to do another work B, then the number of ways to do A or B is n_1+n_2. Here the two works cannot be done at the same time. This is known as the rule of sum.
- If a work can be done in two successive steps, and the first step can be done in n_1 ways, the second step can be done in n_2 ways, then the work can be done in n_1 n_2 ways, This is known as the rule of product.
- Let there be a set containing n distinct elements. An ordered arrangement of r elements of the set is called an r-permutation of n elements,

  called an r-combination of n elements,
- The number of r-permutations of n distinct objects is

  $P(n, r) = n(n-1)(n-2) \ldots (n-r+1)$

- The number of r-combinations of n distinct objects is



- C(n, r) = C(n, n-r),
- C(n+1, r) = C(n, r) + C(n, r-1)



12.8 ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress 1

Ans to Q No 1: One man can be selected in 24 ways,

One woman can be selected in 12 ways.

One woman or one woman can be selected in 24+12 i. e. 36 ways.

Ans to Q No 2: One boy can be selected in 24 ways.

One girl can be selected in 12 ways.

One boy and one girl can be selected in 24

Ans to Q No 3: Ones place can be filled up in 5 ways (any one of the digits 0, 2, 4, 6, 8).

Tens place can be filled up in 9 ways (any one of the digits 1, 2, 3, 4, 5, 6, 7, 8, 9).

the required number of numbers

= 5

Ans to Q No 4: Ones place can be filled up in 5 ways (any one of the digits 1, 3, 5, 7, 9).

Tens place can be filled up in 10 ways (any one of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9)

Hundreds place can be filled up in 9 ways (any one of the digits 1, 2, 3, 4, 5, 6, 7, 8, 9).

the required number of numbers = 5 10

Ans to Q No 5: Ones place can be filled up in 5 ways (any one of the digits 0, 2, 4, 6, 8).

Tens place can be filled up in 10 ways. (any one of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9).

Hundreds place can be filled up in 9 ways (any one of the digits 1, 2, 3, 4, 5, 6, 7, 8, 9).

□ the required number of numbers

= 5□10□

Ans to Q No 6: Do yourself. Ans 4500

Ans to Q No 7: Do yourself. Ans 4500

Ans to Q No 8: One mathematies book or one science book can be selected in 40+28 i.e 69 ways.

Ans to Q No 9: One mathematies book and one science book can be selected in 40□

Ans to Q No 10: A person can enter the hall in 12 ways, i.e, the first step can be performed in 12 ways. the person can come out from the hall in 11 ways, i.e., the second step can be performed in 11 ways.

□ the required number of ways.

= 12□

Ans to Q No 11: Do yourself. Ans 210

Ans to Q No 12: Do yourself. Ans 5040

Ans to Q No 13: Do yourself. Ans $3^6 = 729$

Ans to Q No 14: Do yourself. Ans $6^3 = 216$

Ans to Q No 15: First letter can be filled up in 26 ways.

Second letter can be filled up in 25 ways.

First digit can be filled up in 10 ways.

Second digit can be filled up in 9 ways.

Third digit can be filled up in 8 ways.

Fourth digit can be filled up in 7 ways.

□ the required number of ways

= 26□25□10□9□8□7

Ans to Q No 16: First question can be answered in 2 ways (either true of false).

Similarly, each of the questions can be answered in 2 ways.

= 2 2 2 2 2 2 2 2 2 2

= 2^{10} = 1024

Ans to Q No 17: Number of elements in the domain = 5

Number of elements in the codomain = 7

First element can be associated in 7 ways.

Similarly each of the elements of the domain can be associated in 7 ways.

the required number of functions

= 7 7 7 7 ^{5}

Ans to Q No 18: Number of elements in the domain = 7

Number of elements in the codomain = 5

Each of the elements of the domain can be associated in 5 ways.

the required number of functions

= 5 5 5 5 5 5 ^{7}

Ans to Q No 19: Number of elements in the domain = 5

Number of elements in the codomain = 7

First element can be associated in 7 ways

Second element can be associated in 6 ways

Third element can be associated in 5 ways

Fourth element can be associated in 4 ways

Fifth element can be associated in 3 ways

the required number of one-one functions

= 7 6 5 4

Ans to Q No 20: We note that ; if m > n, there cannot be one-one function from the first set to the second set.

Now, 1st element can be associated in n ways

2nd element can be associated in (n-1) ways

3rd element can be associated in (n-2) ways.

In this way, mth element can be associated in (n-m+1) ways.

the required number of one-one functions.

= n(n-1)(n-2) . . . . (n-m+1)

Ans to Q No 21: [Dictionary meaning of the word palindrome is given below.

'A word, phrase, number or any other sequence of units which has the property of reading the same forwards as it does backwards, character for character, sometimes disregarding punctuation, capitalization and diacritics.']

The required number of palindromes

= 26 25 24

= 358800

Check Your Progress 2

Ans to Q No 1: Number of ways

= 120

Ans to Q No 2: Number of ways = 3 3 3 3 3

Ans to Q No 3: Number of ways

= 1860480

Ans to Q No 4: Do yourself. Ans 60,180

Ans to Q No 5: Ones place can be filled up in 2 ways (one of the digits 2, 8).

The other three places can be filled up in $^5P_3$ ways.

the required number of numbers

= 120

Ans to Q No 6: Ones place can be filled up in 4 ways (one of the digits 1, 3, 5, 7). The other three places can be filled up in $^5P_3$ ways.

the required number of numbers

= $4 \cdot {}^5P_3 = 4 \cdot 5 \cdot 4$

Ans to Q No 7: Ones place can be filled up in 1 way (5). The other three places can be filled up in $^5P_3$ ways.

the required number of numbers

= $1 \cdot {}^5P_3 = 1 \cdot 5 \cdot 4$

Ans to Q No 8: If there is no restriction, 10 answer scripts can be arranged among themselves in $^{10}P_{10}$ i.e. 10! ways.

Again, we know that if the best and the worst scripts come together, the number of arrangements = 9!

= 725760 (Example 8)

if the best and the worst do not come together, the number of arrangements

= 10 ! – 2

= 3628809 – 725760

= 2903040

Ans to Q No 9: Number of ways

= 4! 3!

= 4 3 2 1 3 2 1 5 4 3 2 1

= 17280

Ans to Q No 10: Each arrangement begins with T, and ends with E. So, we are left with six letters R. I. A, N, G, L.

These six letters can be arranged among themselves in $^{6}P_{6}$ ways, i.e. 6! ways, i.e., 6 5 4 3 2

the number of ways = 720

Check Your Progress 3

Ans to Q No 1: 3 men can be selected from 6 men in $^{6}C_{3}$ ways.

4 women can be selected from 7 women in $^{7}C_{4}$.

the required number of ways



= 20

Ans to Q No 2: At least one woman is to be selected. Therefore number of women may be 1, or 2 or 3 or 4. So we have the following possibilities

Men (6)	Women (7)
3	1
2	2
1	3
0	4

the required number of ways

$= {}^6C_3 \cdot {}^7C_1 + {}^6C_2 \cdot {}^7C_2 + {}^6C_1 \cdot {}^7C_3 + {}^6C_0 \cdot {}^7C_4$

$= 20 \cdot 7 + 15 \cdot 21 + 6 \cdot 35 + 1 \cdot$

$= 140 + 315 + 210 + 35$

$= 700$

Ans to Q No 3: At most one man is to be selected. Therefore number of men may be 0, or 1. So, we have the following possibilities

Men (6)	Women (7)
0	4
1	3

the required number of ways

$= {}^6C_0 \cdot {}^7C_4 + {}^6C_1 \cdot {}^7C_3 = 1 \cdot 35 + 6 \cdot$

Ans to Q No 4: Do yourself. Ans 736

Ans to Q No 5: We have the following possibilities.

Man		**Wife**	
Men (3)	Ladies (4)	Men (4)	Ladies (3)
3	0	0	3
2	1	1	2
1	2	2	1
0	3	3	0

the required number of ways

$= ({}^3C_3 \cdot {}^4C_0 \cdot {}^4C_0 \cdot {}^3C_3) + ({}^3C_2 \cdot {}^4C_1 \cdot {}^4C_1 \cdot {}^3C_2) + ({}^3C_1 \cdot {}^4C_2 \cdot {}^4C_2 \cdot {}^3C_1)$

$+ ({}^3C_0 \cdot {}^4C_3 \cdot {}^4C_3 \cdot {}^3C_0)$

$= 485$, after simplification.

12.9 FURTHER READING

1) *Discrete Mathematical Structures with Application to Computer Science.* J.P Tremblay & R. Manohar.

2) *Discrete Structures and Graph Theory,* G. S. S. Bhishma Rao.

