Page No.:
Date : / /

Algebra Copy Notes

by

Mukesh Singh
(ICT 5th batch, 2073)

Sukuna Multiple Campus
Sundarharaincha-12, Morang

Date : / /

Units	Unit name / Contents	Page
Unit-1	Matrices and Determinants	
	1.1 Definition of Matrices	
	1.2 Some Basic Matrices	
	1.3 Algebra of Matrices	
	1.4 Determinants and its Properties	
	1.5 Inverse Matrix	
	1.6 Rank of Matrix	
	1.7 System of linear Equations	
Unit-2	Group Theory	
	2.1 Algebraic System, Binary Operation and its Properties	
	2.2 Cayley's tables	
	2.3 Equivalence relation, Congruence modulo	
	2.4 Group and its Properties	
	2.5 Integral power of elements of a group	
	2.6 Cyclic groups and permutation group	
	2.7 Elementary properties of groups, cyclic groups and permutation group	
	2.8 Subgroup and its Properties	
	2.9 Cosets of a sub-group	
	2.10 Lagrange's theorem	
	2.11 Normal sub-groups	
	2.12 Quotient group	
Unit-3	Group Homorphism	
	3.1 Homorphisms, Endomorphism, Automorphism and Isomorphism	

3.2 Isomorphism theorems: fundamental theorems, diamond and quotient isomorphism theorems, correspondence theorem

Unit-4 Ring Theory (8)

4.1 Definition of Rings and its special classes with examples
4.2 Elementary Property of Rings
4.3 Sub rings, Ideals and Quotient rings with their properties
4.4 Homomorphism of Rings
4.5 Integral Domain (ID), Principal Ideal Domain (PID), Euclidean Domain (ED), Unique Factorization Domain (UFD)

Unit-5 Vector Spaces (5)

5.1 Definition and examples of Vector spaces
5.2 Subspaces
5.3 Linear Combination: linear independence and linear dependence
5.4 Basis and dimension of a vector space

Unit-6 Linear Transformation (5)

6.1 Definition and examples of linear transformations
6.2 Kernel and image of linear transformation
6.3 Algebra of linear transformation
6.4 Matrix representation of linear transformation
6.5 Eigen values and Eigen vectors

Page No.:
Date : / /

Unit-7 Field Theory (5)

7.1. Introduction
7.2 Subfield
7.3 Prime Field
7.4 Field extension and degree of field extension
7.5 Algebraic and transcendental elements

Unit-1

Matrices and Determinants

Page No.:
Date : / /

1.1 Definition of Matrices

A matrix is a rectangular array of numbers or symbols which are generally arranged in rows and columns.

The order of the matrix is defined as the number of rows and columns.

Example

We have a 2×3 matrix that is because the number of rows here is 2 and number of column is 3.

$$A = \begin{bmatrix} -2 & 5 & 6 \\ 5 & -2 & 7 \end{bmatrix}$$

1.2 Some basic matrices

1. Null or Zero Matrix

A matrix having all the elements zero (0) is called a null matrix. It is denoted by O. Thus, $A=[a_{ij}]_{m\times n}$ is a null matrix if $a_{ij}=0$ for all i and j.

Example

$$O=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

2. Row Matrix

A matrix having only one row is called a row matrix. It is represented as $A=[a_{ij}]_{1\times n}$.

Example

$$A=[1\ 2\ 3\ 4]$$

3. Column Matrix

A matrix having only one column is called a column matrix. It is represented as $A=[a_{ij}]_{m\times 1}$.

Example

$$A=\begin{bmatrix}3\\4\\5\end{bmatrix}$$

4. Singleton Matrix

A matrix having only one element is called a singleton matrix.

Example

[2], [3]

5. Horizontal Matrix

A matrix of order $m\times n$ is a horizontal

matrix if $n > m$ i.e. no. of column is greater than number of rows.

Example

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 5 & 1 & 1 \end{bmatrix}$$ Here, $m = 2, n = 4$

$\therefore n > m$.

6. Vertical matrix

A matrix of order $m \times n$ is a vertical matrix if $m > n$ i.e. no. of rows greater than no. of columns.

Example: $$\begin{bmatrix} 2 & 5 \\ 1 & 1 \\ 3 & 6 \end{bmatrix}$$ Here $m = 3, n = 2$

$\therefore m > n$

7. Square matrix

A matrix having equal number of rows and columns is called a square matrix.

Example $$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$ Here, $m = n$

8. Triangular Matrix

A matrix having all of its elements above the diagnol or below the diagnol zero is called a triangular matrix.

Example:

① $$\begin{bmatrix} 1 & 0 & 0 \\ 2 & 4 & 0 \\ 3 & 5 & 6 \end{bmatrix}$$ Lower triangular matrix

② $$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 6 & 5 \\ 0 & 0 & 9 \end{bmatrix}$$ Upper triangular matrix

9. Diagnol Matrix

If all the elements, except the principle diagnol in a square matrix, are zero, it is called a diagnol matrix.

Example $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{bmatrix}$

10. Scalar Matrix

If all the elements in the diagnol of a diagnol matrix are equal, it is called a scalar matrix.

Example $\begin{bmatrix} 7 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 7 \end{bmatrix}$

11. Unit or Identity Matrix

If all the elements of a principle diagnol in a diagnol matrix are 1, then it is called a unit matrix.

Example $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

12. Symmetric Matrix

A square matrix $A=[a_{ij}]$ is known as symmetric matrix if $a_{ij}=a_{ji}$, for all i, j values.

For example:

$$A=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 2 \end{pmatrix}$$

Date : / /

13. Skew-Symmetric Matrix

A square matrix $A = [a_{ij}]$ is a skew-symmetric matrix if $a_{ij} = a_{ji}$, for all values of i, j.

Thus, in a skew-symmetric matrix, all diagonal elements are zero.

Example

$$A = \begin{bmatrix} 0 & 2 & 1 \\ -2 & 0 & -3 \\ -1 & 3 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 2 \\ -2 & 0 \end{bmatrix}$$

Date : / /

1.3 Algebra of Matrices

Algebra of matrices is the branch of mathematics, which deals with vector spaces between different dimensions.

Algebra of matrix involves the operation of matrices, such as Addition, Subtraction, multiplication, etc.

Addition / Subtraction of Matrices

Two matrices can be added / subtracted, iff (if and only if) the number of rows and columns of both the matrices are same, or the order of the matrices are equal.

For addition / subtraction, each element of the first matrix is added / subtracted to the elements present in the 2nd Matrix.

Example

① Addition

$$\begin{bmatrix} 2 & 0 & 5 \\ 3 & 2 & 9 \end{bmatrix} + \begin{bmatrix} 7 & 4 & 1 \\ 8 & 13 & 0 \end{bmatrix} = \begin{bmatrix} 9 & 4 & 6 \\ 11 & 15 & 9 \end{bmatrix}$$

② Subtraction

$$\begin{bmatrix} 10 & -20 & 30 \\ 40 & 50 & 60 \end{bmatrix} - \begin{bmatrix} 1 & -2 & 3 \\ 4 & -5 & 6 \end{bmatrix} = \begin{bmatrix} 9 & -18 & 27 \\ 36 & 55 & 54 \end{bmatrix}$$

Matrix Multiplication

Matrix can be multiplied in two ways:

(i) Scalar multiplication → It involves multiplying a matrix by a scalar quantity.

Eg:

$$5 \times \begin{bmatrix} 5 & 7 \\ 12 & 3 \\ 6 & 2 \end{bmatrix} = \begin{bmatrix} 25 & 35 \\ 60 & 15 \\ 30 & 10 \end{bmatrix}$$

(ii) Multiplication with another matrix: Two matrix can be multiplied iff the number of column of the first matrix is equal to the number of rows of the second matrix.

Consider two matrices M_1 & M_2, having order of $m_1 \times m_1$ and $m_2 \times n_2$,

The matrices can be multiplied if and only if $n_1 = m_2$.

$$\underbrace{\begin{bmatrix} 1 & 2 & 3 \end{bmatrix}}_{1\times 3} \times \underbrace{\begin{bmatrix} 2 & 1 & 3 \\ 3 & 3 & 2 \\ 4 & 1 & 2 \end{bmatrix}}_{3\times 3} = \begin{bmatrix} 1.2+2.3+3.4 \\ 1.1+2.3+3.1 \\ 1.3+2.2+3.2 \end{bmatrix} = \underbrace{\begin{bmatrix} 20 \\ 10 \\ 13 \end{bmatrix}}_{1\times 3}$$

The matrices, given above satisfies the condition for matrix multiplication, hence it is possible to multiply these matrices.

The resultant matrix obtained by multiplication of two matrices, is the order of m_1, n_2, where m_1 is the number of rows in the 1st matrix and n_2 is the number of column of the 2nd matrix.

Date : / /

1.4 Determinants and its properties

Determinants are the scalar quantity obtained by the sum of products of the elements of a square matrix according to a prescribed rule. The determinants help to find the adjoint, inverse of a matrix. Determinants are represented similar to a matrix but with a modulus sign. Determinant of a matrix A is denoted by $|A|$ or $\det(A)$.

Properties of Determinants of Matrices:

1) Reflection Property → The determinant remains unaltered if its rows are changed into columns and the columns into rows.

2) All-Zero Property → If all the elements of a row (or column) are ~~proportional (identical) to the same~~ zero, then the determinant is zero.

3) Proportionality (Repetition) Property → If all the elements of a row (or column) are proportional (identical) to the elements of some other row (or column), then the determinant is zero.

4) Switching Property → The interchange of any two rows (or columns) of the determinant changes its sign.

5) Scalar Multiple Property → If all the elements of a row (or column) of a determinant are multiplied by non-zero constant, then the determinant gets multiplied by the same constant.

6) Sum Property →

$$\begin{vmatrix} a_1+b_1 & c_1 & d_1 \\ a_2+b_2 & c_2 & d_2 \\ a_3+b_3 & c_3 & d_3 \end{vmatrix} = \begin{vmatrix} a_1 & c_1 & d_1 \\ a_2 & c_2 & d_2 \\ a_3 & c_3 & d_3 \end{vmatrix} + \begin{vmatrix} b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \\ b_3 & c_3 & d_3 \end{vmatrix}$$

7) Property of Invariance

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1+\alpha b_1+\beta c_1 & b_1 & c_1 \\ a_2+\alpha b_2+\beta c_2 & b_2 & c_2 \\ a_3+\alpha b_3+\beta c_3 & b_3 & c_3 \end{vmatrix}$$

That is, determinant remains unaltered under an operation of the form $C_i \to C_i + \alpha C_j + \beta C_k$, where $j, k \neq i$ or an operation of the form: $R_i \to R_i + \alpha R_j + \beta R_k$, where $j, k \neq i$.

8) Factor Property → If a determinant Δ becomes zero when we put $x = \alpha$, then $(x-\alpha)$ is a factor of Δ.

9) Triangle Property → If all the elements above or below the main diagnol consist of zeros, then the determinant is equal to the product of diagnol elements. That is,

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ 0 & b_2 & b_3 \\ 0 & 0 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & 0 & 0 \\ a_2 & b_2 & 0 \\ a_3 & b_3 & c_3 \end{vmatrix} = a_1 b_2 c_3$$

10) Determinant of a Cofactor matrix:

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \text{ then } \Delta_1 = \begin{vmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{vmatrix}$$

where, C_{ij} denotes the Cofactor of the elements a_{ij} in Δ.

Page No.:
Date : / /

Q1. Find the determinant of the matrix A, where $A = \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$

Soln:

The determinant of matrix A is

$$|A| = \begin{vmatrix} 4 & 1 \\ 3 & 2 \end{vmatrix} = (4 \times 2) - (3 \times 1)$$
$$= 8 - 3$$
$$= 5$$

Q2. Find the determinant of matrix A, where

$$A = \begin{bmatrix} 1 & 3 & 2 \\ -3 & -1 & -3 \\ 2 & 3 & 1 \end{bmatrix}$$

Soln:

$$|A| = 1 \cdot \begin{vmatrix} -1 & -3 \\ 3 & 1 \end{vmatrix} - 3 \begin{vmatrix} -3 & -3 \\ 2 & 1 \end{vmatrix} + 2 \begin{vmatrix} -3 & -1 \\ 2 & 3 \end{vmatrix}$$

Using determinant rule,

$$|A| = 1.(-1-(-9)) - 3(-3-(-6)) + 2(-9-(-2))$$
$$= 1(-1+9) - 3(-3+6) + 2(-9+2)$$
$$= 8 - 9 - 14$$
$$= -15$$

$\therefore |A| = -15$

Page No.:
Date : / /

1.5 Inverse of Matrix

Inverse of a matrix is usually defined for square matrices. For every $n \times n$ square matrix, there exists an inverse matrix. If A is the square matrix then A^{-1} is the inverse of matrix A and satisfies the property: $AA^{-1} = A^{-1}A = I$, where I is the identity matrix.