12.10 MODEL QUESTIONS

Q 1: Write down the sum rule for counting.

Q 2: Write down the product rule for countting

Q 3: Prove using combinational argument that

$C(2n, 2) = 2\,C(n, 2) + n^2$

Q 4: Prove, using combinational argument, that

for integers , and

Q 5: Two distinguishable dice are rolled. In how many ways can we get a sum of 7 or 9 ?

Q 6: In how many way can we draw a king or a queen from a pack of cards ?

Q 7: A license plate contains two English letters, followed by two digits, followed by two English letters, followed by four digits. How many license plates can be made if repetition of letters and digits are allowed?

Q 8: There are 10 married couple in a group. Find the number of ways of selecting a woman and a man who is not her husband from this group.

Q 9: From 8 boys and 6 girls a team of 8 players is to be forwed. In how many ways can the team be formed so that exactly 3 girls are included excluding a paiticular girl and including a particular boy ?

Q 10: Find the number of one-one functions from a set with n elements to itself.

*** ***** ***

Unit 13: MATHEMATICAL LOGIC

UNIT STRUCTURE

13.1 Learning Objectives

13.2 Introduction

13.3 Definition of Statements

13.3.1 Examples of Statements

13.4 Logical Connectives

13.4.1 Negation

13.4.2 Conjunction

13.4.3 Disjunction

13.4.5 Conditional

13.4.6 Biconditional

13.5 Let Us Sum Up

13.6 Answers to Check Your Progress

13.7 Further Reading

13.8 Model Questions

13.1 LEARNING OBJECTIVES

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

- define statements and examples of statements
- define truth tables about different statements
- know about negation of statements
- know about conjuction, disjunction, conditional and bi-conditional of two statements

13.2 INTRODUCTION

Mathematical logic is the discipline that deal with the methods of reasoning. As all of us know that the main asset that makes humans far more superior than other species is the ability of reasoning. Logic provides rules and techniques for determining whether a given argument or mathematical proof or conclusion in a scientific theory is valid or not. Logic is concerned with studying arguments and conclusions. Logic is used in

mathematics to prove theories and to draw conclusions from experiments in physical science in our every day life to solve many types of problem. Logic is used in computer science to verify the correctness of programs. The rules of logic or techniques of logic are called rules of inference because the main aim of logic is to draw conclusions inferences from given set of hypothesis. In this unit, we will introduce you to the definition and examples of statements, truth table of different statements. We will allso discuss about the logical connectives. Moreover, we will discuss about the converse, opposite and contrapositive of statements.



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

13.3 DEFINITION OF STATEMENTS

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

Assertive sentence : A sentence that makes an assertion is called an assertive sentence or declerative sentence.

For example, " Mars supports life ".is an assertive or a declerative sentence

Imperative sentence : A sentence that expresses a request or a command is called an imperative sentence .

For example, "please bring me a cup of tea." is an imperative sentence.

Exclamatory sentence : A sentence that express some strong feeling is called an exclamatory sentence.

For example, "How big is the whale fish !." is an exclamatory sentence .

Interrogative sentence : A sentence that asks some questions is called an interrogative sentence.

For example, "What is your age ? "is an interrogative sentence .

STATEMENT : *A sentence or proposition is an assertive (or decleartive) sentence which is either true or false but not both. A sentence cannot both true and false at the same time .*

13.3.1 Examples of Statements

IIIUSTRATION 1 : Consider the following sentences :

i) Washington D .C is not in America.

ii) Every rectangle is a square.

iii) The earth is a planet.

iv) Three plus six is 9.

v) The sun is a star.

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

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

IIIUSTRATION 2 : Consider the following sentences :

i) Do your home work.

ii) Give me a glass of water.

iii) How are you ?

iv) Have you ever seen Taj Mahal ?

v) May god bless you !

vi) May you live long !

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



CHECK YOUR PROGRESS

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

i) Paris is in England.

ii) May god bless you ?

iii) 6 has three prime factors .

iv) 18 is less than 16 .

v) How far is chennai from here?

vi) Every rhombus is a square .

vii) There are 35 days in a month.

viii) Two plus three is five.

ix) x +2 = 9

x) The moon is made of green cheese.

13.4 LOGICAL CONNECTIVES

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

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

13.4.1 Negation

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

Let us consider the statement

P : All integers are rational numbers .

The negation of this statement is :

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

or

~ P : It is false that all integer are not rational number.

or

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

or

Consider now the statement ,

P : 7> 9

The negation of this statement is

~ P : 7 < 9

or

~ P : 7= 9

TRUTH TABLE OF NEGATION

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

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

The truth table of ~P is :



Table 2.1

IIUSTRATION EXAMPLES :

Write the negation of the following statements :

(i) is a rational.

(ii) is not a complex number.

(iii) Every natural number is greater than zero.

(iv) All primes are odd.

(v) All mathematicians are man .

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

r :

The negation ~ r of this statement is given by

~ r : It is not the case that

or

~ r :

or

~ r : It is false that

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

u : .

The negation ~ u of this statement is given by

~u : .

or

~u : It is false that .

(iii) The negation of the given statement is :

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

or

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

(iv) The negation of the given statement is

There exists a prime which is not odd.

or

Some primes are not odd.

or

At least one prime is not odd.

(v) The negation of the given statement is :

Some mathematician is not man.

or

There exists a mathematician who is not man.

or

At least one mathematician is not man.

or

It is false that all mathematicians are man.



CHECK YOUR PROGRESS

Q 2: Write the negation of the following statements -

i) Bangalore is the capital of Karnataka.

ii) The Earth is round.

iii) The Sun is cold.

iv) Some even integers are prime.

v) Both the diagonals of a rectangle have the same length.

13.4.2 Conjunction

The conjunction i.e joining of two statements P and Q is the statement P *P and Q*”

IIIUSTRATION EXAMPLES :

(i) The conjunction of the statements :

P : It is raining.

Q : 2+2 = 4 is P

It is raining and 2+2=4 .

(ii) Consider the statement

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

Its components are :

Q : The Earth is round.

R : The Sun is cold.

Truth table : The statement P

both P and Q have the truth value T ; Other wise it has the truth value F.

The truth table for conjunction as follows :



Table 2.2

IIIUSTRATION EXAMPLES :

Translate the following statement into symbolic form :

Ramu and Raghu went to school.

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

Now write P : Ramu went to school.

Q : Raghu went to school

Then the given statement can be written in symbolic form as P

13.4.3 Disjunction

The disjunction of the two statements P and Q is the statement P *P or Q*".

IIUSTRATION 3 :

(i) Consider the compound statement

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

The component statements of this statement are :

Q : Two lines intersect at a point.

R : Two lines are parallel.

(ii) Consider another statement

P : 45 is a multiple of 4 or 6.

Its component statements are :

Q : 45 is a multiple of 4 .

R : 45 is a multiple of 6.

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

Truth table : The statement P

both P and Q have the truth value F, P

or Q is true (or both Pand Q are true). Truth table for disjunction :

Table 2.3



CHECK YOUR PROGRESS

Q 3: Write the following statements in symbolic form :

(i) Pavan is rich and Raghav is not happy.

(ii) Pavan is not rich and Raghav is happy.

(iii) Naveen is poor but happy.

(iv) Naveen is rich or unhappy

(v) Naveen and Amal are both smart .

(vi) It is not true that Naveen and Amal are both smart

(vii) Naveen is poor or he is both rich and unhappy

(vii) Naveen is neither rich nor happy.

IIIUSTRATIVES EXAMPLES :

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

(i) 50 is a multiple of both 2and 5.

(ii) All living things have two legs and two eyes .

(iii) Mumbai is the capital of Gujrat or Maharashtra.

(iv) A rectangle is a quadrilatateral or a 5 sided polygon.

(v)

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

P : 50 is multiple of 2

Q : 50 is multiple of 5

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

(ii) The component statements of the given statement are

P : All living things have two legs.

Q : All living things have two eyes.

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

(iii) The components statements of the given statement are

P : Mumbai is the capital of Gujrat.

Q : Mumbai is the capital of Maharashtra.

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

(iv) The components statement are

P : A rectangle is a quadrilateral.

Q : A rectangle is a 5 sided polygon.

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

(v) The compound statement are

P : .

Q : .

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



CHECK YOUR PROGRESS

Q 4: Write the component statements of the following compound statements and check the compound statement is true or false.

(i) Delhi is in India and 2+2=4.

(ii) Delhi is in England and 2+2=4.

(iii) Delhi is in India and 2+2=5 .

(iv) Delhi is in England and 2+2=5.

(v) Square of an integer is positive or negative.

(vi) The sky is blue and the grass is green .

(vii) The earth is round or the sun is cold.

(viii) All rational numbers are real and all real numbers are complex.

(ix) 25 is a multiple of 5 and 8.

(x) 125 is a multiple of 7or 8.

13.4.5 Conditional

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

Example : Let P : Amulya works hard.

Q : Amulya will pass the examination.

Then P

The statement P is called the *antecedent* and Q is called the *consequent* in P Q. The sign

We will also write P

Truth table for conditional 'P



we will also write P

that P, (iv) P is sufficient for Q, (v) Q is necessary conditions for P, (vi) P implies Q, (vii) Q is implied by P.

IIIUSTRATIVES EXAMPLES :

1. Write each of the following statements in the form " If--then"
   (i) You get job implies that your credentials are good.
   (ii) A quadrilateral is a parallogram if its diagonals bisect each other.
   (iii) To get A+ in the class, it is necessary that you do all the excercisesof the book.

Solution :

(i) we know that "If P, then Q" is equivalent to "P
Therefore,the given statement can be written as
"If you get a job , then your credentials are good."

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

(iii) The given statement can be written as

"If you get A+ in the class, then you do all the exercise of the books".

2. Write the component statements of each of the following statements. Also check whether the statements are true or not.

   (i) If a triangle ABC is equilateral , then it is isosceles.

   (ii) If a and b are integers , then ab is a rational number.

Solution :

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

P : The triangle ABC is equilateral.

Q : The triangle ABC is isosceles.

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

(ii) The component statements are :

P : a and b are integers.

Q : ab is a rational number.

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



CHECK YOUR PROGRESS

Q 5: Write down the truth value of each of the following implication.

(i) If 3+2=7, then Paris is the capital of india.

(ii) If 3+4=7,then 3 7.

(iii) If 4 5,then 5 6.

(iv) If 7 3, then 6 14.

(v) If two integers a and b are such that a>b, then a-b is always a positive integer.

13.4.6 Biconditional (If and only if implication)

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

The following table defines the biconditional :

The statement P

have identical truth values.

Truth table for biconditional (P

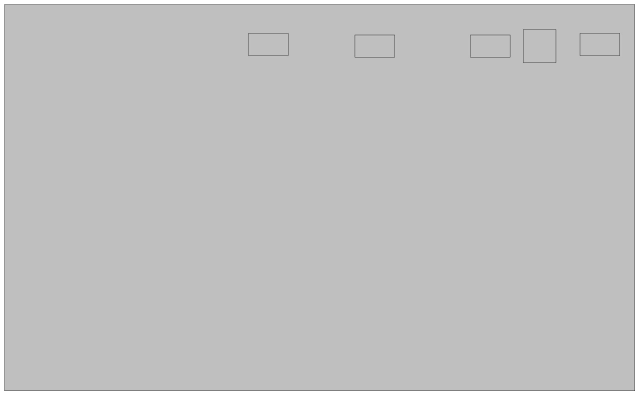


The biconditional P

P Q and Q P i.e (P Q) (Q

for P

Also, truth table for (P Q) (Q



Note that both truth tables are identical.

IIIUSTRATIVES EXAMPLES :

1. Consider the statement :

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

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

   P : A triangle is equilateral.

   Q : A triangle is equiangular.

2. 8

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

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

Biconditional P

a. P if and only if Q

b. P is equivalent to Q

c. P is necessary and sufficient condition for Q

d. Q is necessary and sufficient condition for P

IIIUSTRATION EXAMPLES :

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

(i) 4 2 if and only if 0

(ii) 3 2 if and only if 2

(iii) 3+5 7 if and only if 4+6

Solution :

(i) Let P : 4

Q : 0

Then, the given statement is P

Clearly, P is true and Q is true and therefore, P

the given statement is true, and its truth value is T.

(ii) Let P : 3 < 2

Q : 2<1

Then, the given statement is P

Clearly, P is false and Q is false and therefore, P Q is true. Hence,

the given statement is true, and its truth value is T.

(iii) Let P : 3+5 > 7

Q : 4+6<10

Then, the given statement is P

Clearly, P is true and Q is false and therefore, P

the given statement is false and therefore, its truth value is F.



CHECK YOUR PROGRESS

Q 6: Write down the truth value of each of the following

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

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

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

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

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

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



13.5 LET US SUM UP

- Mathematical logic is concerned with all kinds of reasoning, whether they be legal arguments or mathematical proofs or conclusions in a scientific theory based upon a set of hypotheses.
- Sentences are usually classified as declarative, exclamatory, interrogative and imperative. In our study of logic, we will confine ourselves to declarative sentences only i.e. we begin by assuming that the object language contains a set of declarative sentences. A primary statement is a declarative sentence which cannot be further broken down or analyzed into simpler sentences.
- New statements can be formed from primary statements through the use of sentential connectives. The resulting statements are called *compound statements.*
- The sentential connectives are called logical connectives.the different types of connectives are: *negation(~), AND(conjunction),OR (disjunction), IF---THEN (conditional), IF AND ONLY IF (Bi-conditional) etc.*
- Truth tables have already been introduced in the definitions of the connectives Our basic concern is to determine the truth value of a

statement formula for each possible combination of the truth values of the component statements. A table showing all such truth values is called the truth table of the formula. we constructed the truth table for ~P, P Q, P Q, P Q and P

of the components are known, then the truth value of the resulting statement can be readily determined from the truth table by reading along the row which corresponds to the correct truth value of the component statements.

- The statement P is called the antecedent and Q is called the consequent in P



13.6 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Statement : (i), (iii), (iv), (vi), (vii), (viii) & (x).

Ans to Q No 2: (i) Bangalore is not the capital of Karnataka.

(ii) The earth is not round.

(iii) The sun is not cold.

(iii) No even integer is prime.

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

Ans to Q No 3: (i) P

Q : Raghav is happy

(ii) ~P

(iii) ~R

H : Naveen is happy

(iv) R

(v) P

Q : Amal is smart

(vi) ~(P

(vii) ~R (R

R : Naveen is happy

(viii) ~R

Ans to Q No 4: (i) P : Delhi is in india

Q : 2+2=4

the compound statement is true

(ii) P : Delhi is in England

Q : 2+2=4

the compound statement is false.

(iii) P : Delhi is in india

Q : 2+2=5

the compound statement is false

(iv) P : Delhi is in England

Q : 2+2=5

the compound statement is false

(v) P : Square of an integer is positive

Q : Square of an integer is negative

the compound statement is true.

(vi) P : The sky is blue

Q : The grass is green

The compound statement is true.

(vii) P : The earth is round

Q : The sun is cold

The compound statement is true.

(viii) P : All rational numbers are real

Q : All real numbers are complex.

The compound statement is true.

(ix) P : 25 is a multiple of 5

Q : 25 is a multiple of 8

The compound statement is false.

(x) P : 125 is a multiple of 7

Q : 125 is a multiple of 8

The compound statement is false.

Ans to Q No 5: (i) True (ii) False (iii) True (iv) False (v)True

Ans to Q No 6: (i) True (ii) False (iii) True (iv) False (v) True (vi) True.

13.7 FURTHER READING

1) C. L. Liu, Elements of Diserete Mathemathics, Tata McGraw-Hill Edition

2) Seymour Lipschutz, Marc Lars Lipson, Discrete Mathematics, Tata McGraw-Hill Edition.

13.8 MODEL QUESTIONS

Q 1: Find out which of the following sentences are statements and which are not. Justify your answer.

(i) The real number x is less than 2.

(ii) All real numbers are complex numbers.

(iii) Listen to me, Ravi !

Q 2: Find the component statements of the following and check whether they are true or not:

(i) A line is staight and extends indefinitely in both directions.

(ii) The sky is blue and the grass is green.

(iii) The earth is round or the sun is cold.

(iv) All rational numbers are real and all real numbers are complex

(v) 25 is a multiple of 5 and 8.

Q 3: Write the component statements of each of the following statements.Also, check whether the statements are true or not.

(i) Sets A and B are equal if and only if (A B and B A).

(ii) $|a|<2$ if and only if ($a>-2$ and $a<2$)

(iii) ABC is isosceles if and only if B= C.

(iv) $7<5$ if and only if 7 is not a prime number.

(v) ABC is a triangle if and only if AB+BC>AC.

*** ***** ***

UNIT 14 : BOOLEAN ALGEBRA

UNIT STRUCTURE

14.1 Learning Objectives

14.2 Introduction

14.3 Definition, Properties and Examples

14.4 Basic Laws of Boolean Algebra

14.5 Boolean Expression

14.6 Let Us Sum Up

14.7 Answers To Check Your Progress

14.8 Further Reading

14.9 Model Questions

14.1 LEARNING OBJECTIVES

After going through this unit, you will able to know

- boolean algebra, its properties, examples
- basic laws of boolean algebra
- boolean expression.