The determinant of square matrix here, should not be equal to zero.

The inverse matrix formula can be given as,

$$A^{-1} = \frac{1}{|A|} \cdot \text{Adj } A \quad \text{where } |A| \neq 0.$$

(A is a square matrix.

Page No.:
Date : / /

Q. Find the inverse of matrix A, where

$$A = \begin{bmatrix} 1 & 0 & -1 \\ 3 & 4 & 5 \\ 0 & -6 & -7 \end{bmatrix}$$

Soln:

By using the formula $A^{-1} = \frac{\text{adj } A}{|A|}$, we can obtain the value of A^{-1}.

We have

$$A_{11} = \begin{bmatrix} 4 & 5 \\ -6 & -7 \end{bmatrix} = -28+30 = 2$$

$$A_{12} = -\begin{bmatrix} 3 & 5 \\ 0 & -7 \end{bmatrix} = -(-21-0) = 21$$

$$A_{13} = \begin{bmatrix} 3 & 4 \\ 0 & -6 \end{bmatrix} = -18-0 = -18$$

$$A_{21} = -\begin{bmatrix} 0 & -1 \\ -6 & -7 \end{bmatrix} = -(0-6) = 6$$

$$A_{22} = \begin{bmatrix} 1 & -1 \\ 0 & -7 \end{bmatrix} = -7-0 = -7$$

$$A_{23} = -\begin{bmatrix} 1 & 0 \\ 0 & -6 \end{bmatrix} = -(-6-0) = 6$$

$$A_{31} = \begin{bmatrix} 0 & -1 \\ 4 & -5 \end{bmatrix} = 0+4 = 4$$

$$A_{32} = -\begin{bmatrix} 1 & -1 \\ 3 & 5 \end{bmatrix} = -(5+3) = -8$$

$A_{33} = \begin{bmatrix} 1 & 0 \\ 3 & 4 \end{bmatrix} = 4 - 0 = 4$

$\therefore \text{Adj of } A = \begin{bmatrix} 2 & 21 & 18 \\ 6 & -7 & 6 \\ 4 & -8 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 6 & 4 \\ 21 & -7 & -8 \\ 18 & 6 & 4 \end{bmatrix}$

Also, $|A| = \begin{vmatrix} 1 & 0 & -1 \\ 3 & 4 & 5 \\ 0 & -6 & -7 \end{vmatrix} = \{4 \times (-7) - (-6) \times 5 - 3 \times (-6)\}$

$= -28 + 30 + 18 = 20$

$\therefore A^{-1} = \frac{\text{adj } A}{|A|} = \frac{1}{20} \begin{bmatrix} 2 & 6 & 4 \\ 21 & -7 & -8 \\ 18 & 6 & 4 \end{bmatrix}$

1.6 Rank of Matrix

The rank of the matrix refers to the number of linearly independent rows or columns in the matrix. $\rho(A)$ is used to denote the rank of matrix A. A matrix is said to be of rank zero when all of its elements become zero. The rank of the matrix is the dimension of the vector space obtained by its columns. The rank of matrix cannot exceed more than the number of its rows or columns. The rank of null matrix is zero.

Properties of the Rank of the Matrix:

→ Rank in linear algebra refers to finding column rank or row rank collectively known as the rank of the matrix.

→ Zero matrices have non-zero row. Hence it is an independent row (or column). So the rank of the zero matrix is zero.

→ When the rank equals the smallest dimension it is called full rank matrix.

The rank is commonly denoted by rank(A) or rk(A).

Page No.:
Date : / /

Q1. What is the rank of the matrix $X = \begin{bmatrix} 1 & 2 & 4 & 4 \\ 3 & 4 & 8 & 0 \end{bmatrix}$

Soln:

Since the matrix has more than zero elements, its rank must be greater than zero. And since it has fewer row than columns, its maximum rank is equal to the maximum number of linearly independent row. And because neither row is linearly dependent on the other row, the matrix has 2 linearly independent rows; so its rank is 2.

Q2. Find the rank of the following

$$\begin{pmatrix} 1 & -1 & 2 \\ 3 & 1 & 0 \\ 2 & -2 & 5 \end{pmatrix}$$

Here, $A = \begin{pmatrix} 1 & -1 & 2 \\ 3 & 1 & 0 \\ 2 & -2 & 5 \end{pmatrix}$ is of order 3 so we can have the minor of order 3, 2 and 1.

The only minor of order 3 is:

$$\begin{vmatrix} 1 & -1 & 2 \\ 3 & 1 & 0 \\ 2 & -2 & 5 \end{vmatrix} = 1(5-0) + 1(15-8) + 2(-6-2)$$
$$= 5 + 15 - 16 = 4 \neq 0$$

Hence, the rank of matrix A is 3.

Page No.:
Date : / /

1.7 System of Linear Equations

A system of linear equation is when we have two or more linear equations working together. In a system of linear equations, each equation corresponds with a straight line corresponds and one seeks out the point where the two lines intersect.

Example: Here are two linear equations:

$$2x + y = 5$$
$$-x + y = 2$$

Together they are a system of linear equations.

Date : / /

Solve the following system of linear equations:

① $x+y=6$
$-3x+y=2$

Soln:

$x+y=6$ -①
$-3x+y=2$ -②
$+\quad -\quad =$
$4x \quad =4$
$\therefore x=1$

Put $x=1$ in ①
$1+y=6$
$\therefore y=5$

$\therefore x=1, y=5$

② $2x+y-2z=3$ ①
$x-y-z=0$ -②
$x+y+3z=12$ -③

Soln:

The augmented matrix is:

$$\begin{bmatrix} 2 & 1 & -2 \\ 1 & -1 & -1 \\ 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 12 \end{bmatrix}$$

$R2 \to R2-R3$, we get

$$\begin{bmatrix} 2 & 1 & -2 \\ 0 & -2 & -4 \\ 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 \\ -12 \\ 12 \end{bmatrix}$$

Date : / /

$R_3 \to R_1 - 2R_3$

$$\begin{bmatrix} 2 & 1 & -2 \\ 0 & -2 & -4 \\ 0 & -1 & -8 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 \\ -12 \\ -21 \end{bmatrix}$$

$R_3 \to R_2 - 2R_3$

$$\begin{bmatrix} 2 & 1 & -2 \\ 0 & -2 & -4 \\ 0 & 0 & 12 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 \\ -12 \\ 30 \end{bmatrix}$$ (-12+42

Now,

$2x + y - 2z = 3$ — (4)

$-2y - 4z = -12$ — (5)

$12z = 30$ — (6)

from (6)

$12z = 30$

or, $z = \frac{30}{12} = \frac{5}{2}$

Put $z = 5/2$ in (5)

$-2y - \cancel{4} \times \frac{5}{\cancel{2}} = -12$

or $-2y - 10 = -12$

or $-2y = -2$

$\therefore y = 1$

Put x, y in (1)

$2x + 1 - \cancel{2} \times \frac{5}{\cancel{2}} = 3$

or $2x - 4 = 3$

Or, $2x = 7$

$\therefore x = 7/2$

$\therefore x = 7/2$, $y = 1$ and $z = 5/2$

3) Test the consistency and solve
$2x - 3y + 7z = 5$
$3x + y - 3z = 13$
$2x + 19y - 47z = 32$

Soln:

Writing above equations in matrix form:

$$\begin{bmatrix} 2 & -3 & 7 \\ 3 & 1 & -3 \\ 2 & 19 & -47 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 5 \\ 13 \\ 32 \end{bmatrix}$$

Where

$$A = \begin{bmatrix} 2 & -3 & 7 \\ 3 & 1 & -3 \\ 2 & 19 & -47 \end{bmatrix}, \quad X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad B = \begin{bmatrix} 5 \\ 13 \\ 32 \end{bmatrix}$$

Now, the augmented matrix is:

$$\left[\begin{array}{ccc|c} 2 & -3 & 7 & 5 \\ 3 & 1 & -3 & 13 \\ 2 & 19 & -47 & 32 \end{array}\right]$$

$R_1 : \frac{R_1}{2}$

$$\left[\begin{array}{ccc|c} 1 & -3/2 & 7/2 & 5/2 \\ 3 & 1 & -3 & 13 \\ 2 & 19 & -47 & 32 \end{array}\right]$$

$R_2 : R_2 - 3R_1$

$$\begin{bmatrix} 1 & -3/2 & 7/2 & : & 5/2 \\ 0 & 11/2 & 15/2 & : & \end{bmatrix} \quad \begin{bmatrix} 1 & -3/2 & 7/2 & : & 5/2 \\ 0 & 11/2 & -27/2 & : & 11/2 \\ 2 & 19 & -47 & : & 32 \end{bmatrix}$$

$R_3 : R_3 - 2R_1$

$$\begin{bmatrix} 1 & -3/2 & 7/2 & : & 5/2 \\ 0 & 11/2 & -27/2 & : & 11/2 \\ 0 & 22 & -54 & : & 27 \end{bmatrix}$$

$R_2 : R_2 \times \frac{2}{11}$

$$\begin{bmatrix} 1 & -3/2 & 7/2 & : & 5/2 \\ 0 & 1 & -27/11 & : & 1 \\ 0 & 22 & -54 & : & 27 \end{bmatrix}$$

$R_3 : R_3 - 22R_2$

$$\begin{bmatrix} 1 & -3/2 & 7/2 & : & 5/2 \\ 0 & 1 & -27/11 & : & 1 \\ 0 & 0 & 0 & : & 5 \end{bmatrix}$$

Here, $\rho(2) = 2$ and $\rho(A:B) = 3$

Since, $\rho(A) = 2$ and $\rho(AB) = 3$

We have $\rho(A) \neq \rho(Ac)$

The system is inconsistent.

Date : / /

Solve by matrix method

$x - 2y + 3z = 2$
$2x - 3z = 3$
$x + y + z = 0$

Soln:

Writing in matrix form;

$$\begin{bmatrix} 1 & -2 & 3 \\ 2 & 0 & -3 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix}$$

Where,

$$A = \begin{bmatrix} 1 & -2 & 3 \\ 2 & 0 & -3 \\ 1 & 1 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad B = \begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix}$$

$AX = B \quad \ldots (i)$

Now,

$$|A| = \begin{vmatrix} 1 & -2 & 3 \\ 2 & 0 & -3 \\ 1 & 1 & 1 \end{vmatrix} =$$

$$= 1\begin{vmatrix} 0 & -3 \\ 1 & 1 \end{vmatrix} - (-2)\begin{vmatrix} 2 & -3 \\ 1 & 1 \end{vmatrix} + 3\begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix}$$

$= 1(0+3) + 2(2+3) + 3(2+0)$

$= 3 + 10 + 6$

$= 19 (\neq 0)$

$\therefore$ The system has unique solution, so A^{-1} exist.

Page No.:
Date : / /

Matrix of Co-factor:

$A_{11} = \begin{vmatrix} 0 & -3 \\ 1 & 1 \end{vmatrix} = 0+3 = 3$

$A_{12} = -\begin{vmatrix} 2 & -3 \\ 1 & 1 \end{vmatrix} = -(2+3) = -5$

$A_{13} = \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix} = 2-0 = 2$

$A_{21} = -\begin{vmatrix} -2 & 3 \\ 1 & 1 \end{vmatrix} = -(-2-3) = 5$

$A_{22} = \begin{vmatrix} 1 & 3 \\ 1 & 1 \end{vmatrix} = 1-3 = -2$

$A_{23} = -\begin{vmatrix} 1 & -2 \\ 1 & 1 \end{vmatrix} = -(1+2) = -3$

$A_{31} = \begin{vmatrix} -2 & 3 \\ 0 & -3 \end{vmatrix} = 6-0 = 6$

$A_{32} = -\begin{vmatrix} 1 & 3 \\ 2 & -3 \end{vmatrix} = -(-3-6) = 9$

$A_{33} = \begin{vmatrix} 1 & -2 \\ 2 & 0 \end{vmatrix} = 0+4 = 4$

$\therefore \text{Adj of } A = \begin{bmatrix} 3 & -5 & 2 \\ 5 & -2 & 3 \\ 6 & 9 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 5 & 6 \\ -5 & -2 & 9 \\ 2 & 9 & 4 \end{bmatrix}$

Date : / /

Now,

$X = A^{-1} B$

or, $X = \frac{1}{|A|} \times \text{Adj } A \times B$

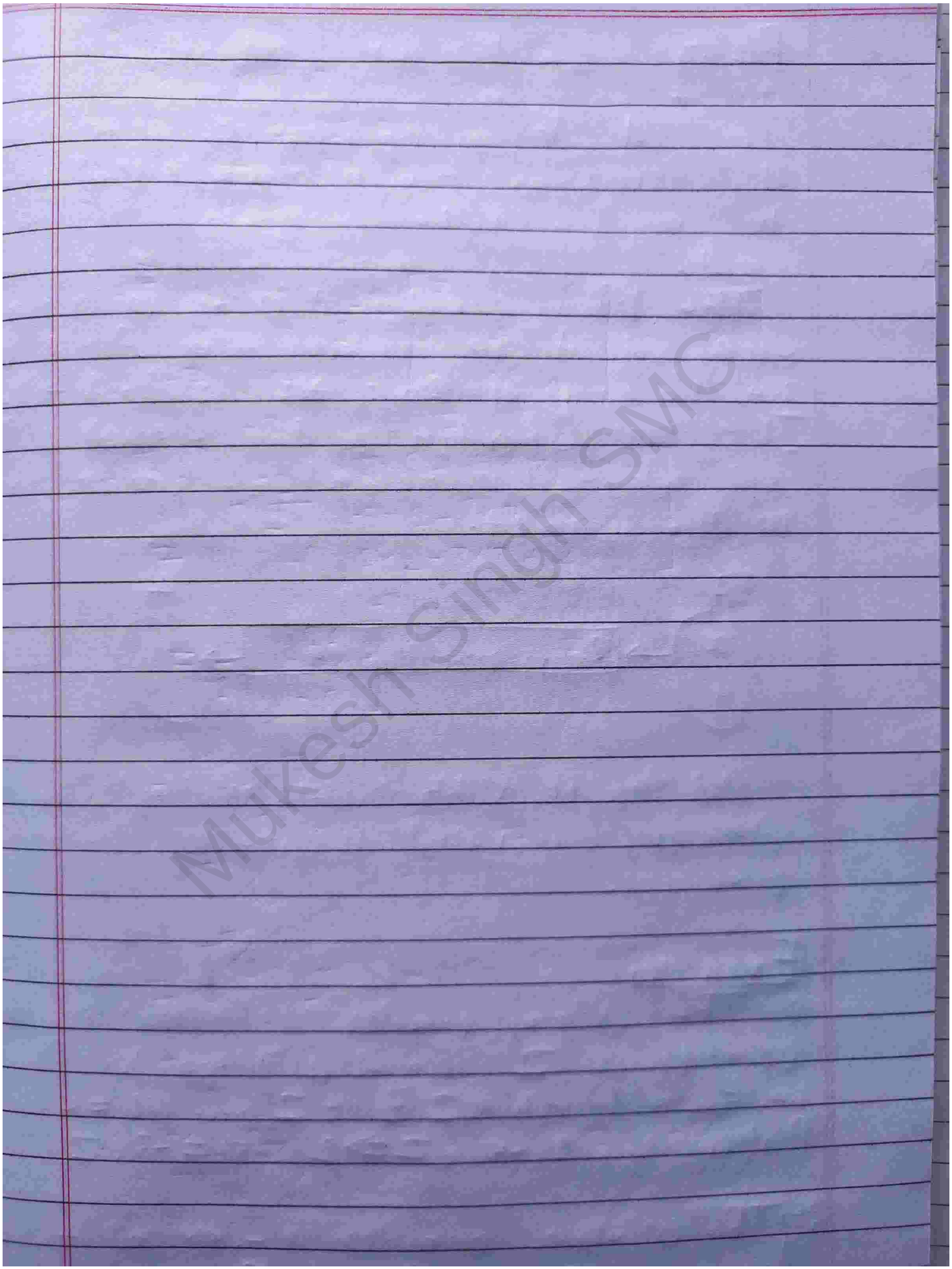
or, $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{19} \begin{bmatrix} 3 & 5 & 6 \\ -5 & -2 & 9 \\ 2 & 9 & 4 \end{bmatrix} \times \begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix}$

or, $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{19} \begin{bmatrix} 3\times2 + 5\times3 + 6\times0 \\ -5\times2 - 2\times3 + 9\times0 \\ 2\times2 - 3\times3 + 4\times0 \end{bmatrix}$

$= \frac{1}{19} \begin{bmatrix} 21 \\ -16 \\ -5 \end{bmatrix}$

$= \begin{bmatrix} 21/19 \\ -16/19 \\ -5/19 \end{bmatrix}$

$\therefore x = 21/19, y = -16/19, z = -5/19$



Unit-2

Group Theory

Page No.:
Date : / /

In modern algebra, group theory is the study of groups, which are systems consisting of a set of elements and a binary operation that can be applied to two elements of the set, which together satisfy certain axioms.

2.1 Algebraic system, Binary operation and its properties

An algebraic system is a mathematical system consisting of a set called the domain and one or more operations on the domain.

The non-empty set S together with a binary operation is called the algebraic system i.e. if * be the binary operation then we denote it by (S, *).

Examples

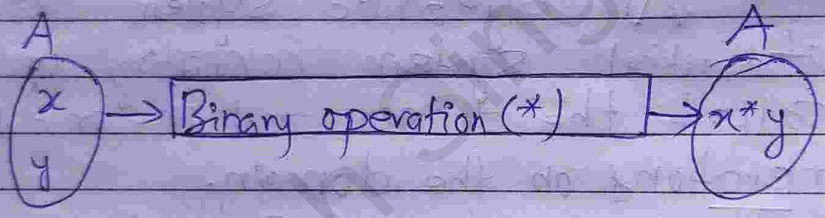
1. (ℕ, ×); ℕ is set of natural numbers.
2. (ℤ, −); ℤ is set of integer.
3. (ℕ, +), (ℚ, +), (ℝ, +), ℚ is set of rational number ℝ set of real numbers.

Page No.:
Date : / /

Binary operation on a set

A binary operation is a calculation that combines two elements (called operands) to produce another element of the same set.

The binary operation '*' (or '.') on a non-empty set A are functions from $A \times A$ to A.
i.e. the binary operation, $* : A \times A \to A$.
It is an operation of two elements of the set whose domains and co-domain are in the same set.



Addition (+), Subtraction (-), multiplication (*), division, exponential is some of the binary operations.

Examples

i) The ordinary operation '+' (addition) is a binary operation on Z (the set of integers).
i.e. for each $a, b, \in Z \; \exists \; c \in Z$ s.t. $a+b = c$.
Particularly, $2, -5 \in Z \Rightarrow 2+(-5) = -3 \in Z$

ii) The algebraic operation +, -, x and ÷ are binary operations on the set R - {0}.

Page No.:
Date : / /

Properties of Binary Operation

1. Closure Property

An operation * on a non-empty set A has closure property, if $a \in A, b \in A \Rightarrow a * b \in A$.

2. Commutative Property

A binary operation * on a set A is commutative if $a * b = b * a$, for all $(a, b) \in A$ (non-empty set). Let addition be the operating binary operation for $a = 8$ and $b = 9$, $a + b = 17 = b + a$.

3. Associative Property

The associative property of binary operations hold if, for a non-empty set A, we can write $(a * b) * c = a * (b * c)$.

Suppose N be the set of natural numbers and multiplication be the binary operation. Let $a = 4, b = 5, c = 6$. We can write $(a \times b) \times c = 120 = a \times (b \times c)$.

4. Distributive Property

Let * and o be the binary operations defined on a non-empty set A. The binary operations are distributive if $a * (b \circ c) = (a * b) \circ (a * c)$ or $(b \circ c) * a = (b * a) \circ (c * a)$.

Consider * to be multiplication and o be subtraction. And $a = 2, b = 5, c = 4$. Then

$a * (b \circ c) = a \times (b - c) = 2 \times (5 - 4) = 2$

And. $(a * b) \circ (a * c) = (a \times b) - (a \times c) = (2 \times 5) - (2 \times 4) = 4$

Page No.:
Date : / /

5. Identity Property

If A be the non-empty set and * be the binary operation on A. An element e is the identity element of $a \in A$, if $a*e = a = e*a$.

If the binary operation is addition (+), $e = 0$ and for * is multiplication (×), $e = 1$.

6. Inverse Property

If a binary operation * on a set A which satisfies $a*b = b*a = e$, for all $a, b \in A$. a^{-1} is invertible if for $a*b = b*a = e$, $a^{-1} = b$. 1 is invertible when * is multiplication.

2.2 Cayley's tables

Named after the 19th century British mathematician Arthur Cayley, a Cayley's table describes the structure of a finite group by arranging all the possible products of all the group's elements in a square table especially an addition or multiplication table. This is useful way to spot patterns, check for commutatively, identify inverse elements and so on. The table looks a bit like possibility spaces used to show the outcomes of two events in probability e.g. the sum of two dice scores.
For example:

Example 1: Let $G = \{1, \omega, \omega^2\}$
Its Cayley table is:

X	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Example 2: let $G = \{(1), (12), (13), (23), (123), (132)\}$
Its Cayley table is:

o	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(123)	(132)	(13)	(23)
(13)	(13)	(132)	(1)	(123)	(23)	(12)
(23)	(23)	(123)	(132)	(1)	(12)	(13)
(123)	(123)	(23)	(12)	(13)	(132)	(1)
(132)	(132)	(13)	(23)	(12)	(1)	(123)

Page No.:
Date : / /

2.3 Equivalence relation, Congruence modulo

Relation

A non-empty subset R of a Cartesian product A×B is called the relation from A to B. It is denoted by ARB or (a,b)∈R. The relation (a,b)∈R, the set of all first elements is called domain of R (denoted by Dom R) and the set of all second elements is called the range or image of R, denoted by Ran(R) or Im(R).

Equivalence Relation

A relation R is said to be equivalence if it satisfies the following properties:

(i) Reflexive: If for each $a \in A, \Rightarrow (a,a) \in R$ then the relation is reflexive relation.

(ii) Symmetric: If for any $(a,b) \in R \Rightarrow (b,a) \in R$ then R is said to be symmetric relation.

(iii) Transitive: If for any $(a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \in R$, then R is said to be transitive relation.

Equivalance definition:

A binary relation ~ on set S is said to be an equivalence if it is:-

Date : / /

(i) Reflexive for every $a \in S \Rightarrow a \sim a$
(ii) Symmetric for all $a, b \in S \Rightarrow a \sim b \Rightarrow b \sim a$.
(iii) Transitive for $a, b, c \in S \Rightarrow a \sim b$ and $b \sim c \Rightarrow a \sim c$.

Equivalence Class

Let R be an equivalence relation on a set S. Then for each $a \in S$ the equivalence class of a under relation R is denoted by $[a]$ and defined by $[a] = \{x : x \in S \text{ and } xRa\}$.

② Decomposition of a set into equivalence classes:

Ex ① Given set $S = \{1, 2, 3\}$
Eq. Relation, $R = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$
Find equivalent classes of $[1]$, $[2]$ and $[3]$.
Soln:
$[1] = \{1, 2\}$
$[2] = \{2, 1\}$
$[3] = \{3\}$

Eg ② Given set, $X = \{a, b, c, d, e\}$
Equivalence relation, $R = \{(a,a), (b,b), (c,c), (d,d), (e,e), (a,b), (b,a), (b,e), (e,b), (a,e), (e,a), (c,d), (d,c)\}$
Find equivalence classes of $[a], [b], [c], [d], [e]$.
Soln:
$[a] = \{a, b, e\}$
$[b] = \{b, a, e\}$
$[c] = \{c, d\}$
$[d] = \{d, c\}$
$[e] = \{e, b, a\}$

Congruence Modulo

Given any positive integer n and any integer 'a', if we divide a by n, we get an integer quotient 'q' and an integer remainder 'r' that obey the following relationship: $a = qn + r$ where $0 \leq r < n$ and $q = [a/n]$ where $[x]$ is the largest integer less than or equal to x.

For example, let $a = 11$, $n = 7$ then
$11 = 1 \times 7 + 4$ where $q = 1$, $r = 4$

If 'a' is an integer and 'n' is a positive integer, we define a mod n to be the remainder when a is divided by n. Thus, for any integer a, we can always write
$11 \pmod 7 = 4$

Two integer a and b are said to be congruent modulo n, if $a \bmod n = b \bmod n$. This can be written as: $a \equiv b \pmod n$
(i.e. remainder of b when divided by n)

For example,
$12 \equiv 5 \pmod 7$ because $12 = 1 \times 7 + 5$
and $5 = 0 \times 7 + 5$

Date : / /

Properties of modulo operator:

- Reflexivity: $a \equiv a \pmod n$
- Symmetry: $a \equiv b \pmod n$ if $b \equiv a \pmod n$ for all a, b and n.
- Transitivity: If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.