14.2 INTRODUCTION

Boolean Algebra is an algebraic structure after the name of British logician George Boole (1813-1864). By an algebraic structure we mean a set equipped with one or more binary operations defined on it satisfying certain axioms. Though it is an abstract algebraic sturucture, it can be used for analysing electrical circuits. Nowadays it is immensely used for the analysis and design of electronic computers.

14.3 DEFINITION, PROPERTIES AND EXAMPLES

Definition : Let B a non-empty set equipped with two binary operations + and . , a unary operation $'$, and two distinct elements 0 and 1. Then B is called a Boolean Algebra if the following conditions are satisfied.

1. Commutative laws

   (i) a + b = b + a, (ii) a.b = b.a,

2. Distributive laws

   (i) a + (b.c) = (a + b).(a + c)

   (ii) a. (b + c) = (a.b) + (a.c),

3. Identity laws

   (i) a + 0 = a, (ii) a.1 = a

4. Complement laws

   (i) a + $a^{/}$ = 1, (ii) a.$a^{/}$ = 0

Note : 1. From the definition it is clear that there cannot a Boolean Algebra with one element.

2. 1 is called unit element, and 0 is called zero element.
3. $a^{/}$ is called complement of a.
4. A Boolean Algebra is generally denoted by (B, + , . , $^{/}$, 0, 1) or (B, +, . ,$^{/}$) or simply by B.
5. The symbols 0 and 1 are not necessaily real numbers 0 and 1 respectively.

Example 1 : B = {0, 1} is a Boolean Algebra under +, . , $^{/}$ defined by

+	1	0	.	1	0		/
1	1	1	1	1	0	1	0
0	1	0	0	0	0	0	1

Solution : From the definition of +, . , $^{/}$, it follows that

1. (i) a + b = b + a

   (ii) a.b = b.a,

2. (i) a + (b.c) = (a+b).(a + c)

   (ii) a.(b+c) = (a.b) + (a.c),

3. (i) a + 0 = a, (ii) a.1 = a,

4. (i) a + $a^{/}$ = 1 (1 + $1^{/}$ = 1 + 0 = 1),

   0 + $0^{/}$ = 0 + 1 = 1)

   (ii) a. $a^{/}$ = 0 (1. $1^{/}$ = 1.0 = 0,

   0.$0^{/}$ = 0.1 = 0)

(b, + , . , $^{/}$) is a Boolean Algebra.

Properties

1. In a Boolean Algebra B, zero element is unique.

Proof : Let (B, + , . , $^{/}$) be a Boolean Algebra.

If possible, let there be two zero elements 0 and 0_1

$a + 0 = a$,

$a + 0_1 = a$,

$0_1 + 0 = 0$ (

Again $0_1 + 0 = 0 + 0_1$ (by commutative law)

$= 0$ ($_1$ is zero element)

$0_1 = 0$

i.e. zero element is unique.

Note : In view of the above property, we will write as “the” zero element.

2. In a Boolean Algebra B, unit element is unique.

Proof : Let (B, +, . , $^{/}$) be a Boolean Algebra.

If possible, let there be two unit elements 1, and 1_u.

$1_u.1 = 1_u$ (

$1_u = 1$

i.e unit element is unique.

Note : In view of the above theorem, we will write as “the” unit element.

3. In a Boolean Algebra B, complement of each element is unique.

Proof : Let (B, + , . , $^{/}$) be a Boolean Algebra.

Let 0 be the zero element, and

1 be the unit element.

Let

If possible, let $a^{/}$ and a_1 be complements of a

$a + a^{/} = 1, a . a^{/} = 0$ ($^{/}$ is complement of a)

$a + a_1 = 1, a . a_1 = 0$ ($_1$ is complement of a)

Now $a^{/} = a^{/}.1$

$= a^{/}. (a + a_1)$

$= (a^{/}.a) + (a^{/}.a_1)$

$= (a.a^{/}) + (a^{/}.a_1)$

$= 0 + (a'.a_1)$

$= (a'.a_1) + 0$

$= a'.a_1$ (1)

Again $a_1 = a_1.1$

$= a_1.(a + a')$

$= (a_1.a) + (a_1.a')$

$= (a.a_1) + (a_1.a')$

$= 0 + (a_1.a^1)$

$= (a'.a_1) + 0$

$= a'.a_1$ (2)

From (1) and (2), we get

$a' = a_1$

Note : In view of the above theorem, we write as "a'" is the complement of a.

4. In a Boolean Algebra B,

(i) $1' = 0$, (ii) $0' = 1$, where 0 is the zero element, and 1 is the unit element.

Proof : (i) Let B be a Boolean Algebra,

Now, by identity laws, we have $a + 0 = 1$ and $a.1 = a$,

Replacing a by 1 in $a + 0 = a$, we get $1 + 0 = 1$.

Replacing a by 0 in $a.1 = 1$, we get $0.1 = 0$

i.e. $1.0 = 0$ ($0.1 = 1.0$, by commutative law)

Thus, $1 + 0 = 1$ (1)

$1.0 = 0$ (2)

From (1) and (2), we conclude that $0 = 1'$ i.e. $1' = 0$ (complement laws)

(ii) Let B be a Boolean Algebra.

Now, by identity laws, we have $a.1 = 1$ and $a + 0 = a$,

Replacing a by 0 in $a.1 = a$, we get $0.1 = 0$.

Replacing a by 1 in $a + 0 = a$, we get $1 + 0 = 1$.

i.e. $0 + 1 = 1$, ($1+ 0 = 0 + 1$, by commutativeled)

Thus, $0.1 = 0$ (1)

$0 + 1 = 1$ (2)

From (1) and (2), we conclude that $0' = 1$ (complement law)

Note : The property (ii), viz $0' = 1$ can be derived from property (i), viz $1' = 0$ by interchanging the binary operations + and . , and by interchanging 0 and 1. Here (ii) is called the dual of (i), and vice versa, i.e. (i) is the dual of (ii) This principle is known as the principle of duality. The principle holds good for every statement and every theorem in a Boolean Algebra.

Example 2 : Let X be a non-empty set Let P(x) be the power set of A, i.e P(x) is the set of all subsets of x.

Let , i.e.

We define

A' = the complement of A.

Clearly, union is a binary operation on P(x), intersection is a binary operation on P(x), complementation is a unary operation on P(x).

Now 1. (i)

(ii) ,

2. (i)

(ii)

3. (i)

(ii)

4. (i)

(ii)

is a Boolean Algebra, where

the unit element.

Example 3: Let B = {1, 2, 5, 10, 11, 22, 55, 110} be the set of all positive divisiors of 110. We define

a + b = l.c.m. of a, b,

a.b = g.c.d. of a, b,



We construct the composition tables for +, . , / as follow?

+	1	2	5	10	11	22	55	110
1	1	2	5	10	11	22	55	110
2	2	2	10	10	22	22	110	110
5	5	10	5	10	55	110	55	110
10	10	10	110	10	110	110	110	110
11	11	22	110	110	11	22	55	110
22	22	22	110	110	22	22	110	110
55	55	55	110	110	55	110	55	110
110	110	110	110	110	110	110	110	110

.	1	2	5	10	11	22	55	110
1	1	1	1	1	1	1	1	1
2	1	2	1	2	1	2	1	2
5	1	1	5	5	1	1	5	5
10	1	2	5	10	1	2	5	10
11	1	1	1	1	11	11	11	11
22	1	2	1	2	11	22	11	22
55	1	1	5	5	11	11	55	55
110	1	2	5	10	11	22	55	110

/	1	2	5	10	11	22	55	110
	110	55	22	11	10	5	2	1

From the above tables, we see that + is a binary operation on B. . is a binary operation on B, and / is a unary operation on B.

Again 1 (i) a+b = l.c.m. of a, b

= l. c. m. of b, a

= b+a, 

(ii) a, b = g.c.d. of a, b

= g.c.d. of b, a

= b.a, 

2. From the tables, we have

(i) a + (b.c) = (a+b).(a+c)

(ii) a.(b+c) = (a.b) + (a.c),

3. (i) a+1 = l .c.m of a, 1

= a,

(ii) a.110 = g.c.d. of a, 110

= a,

4. (i) $a+a^{/}$ = l.c.m of a, $a^{/}$

= l.c.m. of

= 110,

(ii) $a.a^{/}$ = g.c.d. of a, $a^{/}$

= g.c.d. of

= 1,

(B, + , . , /) is a Boolean Algebra; where 1 is the zero element, and 110 is the unit element.

CHECK YOUR PROGRESS



Q 1: Let X ={1}. Show that the set P(x) = {{1}, } is a Boolean Algebra under operations of union, intersection, and complementation in P(x).

Q 2: Let X = {1, 2, 3}, and Let P(X) be the power set of X. Show that P(X) is a Boolean Algebra under operations of union, intersection, and complementation in P(X).

Q 3: Let B = {1, 2, 3, 5, 6, 10, 30} be the set of all positive divisors of 30. Define

a+b = l.c.m. of a, b;

a.b = g.c.d. of a, b

Show that (B, +, . , /) is a Boolean Algebra

Q 4: Let B = {1, 2, 5, 7, 10, 14, 35, 70} be the set of all positive

divisors of 70. Define

a+b = l.c.m of a, b,

a.b = g.c.d. of a, b



Show that (B, +, . , /) is a Boolean Algebra.

Q 5: Give an example of a Boolean Algebra with 16 elements.

Q 6: Let B = {0, a, b, 1}. Define +, . , / in B as follows.

+	0	a	b	1
0	0	a	b	1
a	a	a	1	1
b	b	1	b	1
1	1	1	1	1

.	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

/	0	a	b	1
	1	b	a	0

Show that (B, +, . , /) is a Boolean Algebra.

Q 7: Let B = { 1, 2, 4, 5, 10, 20} be the set of all positive divisors of 20. Define

a+b = l.c.m. of a, b

a.b = g.c.d. of a, b



Examine if (B, +, . , /) is a Boolean Algebra.

14.4 BASIC LAWS OF BOOLEAN ALGEBRA

Let (B, +, . , /) be a Boolean Algebra. Let 0 be the zero element, and 1 be the unit element of B.

1. Idempotent Laws.

(i) a+a = a, (ii) a.a = a,

Proof : (i) a = a+0

= a + (a.a$^{/}$)

= (a+a).(a+a$^{/}$), by associative law

= (a+a).1

= a+a

i.e. a+a = a

(ii) a = a.1

= a.(a + $a^{/}$)

= (a.a) + (a.$a^{/}$), by associative law

= (a.a) + 0

= a.a

Note : The result (ii) is a dual of the result (i), and vice versa. The result (ii) can be obtained from (i) by replacing + by . , . by + , 0 by 1, 1 by 0.

2. Boundedness Laws

(i) a+1 = 1, (ii) a.0 = 0,

Proof : (i) a+1 = (a+1) . 1

= (a+1).(a+$a^{/}$)

= a+(1.$a^{/}$), by associative law

= a+$a^{/}$, (1.$a^{/}$ = $a^{/}$.1 = a)

= 1

(ii) a.0 = (a.0) + 0

= (a.0) + (a.$a^{/}$)

= a.(0+$a^{/}$), by associative law

= a.$a^{/}$, (0+$a^{/}$ = $a^{/}$+0 = $a^{/}$)

= 0

3. Absorption Laws

(i) a+(a.b) = a, (ii) a.(a+b) = a,

Proof : (i) a+(a.b) = (a.1) + (a.b)

= a.(1 + b)

= a.1, (1+b = b+1 = 1, by boundedness law)

= a

(ii) a.(a+b) = (a+0).(a+b)

= a+(0.b)

= a+0, (0.b = b.0 = 0, by boundedness law)

=a

4. Associative Laws

(i) (a+b)+c = a + (b+c)

(ii) (a.b).c = a.(b.c)

Proof : (i) Let L = (a+b) + c

R = a + (b+c)

Now a.L = a.((a+b)+c)

= a.(a+b) + a.c, by distributive law

= a + (a.c), by absorption law

= a, by absorption law

a . R = a.(a+(b+c))

= (a.a)+(a.(b+c)), by distributive law

= a+(a.(b+c)), by idempotent law

= a, by absorption law

$\square$ a.L = a.R

Again a'.L =a'.((a+b) + c)

= a'.(a+b) + (a'.c), by distributive law

= (a'.a) + (a'.b) + (a'.c), by distributive law

= 0 + (a'.b) + (a'.c)

= (a'.b) + (a'.c)

= a'.(b+c)

a'.R = a'.(a + (b+c))

= (a'.a) + a'.(b+c), by distributive law

= 0 + a'.(b+c)

= a'.(b+c)

$\square$ a'.L = a'.R

Now L = 1.L

= (a+a').L

= (a.L) + (a'.L)

= (a.R) + (a'.R)

= (a+a').R

= 1.R

= R

$\square$ L = R

i. e. (a+b) + c = a+(b+c)

(ii) Let L = (a.b).c

R = a. (b.c)

Now a + L = a + ((a.b).c)

= (a + (a.b)).(a+c), by distributive law

= a.(a+c), by absorption law

= a, by absorption law

a + R = a +(a.(b.c))

= (a+a).(a+(b.c)), by distributive law

= a.(a+(b.c)), by idempotent law

= a, by absorption law

$\square$ a + L = a+R

Again $a^{/}$+L = $a^{/}$ + (a.b).c)

= ($a^{/}$ + (a.b)).($a^{/}$+c), by distributive law

= (($a^{/}$+a).($a^{/}$+b)).($a^{/}$+c), by distributive law

= 1.($a^{/}$+b).($a^{/}$+c)

= ($a^{/}$+b).($a^{/}$+c)

= $a^{/}$ + (b.c)

$a^{/}$ + R = $a^{/}$ +(a.(b.c))

= ($a^{/}$+a).($a^{/}$ + (b.c)), by distributive law

= 1.($a^{/}$ + (b.c))

= $a^{/}$ + (b.c)

$\square$ $a^{/}$ + L = $a^{/}$ + R

Now L = 0 + L

= (a.$a^{/}$) + L

= (a+L).($a^{/}$+L)

= (a+R).($a^{/}$+R)

= (a.$a^{/}$) + R

= 0 + R

= R

$\square$ L = R

i.e. (a.b).c = a.(b.c)

5. Involution Law : $\square$

Proof : By definition of complement, we have

a+$a^{/}$ =1, and a.$a^{/}$ = 0

i. e. $a'+a = 1$, and $a'.a = 0$, by commutative law

$\square$ by uniquences of complement, a is the complement of a', i. c., $(a')' = a$.

6. De Morgan's Laws

(i) $(a+b)' = a'.b'$, (ii) $(a.b)' = a'+b'$

Proof : (i) $(a+b) + (a'.b') = b+a + (a'.b')$, by commutative law

$= b +(a+a').(a+b')$, by distributive law

$= b+1.(a+b')$

$= b + (a+b')$

$= b + (b'+a)$, by commutative law

$= (b+b') +a$, by associative law

$= 1+a$

$= 1$, by boundedness law

$(a + b).(a'.b') = ((a+b).a').b'$, by associative law

$= ((a.a') + (b.a')).b'$, by distributive law

$= (0 + (b.a')).b'$

$= (b.a').b'$

$= b.(a'.b')$, by associative law

$= b.(b'.a')$, by commutative law

$= (b.b').a'$, by associative law

$= 0.a'$

$= 0$

Thus, we see that $a'.b'$ is the complement of a+b,

i. e. $(a+b)' = a'.b'$

[Augustus De Morgan (1806 – 1871) was a famous mathematician. He was born in Madurai, India]

Corollary (i) $a+b = (a'.b')'$, (ii) $a.b = (a'+b')'$

Proof : (i) $(a'.b')' = (a')'+(b')'$, by De morgan's law

$= a+b$, by involution law

(ii) $(a'+b') = (a')'.(b')'$, by De morgan's law

$= a.b$, by involution law

7. (i) If $b+a = c+a$, and $b+a' = c+a'$, then $b = c$.

(ii) If $b.a = c.a$, and $b.a' = c.a'$, then $b = c$.

Proof : (i) $b = b+0$

$= b + (a.a^{/})$

$= (b+a).(b+a^{/})$, by distributive law

$= (c+a).(c+a^{/})$, (given)

$= c+(a.a^{/})$, by distributive law

$= c+0$

$= c.$

(ii) $b = b.1$

$= b.(a+a^{/})$

$= (b.a) + (b.a^{/})$, by distributive law

$= (c.a) + (c.a^{/})$, given

$= c.(a + a^{/})$

$= c.1$

$= c$

8. (i) $a+b^{/} = 1$ if and only if $a+b = a$

(ii) $a.b^{/} = 0$ if and only if $a.b = a$

Proof : (i) Let $a+b^{/} = 1$

Now $a + b = (a+b) . 1$

$= (a+b).(a+b^{/})$, given

$= (a+(b.b^{/})$, by distributive law

$= a+0$

$= a$

Conversely, Let $a+b = a$

Now $a+b^{/} = 1.(a+b^{/})$

$= (a+a^{/}).(a+b^{/})$

$= a+(a^{/}.b^{/})$, by distributive law

$= a+(a+b)^{/}$, by De morgan's law

$= a+a^{/}$, given

$= 1.$

(ii) Let $a.b^{/} = 0$

Now $a.b = a.b + 0$

$= a.b+a.b^{/}$, given

$= a.(b+b^{/})$, by distributive law

$= a . 1$

= a

Conversely, let a.b = a

Now $a.b' = 0 + a.b'$

$= (a.a') + (a.b')$

$= a.(a'+b')$, by distributive law

$= a.(a.b)'$, by De Mergan's law

$= a.a'$, given

$= 0$.