If $a_1 \equiv b_1 \pmod n$ and $a_2 \equiv b_2 \pmod n$, or if $a \equiv b \pmod n$ then:

- $a_1 + a_2 \equiv b_1 + b_2 \pmod n$ (Compatibility with addition)
- $a_1 - a_2 \equiv b_1 - b_2 \pmod n$ (Compatibility with subtraction)
- $a_1 a_2 \equiv b_1 b_2 \pmod n$ (Compatibility with multiplication).

Addition and Multiplication modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

X	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	3	4	3	2	1

(b) Multiplication modulo 8

Page No.:
Date: / /

2.4. Group and its properties

A non empty set G together with a binary operation $*$ is said to be a group $(G, *)$ or simply G, if it satisfies the following four properties/conditions:

(i) Closure: for ~~every~~ all $a, b \in G \Rightarrow a*b \in G$.

(ii) Associativity: For all $a, b \in G \Rightarrow (a*b)*c = a*(b*c)$.

(iii) Identity: For all $a \in G$, there exists the identity element e, such that: $a*e = e*a = a$.

(iv) Inverse: For every $a \in G$ there is an inverse element $a^{-1} \in G$ such that: $a*a^{-1} = a^{-1}*a = e$.
Where, e is an identity element and a^{-1} is called the inverse element of a in G.

Commutative: for all $a, b \in G \Rightarrow a*b = b*a$
It is also called abelian group.

By diagrams

	Satisfies
Groupoid/quasi group	→ prop i.
Semi group	→ prop i and ii.
Monoid	→ prop i, ii and iii
Group	→ prop i - iv
Abelian group	→ Prop i - iv and Commutative Property.

Some examples of groups:

Eg: 1) The set of real numbers with binary operation '+' forms a group i.e. $(\mathbb{R}, +)$ is a group.

for, (i) $a, b \in \mathbb{R} \Rightarrow a+b \in \mathbb{R}$, i.e. $2, 3 \in \mathbb{R} \Rightarrow 2+3 \in \mathbb{R}$
(ii) $2, 3, 5 \in \mathbb{R} \Rightarrow (2+3)+5 = 2+(3+5)$.
(iii) $0 \in \mathbb{R}$ acts as additive identity on $\mathbb{R}$.
(iv) for each $a \in \mathbb{R}$, $-a \in \mathbb{R}$ such that
$a+(-a) = -a+a = 0 \in \mathbb{R}$
Furthermore, $(\mathbb{R}, +)$ is satisfies commutative property.
Hence, $(\mathbb{R}, +)$ is an infinite abelian group.

2) $(\mathbb{Q}, +)$ is also abelian group.

3) $(\mathbb{N}, +)$ is not group, because 0 is (additive identity), $0 \in \mathbb{N}$.

4) $(W, +)$ has no inverse element, so $(W, +)$ is not group.

Properties of group:

1) In any group G, the identity element is unique.
2) If $a, b, c \in G$, then $a*c = b*c$ if $a = b$.
3) In any group G, for $a \in G$ a^{-1} is unique.
4) If $a, b \in G$ then $(a*b)^{-1} = b^{-1} * a^{-1}$.
5) If $a \in G$ then $(a^{-1})^{-1} = a$.

Page No.:
Date : / /

6) If every element of group G is its own inverse element prove that G is abdian group.

proof: Let $a, b \in G$ Since every element of G has its own inverse so, $a^{-1} = a$ and $b^{-1} = b$.

Since, $a, b \in G$, $a*b \in G$

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

$\Rightarrow b^{-1} * a^{-1} = a*b \quad (\because (a*b)^{-1} = b^{-1} * a^{-1})$

$\Rightarrow b*a = a*b \quad (\because b^{-1} = b, a^{-1} = a)$.

Hence, G is abelian group.

2.5 Integral Power of elements of a group

If n is a positive integer, we define $a^n = aaa\ldots$ a factor to n factor. Obviously $a^n \in G$ if n is the identity element of the group G, then we define $a^0 = e$.

If n is a positive integer then $-n$ is a negative integer. Now we define $a^{-n} = (a^n)^{-1}$ where $(a^n)^{-1}$ is the inverse of a^n in G. Thus, $a^{-n} \in G$. Thus we have defined a^n for all integral values of n positive, zero or negative.

Example 1

Let $G = \{1, -1, i, -i\}$

order of 1 is 1 $[\because (1)^1 = 1]$

order of -1 is 2 $[\because (-1)^2 = 1]$

order of $-i$ is 4 $[\because (-i)^4 = 1]$

order of i is 4 $[\because (i)^4 = 1]$

order = power

Example 2

$G = \{1, \omega, \omega^2\}$

order of $1 = 1$ $\quad 1^1 = 1$

order of $\omega = 3$ $\quad (\omega)^3 = 1$

order of $\omega^2 = 3$ $\quad (\omega^2)^3 = 1$

2.6 Cyclic groups and permutation groups

Cyclic group

A group G is called a cyclic group if, for some $a \in G$, every element $x \in G$, is of the form a^n, where n is some integer. The element 'a' is called generator of the cyclic group G denoted by $G = (a)$.

There may be more than one generator of a cyclic group if G is a cyclic group generated by a, then we shall write $G = \{a\}$ or $G = \langle a \rangle$. The elements of G will be of the form $\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots$. Of course they are not necessarily distinct.

Examples

Eg.1. The multiplicative group $G = \{1, -1\}$ is a cyclic group generated by -1.

Eg.2. The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic. We can write $G = \{i, i^2, i^3, i^4\}$. The generators are i and $-i$.
for, $i^1 = 1$, $i^2 = -1$, $i^3 = -i$ and $i^4 = 1$.

Eg.3. $(Z, +)$ is cyclic group generated by 1.

Eg.4. The group $(G, \times)$, $G = \{1, \omega, \omega^2\}$ is a cyclic group generated by ω and ω^2.

Date : / /

for.

×	1	ω	ω²
1	1	ω	ω²
ω	ω	ω²	1
ω²	ω²	1	ω

$(\omega)^1=\omega,\ \omega^2=\omega^2,\ \omega^3=1,\ \omega^4=\omega$

$(\omega^2)^1=\omega^2, (\omega^2)^2=\omega, (\omega^2)^3=1,$

$(\omega^2)^4=\omega^2$

Hence, $(G,\times)$ is cyclic group.

Eg.5.

$G=\{(1),(123),(132)\}$ is also cyclic group.

$(123)^1=123, (123)^2=132, (123)^3=(1)$

$(132)^1=132\ (132)^2=(123)\ (132)^3=(1)$

Here, (123) & (132) are generators

Permutation Groups:

A permutation group is a group G whose elements are permutations of a given set M and whose group operations is the composition of permutation in G (which are thought of as a bijective functions from set M to itself).

The group of all permutations of a set M is the symmetric group of M, often written as Sym(M). The term permutation group thus means subgroup of the symmetric group.

If $M=\{1,2\cdots n\}$ the Sym(M) is usually denoted by S_n. and may be called the symmetric group on n letters.

By Cayley's theorem, every group is isomorphic to some permutation group.

Date : / /

Examples

Example 1

Consider the following set G_1 of permutation and the set $M = \{1, 2, 3, 4\}$.

- $e = (1)(2)(3)(4) = (1)$

  This is the identity, the trivial permutation which fixes each element.

- $a = (12)(3)(4) = (12)$

  This permutation interchanges 1 and 2, and fixes 3 and 4.

- $b = (1)(2)(34) = (34)$

  Like the previous one, but exchanging 3 and 4, and fixing the others.

- $ab = (12)(34)$

  This permutation, which is the composition of the previous two, exchanges simultaneously 1 and 2, and 3 with 4.

G_1 forms a group, since $aa = bb = e$, $ba = aab$, and $abab = e$.

Example-2

Let $S = \{1, 2, 3\}$

No. of permutations on $S = 3! = 3 \times 2 \times 1 = 6$.

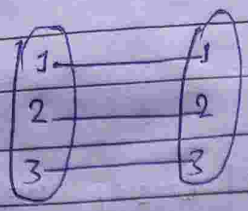
$f : S \to S$

1-1

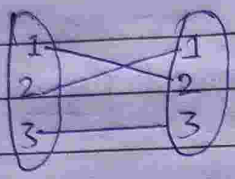
&

onto

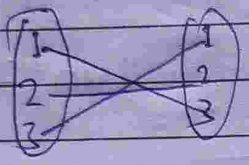
Date : / /



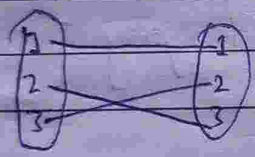
I i.e 1 (one to one) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$



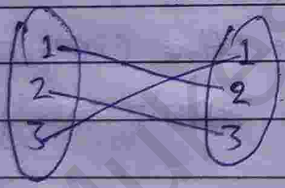
$\Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)$



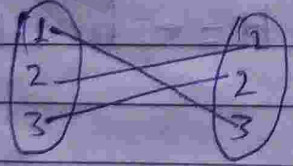
$\Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$



$\Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$



$\Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$



$\Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2)$

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

$\therefore S_3 = \{(1), (12), (13), (23), (123), (132)\}$

2.7 Elementary properties of groups, cyclic groups and permutation group

Elementary Properties of groups:

(i) If $a, b, c \in G$ and $ab = ac$ then $b = c$.
(left Cancellation law)

(ii) If $a, b, c \in G$ and $ba = ca$ then $b = c$
(right cancellation law

(iii) If $a \in G$ then $(a^{-1})^{-1} = a$. The inverse of the inverse of an element is the element itself.

(iv) If $a, b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$. That is the inverse of a product is the product of the inverse of the reverse order.

(v) If $a, b \in G$, then
$ab = e \Rightarrow a = b^{-1}$ and $b = a^{-1}$.

Elementary Properties of Cyclic groups

(i) Every cyclic group is abelian.
Let $G = [a]$ be a cyclic group and $x, y \in G$, where $x = a^r$ and $y = a^s$
Then, $xy = a^r \cdot a^s = a^{r+s} = a^{s+r}$
$= a^s \cdot a^r = yx$
$\therefore G$ is an abelian group.

(ii) If 'a' is a generator of a cyclic group G, then a^{-1} is also its generator.
i.e. If $G = [a] \Rightarrow G = [a^{-1}]$.

(iii) The order of a finite cyclic group is equal to the order of its generator.
i.e. O(finite cyclic group) = O(generator of group)

(iv) Every infinite cyclic group has two and only two generators

(v) The sub-group of every cyclic group is also cyclic.
i.e If $G = [a]$ be a cyclic group then H be a subgroup of G.
If $H = G$ or $H = \{e\}$ then clearly H is also cyclic.

(vi)
Elementary Properties of Permutation group

Date : / /

2.8 Subgroup and its properties

Subgroup:

A non-empty subset H of group G is a subgroup of G, if H itself forms a group under the same binary as that of G.

If H is a subgroup of G then, we write $H \leq G$.

If H is a proper subgroup then, we write $H < G$.

Examples

1) $(\mathbb{Z}, +)$ is a group of integers.
$E = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$ be set of even numbers.
Then $E \subset \mathbb{Z}$ and $(E, +)$ is also group.
Hence, $(E, +)$ is a subgroup of $(\mathbb{Z}, +)$ and we write $E \leq G$.

2) $A = \{\pm 1, \pm 3, \pm 7, \ldots\}$, $A \subset \mathbb{Z}$ but $(A, +)$ is not subgroup of $\mathbb{Z}$ because $1, 3, \in A$ but $1 + 3 = 4 \notin A$.

3) $G = \{1, -1, i, -i\}$ = fourth root of unity, $(G, \cdot)$ is a group and $H = \{1, -1\}$, H is subgroup of G under multiplication i.e. $H \leq G$.

4) $(\mathbb{R}, +)$ is a group and $(\mathbb{R}^+, \cdot)$ is also a group and $\mathbb{R}^+ \subset \mathbb{R}$ but $(\mathbb{R}^+, \cdot)$ is not subgroup of $(\mathbb{R}, +)$ since the binary operation is different.

5) $(\mathbb{R}-\{0\},\cdot)$ is a group. $(\mathbb{R}^+,\cdot)$ is a group of $(\mathbb{R}-\{0\},\cdot)$.

Q. Show that $H=\{1,-1\}$ is a sub-group of $G=\{1,-1,i,-i\}$ under multiplication.

Soln:

Let $G=\{1,-1,i,-i\}$ be a group and $H=\{1,-1\}$ be a is a subgroup of G. Then we have to show ~~that~~ H is a subgroup of G under multiplication i.e. $(H,\times)$ is a group.

Let

×	1	-1	i	-i
1	1	1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

From the above table, we have

The inverse of -1 is -1 and

The inverse of 1 is 1.

So,

For each $1,-1\in H$

We have, $-1\times -1=1\in H$ and $(-1)\times 1=(-1)=-1\in H$.

Hence $H\leq G$.

Page No.:
Date: / /

Properties of Subgroups:

Property 1: A non-empty subset H of group G is a subgroup of G iff and only if
i) $a, b \in H \Rightarrow a.b \in H$
ii) $a \in H \Rightarrow a^{-1} \in H$

Proof

Suppose H is a subgroup of $(G, .)$ then H itself is also a group with the same binary operation in G.
So $a, b \in H \Rightarrow a.b \in H$ (by closure)
and $a \in H \Rightarrow a^{-1} \in H$ (by inverse)

Conversely, Suppose H is a non-empty subset of G and (i) $a, b \in H \Rightarrow a.b \in H$ and (ii) $a \in H \Rightarrow a^{-1} \in H$. Then we have to show that H is a subgroup of G.
By Condition (i), we have $a, b \in H \Rightarrow a.b \in H$ (closure property satisfied).
It also satisfies associative property because H is subset of G.
Again by (ii) $a, a^{-1} \in H \Rightarrow a.a^{-1} \in H \Rightarrow a.a^{-1} = e \in H$ (Identity property also satisfied)
Again by condition (ii) $a \in H \Rightarrow a^{-1} \in H$ So, inverse property is also established.
Hence, H is subgroup of G.

By Shortcut method:

Proof:

The condition is necessary.

Let H is a subgroup then H satisfies closure axiom i.e.

$\forall a, b \in H \Rightarrow a.b \in H$

$\forall a \in H \Rightarrow a^{-1} \in H$ ($\because$ H is subgroup)

Condition is sufficient:

Let (i) and (ii) are given

1) Closure by (1)

2) Associative - it satisfies because H is subset of G.

3) Existence of inverse - by (2) Obviously.

4) Existence of identity

$\forall a, a^{-1} \in H \Rightarrow a.a^{-1} = e \in H$

Hence, H is subgroup of G.

2. Property 2 / Theorem 2:

A non-empty subset H of group G is a subgroup of G if and only if

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

Proof

Condition is necessary.

Let H is subgroup

$\forall b \in H \Rightarrow b^{-1} \in H$

So $\forall a.b^{-1} \in H \Rightarrow ab^{-1} \in H$

Condition is Sufficient:

Let $\forall a, b \in H \Rightarrow ab^{-1} \in H$ (given)

① Existence of identity: $\forall a \in H \Rightarrow a a^{-1} \in H \Rightarrow e \in H$

② Existence of inverse: $\forall e, a \in H \Rightarrow e a^{-1} = a^{-1} \in H$

③ Closure law: Since $\forall a \in H \Rightarrow a^{-1} \in H$
$\Rightarrow \forall a b^{-1} \Rightarrow a(b^{-1})^{-1} = ab \in H$

④ Associative: Since, H is subset of G, so it satisfies associative law.

Property 3/Theorem 3

The intersection of two subgroups of a group G is also a subgroup of G.

Proof:
Let H_1 and H_2 be two subgroups of a group G.
$\because e \in H_1, e \in H_2 \Rightarrow e \in H_1 \cap H_2 \Rightarrow H_1 \cap H_2 \neq \phi$

Now let $a, b \in H_1 \cap H_2$ then
$a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1$ and $a, b \in H_2$
$\Rightarrow ab^{-1} \in H_1$ and $ab^{-1} \in H_2$ [$\because H_1$ and H_2 are subgroups].

$\Rightarrow ab^{-1} \in H_1 \cap H_2$
$\therefore H_1 \cap H_2$ is a subgroup of G.

Page No.:
Date: / /

Generalization

If $H_1, H_2, \ldots, H_n$ be a finite family of subgroups of G; then $H_1 \cap H_2 \cap \ldots \cap H_n$ is also a subgroup of G.

Property 4 / Theorem 4

The Union of two subgroups is not necessarily a ~~group~~ sub-group.

Proof

Let O be the additive group of integers.

$O \rightarrow H_1, H_2$ (subgroups)

$H_1 = \{0, \pm 2, \pm 4, \ldots\}$

$H_2 = \{0, \pm 3, \pm 6, \ldots\}$

$H_1 \cup H_2 = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \ldots\}$

$2 + 3 = 5$ (Not in list)

$\therefore H_1 \cup H_2$ is not a sub-group.

Property 5 / Theorem 5

The union of two sub-groups is a subgroup if and only if one is contained in the other.

Proof

Part 1

Let $H_1 \subset H_2$ or $H_2 \subset H_1$

$H_1 \cup H_2 = H_2$ or H_1

H_1, H_2 are subgroups.

$\therefore H_1 \cup H_2$ is also a subgroup.

Part 2

Let $H_1 \cup H_2$ is a subgroup.

Let $H_1 \not\subseteq H_2$ or, $H_2 \not\subseteq H_1$.

$\swarrow$ $\searrow$

$s \in H_1$ & $s \notin H_2$ ① $t \in H_2$ & $t \notin H_1$ ②

① $s \in H_1 \cup H_2$

② $t \in H_1 \cup H_2$

$\therefore H_1 \cup H_2$ is a subgroup

2.9. Cosets of a Sub-group.

A subgroup H of a group G may be used to decompose the underlying set of G into disjoint equal size subsets called cosets. There are left cosets and right cosets. Cosets (both left & right) have the same number of elements (cardinality) as does H.

Mathematical definition:

Let H be a sub group of a group G and $a \in G$, then the set $aH = \{ah \mid h \in H\}$ is called a left coset of H in G. and $Ha = \{ha \mid h \in H\}$ is called a right coset of H in G.

It is clear that:

$aH \subset G, Ha \subset G \quad \forall a \in G.$

Further we may note that:

$eH = H = He$

Examples

Ex-1

Let $G = \{1, -1, i, -i\}$ and $H = \{1, -1\}$

then $H \leq G$, let $a = i \in G$.

Then $H * a = \{1, -1\} \circ i = \{i, -i\}$ is right coset of H in G.

$a.h = i\{1, -1\} = \{i, -i\}$ is a left coset of H in G.

Here, $aH = Ha$.

In general, $aH \neq Ha$.

Ex-2

Let $G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$ &

$H = \{(1), (12)\}$ & $a = (13) \in G$.

Date : / /

Now, $Hg = \{(1), (12)\}.(12) = \{(1), (13), (12), (23)\}$

$= \{(13), (123)\}$

$\because gH = (13)\{(1), (12)\}$

$= \{(13)(1), (13)(12)\}$

$= \{(1), (132)\}$

$\therefore gH \neq Hg.$

2.10 Lagrange's Theorem:

Lagrange theorem was given by Joseph-Louis Lagrange.

Lagrange theorem states that in group theory, for any infinite group say G, the order of subgroup H of group G divides the order of G. i.e. $O(G) / O(H)$.

The order of the group represents the number of elements.

Lagrange theorem Statement:

As per the statement, the order of the ~~group~~ subgroup H ~~of the~~ divides the order of the group G. This can be represented as: $|G| = |H|$.

Before proving Lagrange's theorem, let us discuss the important terminologies and ~~there~~ three lemmas that help to prove this theorem.

What is Coset?

→ When G is a finite group, and H is a subgroup of G, given that g is an element of G, then
$gH = \{gh : h$ is element of $H\}$ is the left coset with respect to element of G.
and
$Hg = \{hg : h$ is element of $H\}$ is the right coset of H in G with respect to the element of G.

Lemma 1: If G is a group with sub-group H, then there is a one to one correspondence between H

and any coset of H.

Lemma 2: If G is a group with subgroup H, then the left coset relation, $g_1 \sim g_2$ if and only if $g_1 * H = g_2 * H$ is an equivalence relation.

Lemma 3: Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B = \phi$, then $A = B$.

Proof of Lagrange theorem:
Let H be any subgroup of order n of a finite group G of order m. Let us consider the coset breakdown of G related to H.
Now let us consider each coset of aH comprises n different elements.
Let $H = \{h_1, h_2 \ldots h_n\}$ then $ah_1, ah_2, \ldots ah_n$ are the n distinct number of aH.

Suppose, $ah_i = ah_j \Rightarrow h_i = h_j$ be the cancellation law of G.
Since G is finite group, the number of discrete left coset also be finite, say p.
So, total number of elements of all cosets is np which is equal to total number of elements of G. Hence, $m = np$

$p = m/n$.

This shows that, n, the order of H, is a divisor of m, the order of the finite group G. We also see that the index p is also a divisor of the order of the group.

Date : / /

Hence, proved $|G| = |H|$.

Proof of Lagrange's theorem by another method:

To prove: If G is a finite group, $H \leq G$ then $o(H) / o(G)$; [$o(H)$ divides $o(G)$].

Proof

Suppose G be a finite group, H be a subgroup of G, let $o(G) = n$ and $o(H) = m$.

Consider all distinct right coset of H in G, say $Ha_1, Ha_2, \ldots Ha_k$.

These should be finite because G is finite.

We have, $G = Ha_1 \cup Ha_2 \cup Ha_3 \cup \ldots \cup Ha_k$.

Since distinct right cosets are disjoint.

So, $o(G) = o(Ha_1) + o(Ha_2) + o(Ha_3) + \ldots + o(Ha_k)$

$o(G) = o(H) + o(H) + o(H) + \ldots + o(H)$

i.e. $n = m + m + m + \ldots + m$

or, $n = mk$

$\Rightarrow \frac{n}{m} = k$

This show that m divides n.

i.e. $o(H)$ divides $o(G)$ i.e. $o(H) / o(G)$ proved.

Note: Here k means the number of distinct right coset of H in G and is called index of H in G.

Date : / /

Corollary 1: If G is a finite group of order n, $a \in G$ then $o(a) \mid o(G)$.

Proof
Suppose G is a finite group of order 'n'.
Let $a \in G$ and $o(a) = m$.
Consider, $\{G, a^2, a^3, \ldots, a^m = e\} = H$.
Then H is a group since $H \subset G$. So, $H \leq G$.
By Lagrange's theorem,
$o(H) \mid o(G)$

$\Rightarrow m \mid o(G)$ i.e. $o(a) \mid o(G)$.

Corollary 2: If G is a finite group of order n, then $a^n = e$.

Proof
Suppose G is a finite group of order n.
i.e. $o(G) = n$ let $a \in G$ and $o(a) = m$.
Then $a^m = e$.
By Corollary (1) $o(a) \mid o(G) = \frac{m}{n} \Rightarrow n = k^m$, for some $k \in Z$.
Now $a^n = a^{km} = (a^m)^k = e^k = e$.

Corollary 3: Every group of ~~primary~~ prime order is cyclic.

Proof
Let $G = \{e\}$ there is nothing to prove.
Suppose $a \in G$, $a \neq e$.
Consider $\{a, a^2, \ldots, a^m = e\} = H$
then H is a cyclic subgroup of a.

Date : / /

By Lagrange's theorem $o(H) \mid o(G)$

Since, $o(G)$ is a prime number and $o(H) \neq 1$, as $a \neq e$ and $o(H) \mid o(G)$.

So, $o(H) = o(G)$.

Since, H is a subgroup of a having same order of G.

So, $H = G$.

Hence, G is a cyclic group.

2.11 Normal Subgroups

A subgroup N of group G is known as normal subgroup of G if every left coset of N in G is equal to the corresponding right coset of N in G. That is $gN = Ng$ for every $g \in G$.

Mathematical definition:

Let G be a group and N be a subgroup of G. Then N is said to be normal sub-group of g if $gng^{-1} \in N \ \forall n \in N, g \in G$.

i.e. if $gNg^{-1} = \{gng^{-1} : n \in N, g \in G\}$ Then N is normal sub-group of G.

It is written as $N \trianglelefteq G$. or $N \triangleleft G$.

OR, if $gNg^{-1} \subset N \ \forall g \in G$, then $N \trianglelefteq G$.

Example:

$N = [\{1, -1\}, g]$ is a normal subgroup of $G = [\{1, -1, i, -i\}, g]$ because for every $g \in G$ and $n \in N$

$gng^{-1} = gg^{-1}n = en = n \in N$. [$\because G$ is commutative]

Page No.:
Date : / /

Properties of Normal Subgroups:

Property 1 / Theorem 1

A subgroup N of a group G is normal subgroup of G iff $gNg^{-1} = N$.

Proof

Suppose N is a normal subgroup of G then we have to show $gNg^{-1} = N$.