9. (i) $a+(a'.b) = a+b$

(ii) $a.(a'+b) = a.b$

Proof : (i) $a+(a'.b) = (a+a').(a+b)$, by distributive law

$= 1.(a+b)$

$= a+b$

(ii) $a.(a'+b) = (a.a') + (a.b)$

$= 0 + (a.b)$

$= a.b$

Example 4: Let B be a Boolean Algebra.

Let a, b ∎

$a.(a.b)' = a.b'$

Solution : $a.(a.b)'$

$= a.(a'+b')$, by De Morgan's law

$= (a.a') + (a.b')$

$= 0 + (a.b')$

$= a.b'$

Example 5: Let B be a Boolean Algebra, and a, b, c ∎

$(a+b).(b+c).(c+a) = a.b + b.c + c.a$

Solution : $(a+b).(b+c).(c+a)$

$= (a+b).(b.c + b.a + c.c + c.a)$

$= (a+b).(b.c + b.a + c + c.a)$

$= a.(b.c) + a.(b.a) + a.c + a.(c.a) + b.(b.c) + b.(b.a) + b.c + b.(c.a)$

$= a.b.c + a.(a.b) + a.c + a.(a.c) + (b.b).c + (b.b).a + b.c + a.b.c$

$= (a.b.c + a.b.c) + (a.a).b + a.c + (a.a).c + b.c + b.a + b.c)$

$= a.b.c + a.b + a.c + a.c + b.c + b.a + b.c$

= a.b.c + (a.b + a.b) + (a.c + a.c) + (b.c + b.c)

= a.b.c + a.b + a.c + b.c

= a.b. (c+1) + a.c + b.c

= a.b.1 + c.a + b.c

= a.b + b.c + c.a

Example 6 : Let B be a Boolean Algebra, and a, b

and only if a = 0 and b = 0 Write the dual of the above proposition and prove it

Solution : Let a = 0, and b = 0

a+b = 0+0

= 0

Converselt, Let a+b = 0

Now a = a+0

= a+(b.b$^{/}$)

= (a+b).(a+b$^{/}$), by distributive law

= 0.(a+b$^{/}$), given

=0

b = b+0

= b + (a.a$^{/}$)

= (b+a).(b+a$^{/}$)

= (a+b).(b+a$^{/}$)

= 0.(b+a$^{/}$)

= 0

2nd Part

Dual of the above proposition is a.b = 1

If a = 1, b = 1,

a.b = 1.1 = 1

Conversely, Let a.b = 1

Now a = a.1

= a.(b+b$^{/}$)

= (a.b) + (a.b$^{/}$)

= 1 + (a.b$^{/}$)

= 1

$b = b.1$

$= b.(a+a')$

$= (b.a) + (b.a')$

$= (a.b) + (b.a')$

$= 1 + (b.a')$

$= 1$

Example 7 : Let B be a Boolean Algebra and a, b, c
following expressions are equal.

(i) $(a+b).(a'+c).(b+c)$

(ii) $a.c + a'.b + b.c$

(iii) $(a+b).(a'+c)$

(iv) $a.c + a'.b$

Solution : $(a+b).(a'+c).(b+c)$

$= (a+b).(a'.b + a'.c + c.b + c.c)$

$= (a+b).(a'.b + a'.c + c.b + c)$

$= a.a'.b + a.a'.c + a.c.b + a.c + b.a'.b + b.a'.c + b.c.b + b.c$

$= 0.b + 0.c + a.c.b + a.c + b.a' + b.a'.c + b.c + b.c$

$= b.c.(a + a') + a.c + b.c + b.a'$

$= b.c.1 + a.c + b.c + a'.b$

$= b.c + a.c + b.c + a'.b$

$= a.c + a'.b + b.c$ (1)

Again, $(a+b).(a'+c)$

$= a.a' + a.c + b.a' + b.c$

$= 0 + a.c + a'.b + b.c$

$= a.c + a'.b + b.c$ (2)

Again, $a.c + a'.b + b.c$

$= a.c + a'.b + 1.b.c$

$= a.c + a'.b + (a+a').b.c$

$= a.c + a'.b + a.b.c + a'.b.c$

$= ((a.c) + (a.c).b) + ((a'.b) + (a'.b).c)$

$= a.c + a'.b$, by absortion law (3)

From (1), (2) and (3), we conclude that

$(a+b).((a'+c).(b+c)$

= a.c + $a^{/}$.b + b.c

= (a+b).($a^{/}$+c)

= a.c + $a^{/}$.b



CHECK YOUR PROGRESS

Q 8: Prove that there cannot be a Boolean Algebra with 3 elements.

Q 9: Let B be a Boolean Algebra, and let a, b, c B. If a+c=a, b+c=b, show that (a.b) + c = a.b

Q 10: Let B be a Boolean Algebra. Let a, b B. Show that a+(a+b)$^{/}$ = a+$b^{/}$.

Q 11: Let B be a Boolean Algebra, and let a, b B. Prove that the following properties are equivalent

(i) a+b=a, (ii) a+$b^{/}$=1, (iii) a.b=b

Write the dual of the above proposition and prove it.

Q 12: Let B be a Boolean Algebra, and let a, b, c B. Show that

[(abc+$a^{/}b^{/}$)$^{/}$ + bc]$^{/}$ = $a^{/}b^{/}$

[Here abc means a.b.c]

14.5 BOOLEAN EXPRESSION

Let us consider the Boolean Algebra B={0, 1}, where +, . , and $^{/}$ are defined by

+	0	1
0	0	1
1	1	1

.	0	1
0	0	0
1	0	1

/	0	0
	1	0

A literal symbol that is used to represent an element of B is called a Boolean variable. Thus, if x denotes a Boolean variable, then x will have the value 0 or 1. If x is a Boolean variable, $x^{/}$ is also a Boolean variable.

Let x, y be two Boolean variables. The values of x, y may be given by the following table.

x	y

1	1
1	0
0	1
0	0

Let x, y, z be three Boolean variables. The values of x, y, z may be given by the following table.

x	y	z
1	1	1
1	1	0
1	0	1
0	1	1
1	0	0
0	1	0
0	0	1
0	0	0

By a Boolean expression, we mean an expression that is construted by a finite set of symbols, each representing a Boolean variable, by applying the binary operations +, and . , and the unary operation /. Thus. $x.y + x^{/}$ is a Boolean expression of two variables. Similarly x.y+y.z+z.x is a Boolean expression of three variables.

We note that 0 and 1 are Boolean expressions. Any variable is a Boolean expression.

Corresponding to a Boolean expression, we can construct a table known as the truth table (or the assignment table or the value table).

We construct a truth table for the Boolean expression $xy+x^{/}$ (By xy we mean x.y).

x	y	xy	$x^{/}$	$xy+x^{/}$
1	1	1	0	1
1	0	0	0	0
0	1	0	1	1
0	0	1	1	1

Two Boolean expressions of variables $x_1, x_2, \ldots, x_n$ are said to be

equal if they assume the same values for every assignment of values 0, 1 to the variables $x_1, x_2, \ldots, x_n$.

The equality of two Boolean expressions is denoted by " = ".

Example 8: Construct the truth table for the Boolean expression xy + xz of the variables x, y, z.

Solution :

x	y	z	xy	xz	xy+xz
1	1	1	1	1	1
1	1	0	1	0	1
1	0	1	0	1	1
0	1	1	0	0	0
1	0	0	0	0	0
0	1	0	0	0	0
0	0	1	0	0	0
0	0	0	0	0	0

Example 9: Construct the truth table for the Boolean expression $xy+x'y+xy'+x'y'$ of the variables x, y.

Solution :

x	y	x'	y'	xy	$x'y$	xy'	$x'y'$	$xy+x'y+xy'+x'y'$
1	1	0	0	1	0	0	0	1
1	0	0	1	0	0	1	0	1
0	1	1	0	0	1	0	0	1
0	0	1	1	0	0	0	1	1

Example 10: Prove that the Boolean expressions $(xy+x)'$ and $(x'+y')x'$ are equal.

Solution :

x	y	xy	xy+x	$(xy+x)'$
1	1	1	1	0
1	0	0	1	0
0	1	0	0	1
0	0	0	0	1

Again,

x	y	x'	y'	$x'+y'$	$(x'+y')x'$
1	1	0	0	0	0
1	0	0	1	1	0
0	1	1	0	1	1
0	0	1	1	1	1

Looking at the last column of the above two tables, we conclude that $(xy+x)' = (x'+y')x'$.