Since N is normal subgroup of G, so by definition

$gNg^{-1} \subset N \quad \forall g \in G \quad \ldots$ (i)

Since $g \in G \Rightarrow g^{-1} \in G$

$\therefore g^{-1} N (g^{-1})^{-1} \subset N$

$\Rightarrow g^{-1} N g \subset N$

$\Rightarrow g(g^{-1} N g) g^{-1} \subset gNg^{-1}$

$\Rightarrow (gg^{-1}) N (gg^{-1}) \subset gNg^{-1}$

$\Rightarrow N \subset gNg^{-1} \quad \ldots$ (ii)

from (i) and (ii) $gNg^{-1} = N$

Conversely, suppose $gNg^{-1} = N \quad \forall g \in G$

obviously $gNg^{-1} \subset N \quad \forall g \in G$

$\therefore N$ is normal subgroup of G i.e. $N \trianglelefteq G$.

Property 2 / Theorem 2

A subgroup N of G is normal iff every right coset of N in G is equal to the every left coset of N in G.

i.e. $N \trianglelefteq G$ iff $Ng = gN \quad \forall g \in G$)

Proof

Suppose N is a normal subgroup of G then $gNg^{-1} = N$.

$\Rightarrow (gNg^{-1}) g = Ng \quad \forall g \in G$

$\Rightarrow gNg^{-1}g = Ng \quad \forall g \in G.$
$\Rightarrow gN = Ng \quad \forall g \in G. \quad [\because g^{-1}g = e = 1]$

Conversely suppose $Ng = gN \quad \forall g \in G.$
$\Rightarrow Ngg^{-1} = gNg^{-1} \quad \forall g \in G$
$\Rightarrow N = gNg^{-1} \quad \forall g \in G$
i.e. $gNg^{-1} \in N \quad \forall g \in G.$
So, N is normal subgroup of G.

Property 3 / Theorem 3
Every subgroups of abelian group is normal.

Proof
Let G be an abelian group and H be a subgroup of G. Let $g \in G$ and $h \in H$. Then
$ghg^{-1} = gg^{-1}h \quad (\because G \text{ is abelian})$
$= eh = h \in H$
$\therefore ghg^{-1} \in H$ for $g \in G$ and $h \in H$
$\therefore H$ is a normal subgroup of G.

Property 4 / Theorem 4.
The intersection of two normal subgroups of G is also a normal subgroup of G. (TU 2063)

Proof
Let H and K be two normal subgroups of G. We have to show $H \cap K$ is also normal subgroup of G. Since H and K are subgroups of G.
So, $H \cap K$ is also subgroup of G.
Let $g \in G$ and $n \in H \cap K$, then $n \in H$ and $n \in K$.
Since H is a normal subgroup of G. So, $g \in G, n \in H \cap K$, then $n \in H$ and $n \in K$.

Page No.:
Date : / /

Since H is a normal subgroup of G. So,
$g \in G, n \in H \Rightarrow gng^{-1} \in H$.
Also K is normal subgroup of G. So,
$g \in G, n \in K \Rightarrow gng^{-1} \in K$.
$\therefore gng^{-1} \in H \cap K \quad \forall g \in G, n \in H \cap K$.
Hence, $H \cap K$ is normal subgroup of G.

Date : / /

2.12 Quotient Group (or factor Group)

A quotient group or factor group is a mathematical group obtained by aggregating similar elements of a larger group using an equivalent relation that preserves some of the group structure.

Mathematical definition:

Let N be a normal subgroup of G. Then it can be verified that the cosets of G relative to N form a group. This group is called the quotient group or factor group of G relative to N and denoted by G/N.

Example

Find the quotient group G/N and also prepare its operation table, when $G = [\{1, -1, i, -i\}, \times]$, $N = [\{1, -1\}, \times]$.

Soln:

Since G is a commutative group, therefore $N \triangleleft G$.

Consequently, G/N exist having following cosets of N:

$N_1 = \{1.1, -1.1\} = \{1, -1\} = N$

$N(-1) = \{1.(-1), -1.(-1)\} = \{-1, 1\} = N$

$N.i = \{1.i, -1.i\} = \{i, -i\} = Ni$

$N(-i) = \{1.(-i), -1.(-i)\} = \{-i, i\} = Ni$

Thus, we see that $G/N = \{N, Ni\}$

Page No.:
Date : / /

Composition table of G/H is as follows:

	N	Ni
N	N	Ni
Ni	Ni	N

Properties / Theorems of Quotient group:

Theorem 1:

Show If N is a normal subgroup of a finite group G, then prove that $o(G/H) = \frac{o(G)}{o(H)}$

Soln:

$o(G/H)$ = number of distinct right (or left) cosets of H in G, as G/N is the collection of all right (or left) cosets of H in G.

$= \frac{\text{number of distinct elements in } G}{\text{number of distinct elements in } H}$

$= \frac{o(G)}{o(H)}$

by Lagrange's theorem.

Theorem 2

Show that every quotient group of a cyclic group is cyclic, but not conversely.

Soln

Let N be a subgroup of cyclic group G. Then N is cyclic because every cyclic group is abelian. Therefore N is a normal subgroup of G.

Let a be a generator of G and a^k be any element of G, where k is an integer. Then Na^k

is any element of G/N.

Also it can be easily proved that $(Na)^k = Na^k$ for every integer k. Therefore G/N is cyclic and its generator is Na.

Its converse is not true; for example if S_3 and A_3 are symmetric and alternating groups of the three symbols a, b, c then the quotient group S_3/A_3 is cyclic, where S_3 is not.

Unit-3

Group Homomorphism

Page No.:
Date : / /

3.1 Homomorphism, Endomorphism, Automorphism and Isomorphism

A. Homomorphism

Let $(G, \cdot)$ and $(G', *)$ be two groups, then a mapping $\phi: G \to G'$ is said to be homomorphism if,

$\phi(x \cdot y) = \phi(x) * \phi(y) \quad \forall x, y \in G$.

i.e. $\phi: G \to G'$ is such that $\forall x, y \in G$, $x \mapsto \phi(x)$, $y \mapsto \phi(y)$

$x \cdot y \longmapsto \phi(x \cdot y) = \phi(x) * \phi(y)$.

Examples

Eg-1. Let $G = G'$ and $\phi: G \to G'$ is defined by $\phi(x) = e \; \forall x \in G$, then show that ϕ is homomorphism.

Soln:

Let $x, y \in G$ then $x \cdot y \in G$.

Now $\phi(x \cdot y) = e$.

Again, $\phi(x) \cdot \phi(y) = e \cdot e = e$

Hence, $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$

So, ϕ is a homomorphism.

Eg-2. Show that the mapping $\phi: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by $\phi(x) = 2x \; \forall x \in \mathbb{Z}$ is a homomorphism.

Soln:

Let $x, y \in \mathbb{Z}$ then $x + y \in \mathbb{Z}$

$\phi(x+y) = 2(x+y)$

Again, $\phi(x) + \phi(y) = 2x + 2y = 2(x+y)$

$\therefore \phi(x+y) = \phi(x) + \phi(y)$

So, ϕ is a homomorphism.

Eg-3. The mapping $\phi : (Z, +) \to (Z, +)$ defined by $\phi(x) = 2x + 3 \ \forall \ x \in Z$ is not homomorphism.

Proof

Let $x, y \in Z$ then $x + y \in Z$.

Now, $\phi(x+y) = 2(x+y) + 3 = 2x + 2y + 3$

$\phi(x) + \phi(y) = 2x + 3 + 2y + 3 = 2x + 2y + 6$

$\therefore \phi(x+y) \neq \phi(x) + \phi(y)$.

So, ϕ is not homomorphism.

Basic Properties of Homorphism.

Let $\phi : G \to G'$ be group homorphism e and e' be identity element of G and G' respectively. Let g be an element of G. Then prove the following properties:

(i) $\phi(e) = e'$

(ii) $\phi(x^{-1}) = [\phi(x)]^{-1}$

(iii) $\phi(xy^{-1}) = \phi(x)[\phi(y)]^{-1}$

(iv) $\phi(g^n) = [\phi(g)]^n$

(v) if $|g| = n$, then $|\phi(g)| = n$

(vi) if $\phi(g) = g'$, then $\phi^{-1}(g) = \{g \in G \mid \phi(g) = g'\} = g \ker \phi$

(i) $\phi(e) = e'$

Proof

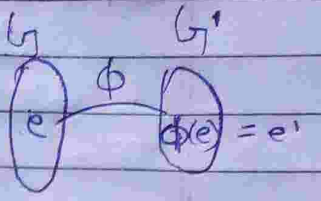
For any $x \in G$, we have

$x \cdot e = x \Rightarrow \phi(x \cdot e) = \phi(x)$

$\Rightarrow \phi(x) \cdot \phi(e) = \phi(x)$

$\Rightarrow \phi(x) \cdot \phi(e) = \phi(x) \cdot e'$

$\therefore \phi(e) = e'$ [By left cancellation law].



(ii) $\phi(x^{-1}) = [\phi(x)]^{-1}$

Proof

We have, for any $x \in G$,

$x \cdot x^{-1} = e = x^{-1} \cdot x$

$\Rightarrow \phi(x \cdot x^{-1}) = \phi(e) = \phi(x^{-1} \cdot x)$

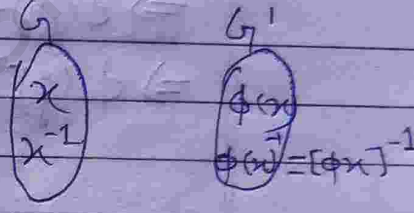
$\Rightarrow \phi(x) \cdot \phi(x^{-1}) = e' = \phi(x^{-1}) \cdot \phi(x)$ ($\because \phi$ is homomorphism)

$\Rightarrow \phi(x) \cdot \phi(x^{-1}) = e'$

Hence $\phi(x^{-1})$ is the inverse of $\phi(x)$

$\Rightarrow [\phi(x)]^{-1} = \phi(x^{-1})$

$\therefore \phi(x^{-1}) = [\phi(x)]^{-1}$ proved.



(iii) $\phi(xy^{-1}) = \phi(x)[\phi y]^{-1}$

Proof

$\phi(xy^{-1}) = \phi(x) \cdot \phi(y^{-1})$ [by homomorphism]

$\Rightarrow \phi(xy^{-1}) = \phi(x)[\phi(y)]^{-1}$ [By property 2].

(iv) $\phi(g^n) = [\phi(g)]^n$

Proof

We use induction on n.

If $n=1$ then obviously $\phi(g^{-1}) = \phi(g)$

Suppose the statement is true for $n \geq 1$.

and less than n, then

$\phi(g^n) = \phi(g \cdot g^{n-1})$

$= \phi(g) \cdot g\phi(g^{n-1})$

$= \phi(g) \cdot [\phi(g)]^{n-1}$ (by induction)

$= (\phi(g))^n$

If $n = -r$ with $r > 0$

Since, $g^n \cdot g^r = e_G$

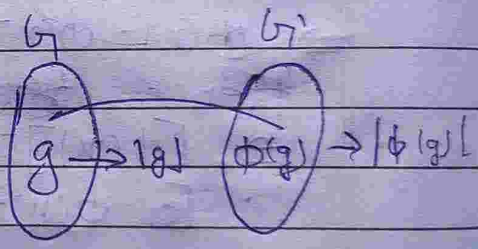
We get,

$\phi(g^n) \cdot \phi(g^r) = \phi(e_G) = e_H$

$\Rightarrow \phi(g^n) = [\phi(g^r)]^{-1}$

$\Rightarrow \phi(g)^{-r} = \phi(g^n)$ proved.

(v) If $|g| = n$, then $|\phi(g)| = n$



Since, $|g| = n \Rightarrow g^n = e$

Now,

$[\phi(g)]^n = \phi(g^n)$

$= \phi(e) = e'$

[By property (i)]

$\Rightarrow |\phi(g)| \mid n$

$\Rightarrow |\phi(g)| = n$.

(vi) If $\phi(g) = g'$, then $\phi^{-1}(g) = \{g \in G \mid \phi(g) = g'\} = g \ker \phi$

Proof

Let $x \in \phi^{-1}(g')$

$\Rightarrow \phi(x) = g^{-1}$

$\Rightarrow \phi(x) = \phi(g)$ [By statement]

$\Rightarrow \phi(g^{-1})\phi(x) = \phi(g^{-1})\phi(g)$ [multiplying both sides by $\phi(g^{-1})$]

$\Rightarrow \phi(g^{-1}x) = \phi(g^{-1}g)$ [ϕ is homomorphism]

$\Rightarrow \phi(g^{-1}x) = \phi(e)$ [$\because g^{-1}g = e$]

$\Rightarrow \phi(g^{-1}x) = e'$ (By property 1)

$\Rightarrow g^{-1}x \in \ker\phi$

$\Rightarrow x \in g \ker\phi$

$\Rightarrow \phi^{-1}(g') \subseteq g\ker\phi$ - (1)

Conversely

Let $z \in g\ker\phi$

$z = gu$ where, $u \in \ker\phi$

We have to prove that

$z \in \phi^{-1}(g')$

Now, $\phi(z) = \phi(gu)$

$= \phi(g).\phi(u)$ [$\because \phi$ is homomorphism]

$= \phi(g).e'$ [$\because u \in \ker$]

$= \phi(g) = g'$

$\therefore \phi(z) = g'$

$z \in \phi^{-1}(g')$

$\Rightarrow g\ker\phi \subseteq \phi^{-1}(g')$ - (2)

From eqn (1) & (2)

$\phi^{-1}(g') = g\ker\phi$ Hence proved.

Date : / /

Kernel of Homomorphism:

Let $\phi : G \to G'$, e and e' be the identity element of G and G' respectively. Then kernel of ϕ is the set of all elements $x \in G$ such that $\phi(x) = e'$. It is denoted by $\ker\phi$ or $K\phi$.

Image of homomorphism:

Let $\phi : G \to G'$ be a group ~~homo~~ homomorphism. Then the set $\phi(G) = \{\phi(x) : x \in G\}$ is called the image of a homomorphism ϕ.

#B) Endomorphism

An endomorphism is a linear mapping ϕ of a linear space V into itself, where V is assumed to be over the field of numbers F. An endomorphism that is also an isomorphism is an automorphism. For example an endomorphism of a vector space V is a linear map $\phi: V \to V$ and an endomorphism of a group G is a group homomorphism $\phi: G \to G$.

In general, we can talk about endomorphism in any category. In the category of sets, endomorphisms are functions from a set S to itself.

In any category, the composition of any two endomorphism of X is again endomorphism of X.

A mapping ϕ is linear if

$$\phi(c_1 v_1 + c_2 v_2) = c_1 \phi(v_1) + c_2 \phi(v_2)$$

for any c_1, c_2 in F and v_1, v_2 in V.

c) Automorphism

An isomorphic mapping of a group G onto G itself is called an automorphism of G.

It is denoted by A_G or $Aut(G)$.

A mapping $\phi: G \to G$ is called automorphism of G if:

(i) ϕ is a bijection

and (ii) $\phi(ab) = \phi(a).\phi(b) \quad \forall a, b \in G$.

Examples

1) The identity mapping I_G is an automorphism on G because I_G is a bijection and $I_G(ab) = ab = I_G(a).I_G(b) \quad \forall a, b \in G$.

2) The mapping of $\phi: (C,+) \to (C,+)$, $\phi(z) = \bar{z} \quad \forall z \in C$ is an automorphism on C because for any $z_1, z_2 \in C$

$\phi(z_1) = \phi(z_2) \Rightarrow \bar{z_1} = \bar{z_2} \Rightarrow z_1 = z_2$.

$\therefore f$ is one-to-one.

and for every $z \in C$ there exists $\bar{z} \in C$ such that $\phi(\bar{z}) = \overline{(\bar{z})} = z$.

$\therefore f$ is onto.

Again,

$\phi(z_1 + z_2) = \overline{z_1 + z_2} = \bar{z_1} + \bar{z_2} = f(z_1) + f(z_2)$

Therefore ϕ is an isomorphism on the group C.

i.e. It is an automorphism on group C.

Date : / /

D) Isomorphism

Isomorphism is a one-to-one correspondence (mapping) between two sets that preserves the binary relationship between the elements of the sets. For example, a set of natural numbers can be mapped onto the set of even natural numbers by multiplying each natural number by 2.

Mathematical definition:

Let $\phi: G \to G'$ be group homomorphism. Then ϕ is said to be isomorphism if:

(i) ϕ is one-to-one i.e. $\phi(a) = \phi(b) \Rightarrow a = b \quad \forall a, b \in b$.

(ii) ϕ is onto i.e. $\phi(G) = G'$

and (iii) ϕ is morphism i.e. $\phi(a.b) = \phi(a) \circ \phi(b), \forall a, b \in b$.

From the above definition, it is clear that a group morphism is an isomorphism if ϕ is a bijection.

Isomorphic groups:

If ϕ is an isomorphism from G onto G' then G and G' are called isomorphic groups and we write symbolically, $G \cong G'$.

Note

A homomorphism $\phi: G \to G'$ is

(i) an epimorphism if ϕ is onto.

(ii) a monomorphism if ϕ is one-to-one.

(iii) an isomorphism if it is one to one and onto.

Example

For every group G, the identity mapping I_G defined by: $I_G: G \to G$, $I_G(x) = x, \forall x \in G$

is an isomorphism of G_1 onto itself, because I_{G_1} is clearly one-to-one, onto and $a, b \in G_1$.

$I_2(ab) = ab = I_{G_1}(a) \cdot I_{G_1}(b)$.

Page No.:
Date : / /

3.2 Isomorphism theorems : fundamental theorem, diamond and quotient isomorphism theorems, Correspondence theorem.

1) Fundamental theorem (1st isomorphism theorem)

Let ϕ be a group homomorphism ~~from~~ from G onto H with $\ker \phi = K$. Then the mapping from G/K to $\phi(G)$ given by $Ka \to \phi(a)$ is an isomorphism.

i.e. $\frac{G}{\ker \phi} \approx \phi(G)$.

Proof

Let $\psi : \frac{G}{K} \to \phi(G)$ by $\psi(Ka) = \phi(a)$

We have to show:

(i) ψ is well defined and 1-1.

(ii) ψ is onto ~~and~~ homomorphism.

(i) ψ is well defined and 1-1.

Let, $\psi(Ka) = \psi(Kb)$

$\Leftrightarrow \phi(a) = \phi(b)$

$\Leftrightarrow \phi(a)[\phi(b)]^{-1} = \phi(b)[\phi(b)]^{-1}$

$\Leftrightarrow \phi(a)\phi(b^{-1}) = e_H$ [e_H = identity of H]

$\Leftrightarrow \phi(ab^{-1}) = e_H$

$\Leftrightarrow ab^{-1} \in \ker \phi = K$ i.e. $ab^{-1} \in K$ i.e. $a \in Kb$

$\Leftrightarrow Ka = Kb$

$\therefore \psi$ is 1-1 & well defined.

(ii) ψ is onto & homomorphism

Let $Ka, Kb \in \frac{G}{K}$ then

Now, $\psi(Ka, Kb) = \psi(Kab)$

$= \phi(ab)$

$= \phi(a) \cdot \phi(b)$

$= \psi(Ka) \cdot \psi(Kb)$

(ψ is homomorphism)

~~And for each $\phi(a) \in \phi(G)$~~

And,

Let $b \in \phi(G)$ then $\exists\ a \in G$ such that $\phi(a) = b$ [$\because b \in \phi(G)$]

i.e. $\psi(Ka) = b \cdot \phi(a) = b$

i.e $\psi(Ka) = b$. (ψ is onto).

So,

So, ψ is onto homomorphism.

So from (I) & (II)

$\frac{G}{K} = \frac{G}{\ker\phi} \cong \phi(G)$.

Page No.:
Date : / /

2) Diamond Theorem or 2nd Isomorphism Theorem

If A is a normal subgroup of G and B is a subgroup of G then,

$$\frac{AB}{A} \cong \frac{B}{A \cap B}.$$

Proof

Let $A \trianglelefteq G$ and $B \leq G \Rightarrow AB \leq G$ and $A \cap B \trianglelefteq B$.

Let $\phi : B \to \frac{AB}{A}$ by $\phi(b) = A_{ab} = A_b$ (at least one identity)

Then, we have to show:

i) ϕ is well defined & 1-1

ii) ϕ is onto homomorphism.

iii) $\ker \phi = A \cap B$.

i)

Let, $a, b \in B$ and if $a = b$ then,

$\phi(a) = A_{ab} = A_a$

$\Leftrightarrow \phi(a) = A_b \quad [\because a = b]$

$\Leftrightarrow \phi(a) = \phi(b)$ $\therefore \phi$ is well defined & 1-1.

ii)

Let, $a, b \in B$

If $\phi(ab) = A_{ab}$

$= A_a . A_b \quad [\because$ quotient group$]$

$= \phi(a)\,\phi(b)$

And for each,
$A_{ab} = A_b \in \frac{AB}{A} \quad \exists\ b \in B$

Such that,
$\phi(b) = A_b$ [from 1st isomorphism theorem $B \simeq \frac{AB}{A}$]

$\therefore \phi$ is onto homomorphism

(ii) $\ker \phi = A \cap B$

Since,
$\phi : B \to \frac{AB}{A}$ then by definition of kernel

$\ker \phi = \{ b \in B : \phi(b) = A \}$
$= \{ b \in B : A_b = A \}$
$= \{ b \in B : b \in A \}$
$= A \cap B$

Hence, $\frac{B}{A \cap B} \simeq \frac{AB}{A}$

i.e. $\frac{AB}{A} \simeq \frac{B}{A \cap B}$ proved.

Page No.:
Date: / /

3) ~~3rd~~ Third isomorphism theorem / Quotient Theorem.

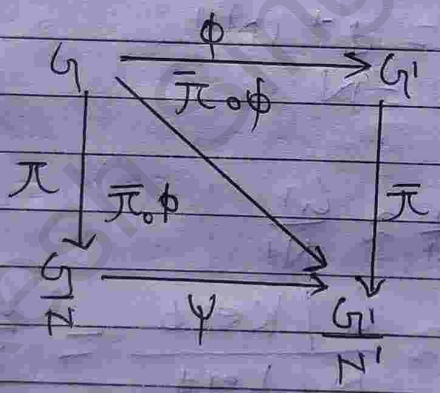
Let G be a group and let H & K ~~are~~ be normal subgroups of G with $H \leq K$ then

$$\left(\frac{G/H}{K/H}\right) = \left(\frac{G}{K}\right)$$

OR

Let ϕ be a homomorphism G onto G' with Kernel K and $N' \Delta G'$ and $N = \phi^{-1}(N') = \{x \in G : \phi(x) \in N'\}$ then $\frac{G}{N}$ is isomorphic to $\frac{G'}{N'}$

i.e. $\frac{G}{N} \cong \frac{G/K}{N/K}$.



Proof

Let $\phi : G \to G'$ be an onto homomorphism.

So, $G' \cong \frac{G}{K} \Rightarrow G' = \frac{G}{K}$

Define.

$\pi' : G' \to \frac{G'}{N'}$ is also ~~an~~ onto homomorphism.

Then, the composition $\pi' \cdot \phi$ is also an onto homomorphism.

From G to $\frac{G'}{N}$

Date : / /

i.e. $\pi' \cdot \phi : G \to \frac{G'}{N}$

So, by 1st Isomorphism theorem,

$$\frac{G}{\ker\phi} \simeq \frac{G'}{N}$$

Now,

$\ker(\pi' \cdot \phi) = N$

$\therefore N \triangle G$

So,

$$\begin{aligned}\ker(\pi' \cdot \phi) &= \{x \in G : \pi' \cdot \phi(x) = N'\} \\ &= \{x \in G : \pi'(\phi x) = N'\} \\ &= \{x \in G : N'\phi(x) = N'\} \\ &= \{x \in G : \phi(x) \in N'\} \quad [\because Hh = H \Rightarrow h \in H] \\ &= \phi^{-1}(N') \\ &= N\end{aligned}$$

Hence $\frac{G}{N} \simeq \frac{G'}{N'}$

$\therefore$ i.e. $\frac{G}{N} \simeq \frac{G/\ker\phi}{N/\ker\phi} = \frac{G/k}{N/k}$ proved.

4) Fourth Isomorphism theorem / Correspondence theorem.

Let $\phi: G \to G'$ be an epimorphism of groups with Kernel K. Then there is a one-one correspondence between the subgroups of G which contains Kernel K and the set of all subgroups of G'. Under this correspondence normal subgroup corresponds to normal subgroup.

Proof:

Let $\psi: C(G) \to C(G')$

Where,

$C(G)$ is family of sub-group of G containing $\ker \phi = K$ and $C(G')$ is the family of subgroup and G' by. $\psi(H) = \phi(H)$.

We show

(i) ψ is well defined & 1-1.

(ii) ψ is onto homomorphism

(iii) $\cdots \Delta G \to \cdots \Delta G'$

(i)

Let $\psi(H_1) = \psi(H_2)$

$\Leftrightarrow \phi(H_1) = \phi(H_2)$

$\Leftrightarrow \phi^{-1}(\phi(H_1)) = \phi^{-1}(\phi(H_2))$

$\Leftrightarrow H_1 = H_2$.

ii) for each $H' \leq G' \exists \phi^{-1}(H') \in C(G)$ such that.