CHECK YOUR PROGRESS

Q 13: Let $f(x, y, z) = xy + z'$ be a Boolean expression of three variables x, y, z. Find the values of f(1, 1, 0), f(0, 1, 1), f(0, 1, 0), f(1, 1, 1), f(0, 0, 0).

Q 14: Construct truth tables for the following Boolean expressions.

(i) $x + yx'$ (ii) $x(x+y')$

(iii) $xy + yz + zx$ (iv) $xy' + x(y'+z)$

Q 15: Examine if the following Boolean expressions are equal

(i) $(x+y)'$, $x'y'$

(ii) $(xy)'$, $x' + y'$

(iii) $x(y+z)$, $xy+xz$

(iv) $xz + (x'+y')'$, $x(y+z)$



14.6 LET US SUM UP

- Let B be a non-empty set equipped with two binary operations + and . , a unary operation /, and two distinct elements 0 and 1. Then B is called a Boolean Algebra if the following conditions are satisfied.

  1. (i) a+b = b+a, (ii) a.b = b.a,
  2. (i) a+ (b.c) = (a+b).(a+c)

     (ii) a.(b+c) = (a.b)+(a.c),
  3. (i) a+0 = a, (ii) a.1 = 1,

(ii) $a+a^{/} = 1$, (ii) $a.a^{/} = 0$,

0 is called the zero element.

1 ia called the unit element.

$a^{/}$ is the complement of a.

- In a Boolean Algebra, zero element is unique.
- In a Boolean Algebra, unit element is unique.
- In a Boolean Algebra, complement of each element is unique.
- In a Boolean Algebra B, $1^{/} = 0$, $0^{/} = 1$.
- Every statement and every theorem in a Boolean Algebra remains valid if the binary operations + and . , and the zero element 0 and the unit element 1 are interchanged. This principle is known as the principle of duality.
- In a Boolean Algebra B,

  1. (i) $a+a = a$, (ii) $a.a = a$,
  2. (i) $a+1 = 1$, (ii) $a.0 = 0$
  3. (i) $a+(a.b) = a$, (ii) $a.(a+b) = a$
  4. (i) $(a+b)+c = a+(b+c)$

     (ii) $(a.b).c = a.(b.c)$,
  5. $(a^{/})^{/} = a$
  6. (i) $(a+b)^{/} = a^{/}.b^{/}$, (ii) $(a.b)^{/} = a^{/}+b^{/}$
  7. (i) If $b+a=c+a$, and $b+a^{/} = c+a^{/}$, then $b=c$

     (ii) If $b.a. = c.a$, and $b.a^{/} = c.a^{/}$, then $b=c$
  8. (i) $a+b^{/}=1$ if and only if $a+b = a$

     (ii) $a.b^{/} = 0$ if and only if $a.b = a$
  9. (i) $a+(a^{/}.b) = a+b$

     (ii) $a.(a^{/}+b) = a.b$
- A literal symbol that is used to represent an element of the Boolean Algebra B = {0, 1} is called a Boolean variable. In B, +, . , / are defined by

+	0	1
0	0	1
1	1	1

.	0	1
0	0	0
1	0	1

/	0	
	1	0

- By a Boolean expression, we mean an expression that is constructed by a finite set of symbols, each representing a Boolean variable, by

applying the binary operations + and . , and the unary operation /.

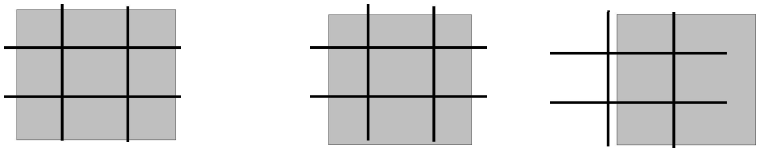
- 0 and 1 are Boolean expressions.
- Any variable is a Boolean expression.
- Two Boolean expressions of variables $x_1, x_2, \ldots, x_n$ are said to be equal if they assume the same values for every assignment of values 0, 1 to the variables $x_1, x_2, \ldots, x_n$.

  The equality of two Boolean expressions is denoted by " = ".

14.7 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Here x = {1}

P(x) = {{1},



From the tables, we see that is a binary operation on P(x), binary operation on P(x), / is a unary operation on P(x).

Now, 1. (i)

(ii)

2. (i)

(ii)

3. (i)

(ii)

4. (i)

(ii)

is a Boolean Algebra, where

and {1} is the unit element.

Ans to Q No 2: Left as an exercise.

Ans to Q No 3: We construct the composition tables for +, . , / as follows.

+	1	2	3	5	6	10	15	30
1	1	2	3	5	6	10	15	30
2	2	2	6	10	6	10	30	30
3	3	6	3	15	6	30	15	30
5	5	10	15	5	30	10	15	30
6	6	6	6	30	6	30	30	30
10	10	10	30	10	30	10	30	30
15	15	30	15	15	30	30	15	30
30	30	30	30	30	30	30	30	30

.	1	2	3	5	6	10	15	30
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
3	1	1	3	1	3	1	3	3
5	1	1	1	5	1	5	5	5
6	1	2	3	1	6	2	3	6
10	1	2	1	5	3	5	15	15
15	1	1	3	5	3	5	15	15
30	1	2	3	5	3	10	15	30

/	1	2	3	5	6	10	15	30
	30	15	10	6	5	3	2	1

From the above tables, we see that + is a binary operation on B, . is a binary operation on B, and $'$ is a unary operation on B.

Again, 1. (i) a+b = l.c.m of a, b

= l.c.m of b, a

= b+a,

(ii) a.b = g.c.d of a, b

= g.c.d of b, a

= b.a,

2. From the tables, we have

(i) a+(b.c) = (a+b).(a+c)

(ii) a.(b+c) = (a.b)+(a.c),

3. (i) a+1 = l.c.m of a, 1 = a,

(ii) a. 30 = g.c.d of a, 30 = 1,

4. (i) $a+a^{/}$ = l.c.m of a, $a^{/}$

= l.c.m of a,

= 30

(ii) $a.a^{/}$ = g.c.d of a, $a^{/}$

= g.c.d of a,

=1

(B, +, . , /) is a a Boolean Algebra, where 1 is the zero element, and 30 is the unit element.

Ans to Q No 4: Left as an exercise.

Ans to Q No 5: Let X = {1, 2, 3, 4}

Then the power set P(x) of x contains 2^4 i.e. 16 elements.

The set P(x) is a Boolean Algebra under operations of union, intersection, and complementation in P(x).

Ans to Q No 6: Here B = {0, a, b, 1}

+, . , / are defined in B as follows

+	0	a	b	1
0	0	a	b	1
a	a	a	1	1
b	b	1	b	1
1	1	1	1	1

.	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

/	0	a	b	1
	1	b	a	0

From the tables, we see that + is a binary operation on B, . is a binary operation on B, $^{/}$ is a unary operation on B.

Now,

1. (i) + is commutative on B.

   (ii) . is commutative on B.

2. (i) + is distributive over . in B

   (ii) . is distributive over + in B

3. (i) a+0 = a

   (ii) a.1 = 1,

4. (i) $a+a' = 1$

(ii) $a.a' = 0$,

(B, +, . , /) is a Boolean Algebra, where 0 is the zero element, and 1 is the unit element.

Ans to Q No 7: Here B = {1, 2, 4, 5, 10, 20} is the set of all positive divisors of 20.

We construct the composition tables as follows.

+	1	2	4	5	10	20
1	1	2	4	5	10	20
2	2	2	4	10	10	20
4	4	4	4	20	20	20
5	5	10	20	5	10	20
10	10	10	20	10	10	20
20	20	20	20	20	20	20

.	1	2	4	5	10	20
1	1	1	1	1	1	1
2	1	2	2	1	2	2
4	1	2	4	1	2	4
5	1	1	1	5	5	5
10	1	2	2	5	10	10
20	1	2	4	5	10	20

/	1	2	4	5	10	20
	20	10	5	4	2	1

From the tables, we see that + is a binary operation on B, . is a binary operation on B, / is a unary operation on B.

Now, 1 (i) a+b = l.c.m of a, b

= l.c.m of b, a

= b+a

(ii) a.b = g.c.d of a, b

= g.c.d of b, a

= b.a

2. From the tables, we have

(i) a+(b.c) = (a+b), (a+c)

(ii) a.(b+c) = (a.b) + (a.c),

3. (i) a+1 = l.c.m of a, 1=a

(ii) a.20 = g.c.d of a, 20

= a,

The conditions 4 (i), and 4 (ii) are not satisfied. For

$10+10' =$ l.c.m of 10, $10'$

= l.c.m of 10, 2=10

B is not a Boolean Algebra.

Note : We state the following theorem without proof.

Let n > 1 be a natural number. Let B be the set of all positive divisors of n. We define +, . , / in B as follows.

a+b = l.c.m of a, b

a.b = g.c.d of a, b

$a^{/}$ =

Then B is a Boolean Algebra if and only n is not divisible by any square intager.

In the above example, n = 20 and 20 is divisible by 4, which is a square integer.

Ans to Q No 8: If possible, let B be a Boolean Algebra with 3 elements.

Let B {0, 1, a}, where

We know that $0^{/} = 1$, $1^{/} = 0$

$a^{/} = a$

Now a = a.a

= $a.a^{/}$

= 0, which is a contradition

there cannot be a Boolean Algebra with 3 elements.

Ans to Q No 9: (a.b) + c = c+(a.b), by commutative law

= (c+a).(c+b), by distributive law

= (a+c). (b+c), by commutative law

= a.b, (given)

Ans to Q No 10: $a+(a+b)^{/} = a+(a^{/}.b^{/})$

$= (a+a^{/}).(a+b^{/})$

$= 1. (a+b^{/})$

$= a+b^{/}$

Ans to Q No 11: First we prove that (i)

We have a+b = a

$a+b^{/} = 1. (a+b^{/})$

$= (a+a^{/}).(a+b^{/})$

$= a+(a'.b')$

$= a+(a+b)'$

$= a+a'$

$= 1$

Next we prove that (ii) ▢

We have $a+b' = 1$

▢ $a+b = (a+b).1$

$= (a+b).(a+b')$

$= a+(b.b')$

$= a+0$

$= a$

Now $a.b = (a+b).b$

$= b.(a+b)$

$= b.\ (b+a)$

$= b$, by absorption law

Next we prove that (iii) ▢

We have $a.b = b$

Now $a+b = a+ (a.b)$

$= a$, by absorption law

Thus, we see that the properties (i), (ii), and (iii) are equivalent.

2nd Part : The dual of the above proposition is

(i) $a.b = a$, (ii) $a.b' = 0$, (iii) $a+b = b$

It can be proved by replacing . by + , + by . , 1 by 0, and 0 by 1 in the first part.

Ans to Q No 12: $[(abc+a'b')' + bc]'$

$= (abc+a'b')\ (b'+c')$, by De Mergan's law

$= abc\ b' + abc\ c' + a'b'b'+a'b'c'$

$= ac\ 0 + ab\ 0 + a'b' + a'b'c'$, $[bb'=0,\ cc' = 0,\ b'b'=b']$

$= a'b' + a'b'c'$

$= a'b'\ 1 + a'b'c'$

$= a'b'\ (1+c')$

$= a'b'$, $1+c'=1$

Ans to Q No 13: $f(x, y, z) = xy+z'$

$f(1, 1, 0) = 1.1 + 0'$

$= 1+1$

$= 1$

$f(0, 1, 1) = 0.1 + 1'$

$= 0 + 0$

$= 0$

$f(0, 1, 0) = 0.1 + 0'$

$= 0+1$

$= 1$

$f(1, 1, 1) = 1.1.+1'$

$= 1+0$

$= 1$

$f(0, 0, 0) = 0.0 + 0'$

$= 0+1$

$= 1$

Ans to Q No 14:

(i)

x	y	x'	yx'	$x+yx'$
1	1	0	0	1
1	0	0	0	1
0	1	1	1	1
0	0	1	0	0

(ii)

x	y	y'	$x+y'$	$x(x+y')'$
1	1	0	1	1
1	0	1	1	1
0	1	0	0	0
0	0	1	1	0

(iii)

x	y	z	xy	yz	zx	xy+yz+zx
1	1	1	1	1	1	1
1	1	0	1	0	0	1
1	0	1	0	0	1	1
0	1	1	0	1	0	1
1	0	0	0	0	0	0
0	1	0	0	0	0	0
0	0	1	0	0	0	0
0	0	0	0	0	0	0

(iv) Left as an exercise

Ans to Q No 15:

(i)

x	y	x+y	$(x+y)'$	x'	y'	$x'y'$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

From column 4 and column 7, we conclude that $(x+y)' = x'y'$

(ii) Left as an exercise.

(iii) Left as an exercise.

(iv)

x	y	z	xz	x'	y'	$x'+y'$	$(x'+y')'$	$xz+(x'+y')'$	y+z	x(y+z)
1	1	1	1	0	0	0	1	1	1	1
1	1	0	0	0	0	0	1	1	1	1
1	0	1	1	0	1	1	0	1	1	1
0	1	1	0	1	0	1	0	0	1	0
1	0	0	0	0	1	1	0	0	0	0
0	1	0	0	1	0	1	0	0	1	0
0	0	1	0	1	1	1	0	0	1	0
0	0	0	0	1	1	1	0	0	0	0

From column 9 and column 11, we conclude that

$xz + (x'+y')' = x(y+z)$

14.8 FURTHER READING

1) Sen, M. K, Chakraborty B. C. : *Introduction to Discrete Mathematies* (2010), Books and Allied (P) Ltd, Kolkata 700010.

2) Dasgupta Asok : *Abstract and Linea Algebra* (2014), Asoke Prakasan, Kolkata 700007.

14.9 MODEL QUESTIONS

Q 1: Let X = {1, 2}. Let P (x) be the power set of X. Show that the set P(x) is a Boolean Algebra under union, intersection, and complementation in P(x).

Q 2: Let B = {1, 2, 5, 10, 17, 34, 85, 170} be the set of all positive divisors of 170. Define +, . , / in B as follows.

a+b = l.c.m of a, b

a.b = g.c.d of a, b

$a^{/}$ =

Examine if (B, +, . , /) is a Boolean Algebra.

Q 3: Let B = {1, 2, 3, 4, 6, 8, 12, 24} be the set of all positive divisors of 24. Define +, . , / in B as follows.

a+b = l.c.m of a, b

a.b = g.c.d of a, b

$a^{/}$ =

Examine if (B, +, . , /) is a Boolean Algebra.

Q 4: Let (B, +, . , /) be a Boolean Algebra, and let a, b

following in simplied form

(i) $(a+b).(a^{/}+b^{/}).(a^{/}+b).(a+b^{/})$

(ii) $(a.b)+(a^{/}.b)+(a.b^{/})+(a^{/}.b^{/})$

Q 5: Let (b, +, . , /) be a Boolean Algebra, and let a, b, c, d

a.c + b.d = (a+b).(b+c).(c+d).(d+a)

Q 6: Give an example of a Boolean Algebra that has infinite number of elements.

Q 7: Let (B, +, . , /) be a Boolean Algebra, and let a, b, c

$(a+b')\cdot(b+c')\cdot(c+a')=(a'+b)\cdot(b'+c)\cdot(c'+a)$

Q 8: Let $f(x, y, z) = x.y.z + x.y'.z + x'.y.x + x'.y'.z'$ be a Boolean expression of three variables x, y, z. Find the values of f(1, 1, 1), f(1, 1, 0), f(1, 0, 1), f(0, 1, 1), f(0, 0, 0).

Q 9: Construct truth tables for the following Boolean expressions

(i) $xy+x(x+y)$ (ii) $x'y+xy'+x(x+y')$ (iii) $xyz+xy'z+x'yz+xyz'$

Q 10: Examine if the following Boolean expressions are equal

(i) $(x+y+z)'$, $x'y'z'$

(ii) $(xyz)'$, $x'+y'+z'$

(iii) $x.(x+y)$, x

(iv) $(x+y)z'$, $xz'+yz'$

*** ***** ***



REFERENCES

- Fraleigh, John B : A First in Abstract Algebra (First Indian Reprit, 2003, Person Education (Singapore) Pvt. Ltd., Indian Delhi 110, 092.
- Mapa, S. K. : Higher Algebra (Abstract and Linear) (1994), Ashok Prakashan, Calcutta 700 007.
- Khanna, V. K. and Bhambri, S. K. : A Course in Abstract Algebra (2006), Vikas Publishing House Pvt. Ltd, New Delhi 110 014.
- Singh, Surajeet and Zameeruddin, Qazi Modern Algebra (2006, Vikas Publishing House Pvt. Ltd, New Delhi 110 014.
- Tamuli B. K. : Contemporary Algebra (1977), New Book Stall, Guwahati-781 001.
- Pundir S . K. : Advance Abstract Algebra, Krishna Prakashan Media (P) Ltd, Meerut 250 001
- Sharma, J. K. : Discrete Mathematics, Macmillian Publishing India Ltd., New Delhi- 110002