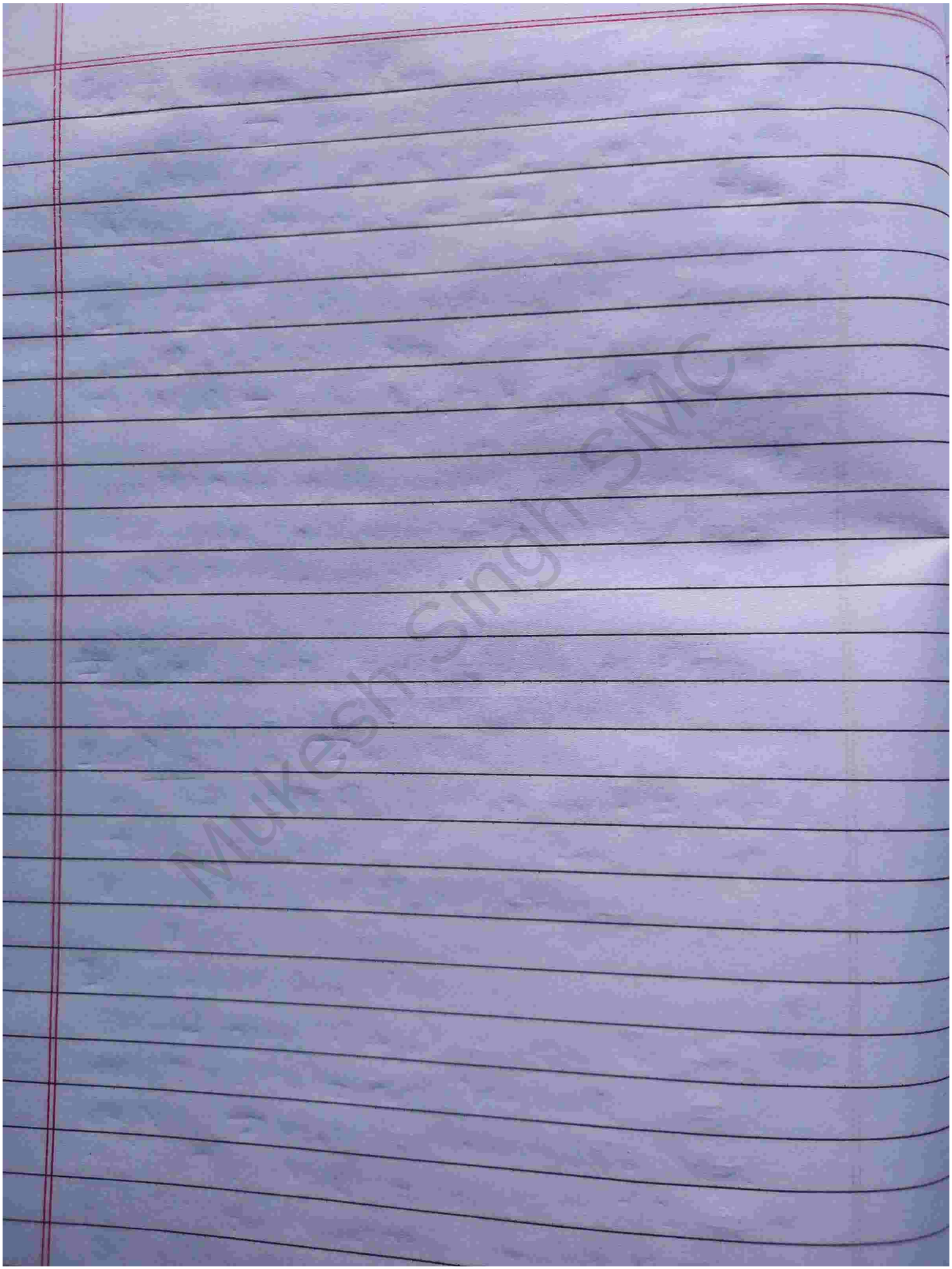
$\phi^{-1}(H') \leq G$.

then, $\phi(\phi^{-1}(H')) = H'$

Page No.:
Date : / /

(P.T.O.)
vii) If $H \in c(G)$
i.e. $H \trianglelefteq G \Rightarrow \phi(H) \trianglelefteq G$

Hence, ... $\trianglelefteq G \to \cdots \trianglelefteq G$.


Mukesh Singh SMC

Unit-4
Ring Theory

Page No.:
Date: / /

4.1 Definition of Rings and its special classes with examples

Definition of a Ring:

Let R be a non-empty set, '+' and '·' be two binary operations on R; (addition and multiplication). Then R is said to be a ring if R with this '+' and '·' if it satisfies the following properties:

1. Closure law : for any $a, b \in R \Rightarrow a+b \in R$ & $a \cdot b \in R$.
2. Associative law : for any $a, b, c \in R$, $(a+b)+c = a+(b+c)$ & $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Existence of identity:
   There exist an element denoted by '0' in R such that $a+0 = 0+a = a \ \forall a \in R$.
4. Existence of inverse for each $a \in R \ \exists \ -a \in R$ such that $a+(-a) = (-a)+a = 0 \ \forall a \in R$.
5. Commutative law : for any $a, b \in R$, $a+b = b+a$.
6. Distributivity for any $a, b, c \in R$; $a(b+c) = ab+ac$. and $(b+c)a = ba+ca$.

OR

$(R, +, \cdot)$ is said to be a ring if
(i) $(R, +)$ is an additive abelian group.
(ii) Multiplication is closed, Associative & Distributive.

Examples of Ring

Let Z be set a integers with the usual addition and multiplication forms a ring, called ring of integers. i.e. $(Z, +, \cdot)$ is a ring.

1. $(\mathbb{Q}, +, \cdot)$ is a ring.
2. $(R, +, \cdot)$ is a ring.
3. $M_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R \right\}$; the set of all 2×2 matrix with real entries, then with the usual matrix addition and multiplication $M_2(R)$ forms a ring.

Some special cases/classes of Rings.

1. Null (or Zero Ring)

The set R containing only '0' forms a ring with usual addition and multiplication which is called null ring.

2. Commutative Ring

A ring $(R, +, \cdot)$ is said to be commutative ring if $a.b = b.a \quad \forall a, b \in R$.

e.g. $(Z, +, \cdot)$ is commutative ring.

But $M_2(R)$ = set of all 2×2 matrices is not commutative ring because matrix multiplication is not commutative.

3. Ring with identity element (with unit element)

A ring $(R, +, \cdot)$ is said to be a ring of unit element if $\exists 1 \in R$ such that:

$1.x = x.1 = x \quad \forall x \in R$.

(i) $(Z, +, \cdot)$ is a ring with unit element.

(ii) $E = \{0, \pm 2, \pm 4 \ldots\}$ = set of all even integers.

$(E, +, \cdot)$ is a ring without unit element.

4. Rings with or Without Zero divisors

Let R be a ring and $a, b \in R$. Then a ring element $a (\neq 0)$ is called a divisor of zero if there exists an element $b (\neq 0)$ in the ring such that either $a.b = 0$ or $b.a = 0$. (i.e. a & b are zero divisors or divisor of zero)

In this case, the Ring R is called ring with zero divisors.

Example

Let $M_2(R)$ = set of all 2×2 matrices.

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq 0$ and $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq 0$,

$A, B \in M_2(R)$.

Now, $A.B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Here, A & B are zero divisors and the ring $M_2(R)$ is the ring with zero divisor.

A ring $(R, +, \cdot)$ is said to be ring without zero divisors if $a.b = 0$ implies $a = 0$ or $b = 0$.

Example

$(Z, +, \cdot)$ is a ring without zero divisor.

$(Q, +, \cdot)$ is a ring without zero divisor.

5. Integral Domain

A commutative ring $(R, +, \cdot)$ with unit element is said to be integral domain if R has no zero divisor. i.e. $a.b=0 \Rightarrow a=0$ or $b=0$.

Examples

i) $(\mathbb{Z}, +, \cdot)$ is an integral domain.

ii) $(\mathbb{C}, +, \cdot)$ ($\mathbb{C}$ = Complex number) is also an integral domain.

iii) $(\mathbb{Q}, +, \cdot)$ and $(\mathbb{R}, +, \cdot)$ are integral domains.

iv) $M_2(\mathbb{R})$ is not an integral domain because it does not satisfy commutative law.

6. Division Ring

A ring $(R, +, \cdot)$ with unit element is said to be a division ring if every non-zero element $a \in R$ has multiplicative inverse $a^{-1} \in R$.

i.e. : $\exists\, a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Examples

i) $(\mathbb{Q}, +, \cdot)$ is division ring.

ii) $(\mathbb{R}, +, \cdot)$ is division ring.

iii) The set of all 2×2 non-singular matrices is also division ring.

iv) $(\mathbb{Z}, +, \cdot)$ is not division ring.

v) $M_2(\mathbb{R})$ is not division ring.

Field: A commutative division ring is called a field.

OR, A commutative ring $(R, +, \cdot)$ with unit element is said to be a field if every non-zero element $a \in R$ has multiplicative inverse $a^{-1} \in R$.

Page No.:
Date : / /

Examples

i) $(R, +, \cdot)$ is field.

ii) $(Q, +, \cdot)$ is field.

iii) $(C, +, \cdot)$ is also field (set of all complex number)

iv) $(Z, +, \cdot)$ is not field.

v) The set of all 2×2 non-singular matrices is not field because it is non commutative.

Date : / /

4.2 Elementary Properties of Rings

Let $(R, +, \cdot)$ be a ring. let ~~$a, b \in R$~~ $a, b, c \in R$ then.

1. $a+b = a+c \Rightarrow b = c$
2. $a+b=0$ then $a = -b$ and $b = -a$
3. $a+x = b \Rightarrow x = b+(-a)$
4. $-(-a) = a$.
5. $a.0 = 0$
6. $(-a).b = a(-b) = -ab$
7. $(-a).(-b) = ab$
8. $a(b-c) = ab - ac$ & $(b-c)a = ba - ca$

Proof

1. $a+b = a+c$

$\Rightarrow (-a) + a + b = (-a) + a + c$

$\Rightarrow 0 + b = 0 + c$

$\Rightarrow b = c$ proved.

2. $a+b = 0$

$\Rightarrow (-a) + a + (b) = 0 + (-a)$

$\Rightarrow 0 + b = 0 + (-a)$

$\Rightarrow b = -a$

$\Rightarrow a = -b$ proved.

3. $a+x = b$

$\Rightarrow (-a) + a + x = (-a) + b$

$\Rightarrow 0 + x = -a + b$

$\Rightarrow x = b + (-a)$ proved.

Date : / /

4. $a = 0 + a$

$\Rightarrow a = -(-a) + (-a) + a$

$\Rightarrow a = -(-a) + 0$

$\Rightarrow a = -(-a)$

$\Rightarrow -(-a) = a$ proved.

5. We have,

$a \cdot 0 = a(0 + a)$

$\Rightarrow a \cdot 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow 0 = a \cdot 0$

$\Rightarrow a \cdot 0 = 0$ proved.

6. $(-a) \cdot b = 0 + (-a) \cdot b$

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

$= -(ab) + [a + (-a)]b$

$= -(ab) + 0 \cdot b$

$\Rightarrow (-a) \cdot b = -(ab)$ proved.

7. $(-a)(-b) = -a(-b)$

$\Rightarrow (-a)(-b) = ab$ proved.

8 $a(b-c) = a \cdot b - a \cdot c$

$= a(b-c)$

$= a[b + (-c)]$

$= a \cdot b + a(-c)$

$\Rightarrow a(b-c) = ab - ac$ proved.

Similarly,

$(b-c)a = bc - ca.$

Date : / /

4.3 Sub-rings, Ideals and Quotient rings with their properties.

Sub rings

A non-empty subset S of a ring R is said to be a sub ring of R if S itself forms a ring under the same binary operations of R.

Example

1. The ring $(\mathbb{Z}, +, \cdot)$ is a sub-ring of $(\mathbb{Q}, +, \cdot)$
2. The set $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \ldots\}$ $= E$ is a sub ring of $(\mathbb{Z}, +, \cdot)$.
3. The set $2\mathbb{Z}+1 = \{2n+1 : n \in \mathbb{Z}\} = \{+1, \pm 3, \pm 5 \ldots\}$ is a sub set of $\mathbb{Z}$ but it is not sub-ring of $\mathbb{Z}$.

Properties / theorems of Sub-rings:

Property 1 / Theorem 1

A non-empty subset S of a ring R is a sub ring of R if for each $a, b \in S \Rightarrow$ (i) $a-b \in S$ and (ii) $a \cdot b \in S$.

Proof

Suppose S is a sub-ring of a ring R. Let $a, b \in S$ then $-b \in S$ because S itself is a ring.

Now, $a-b \in S \Rightarrow a+(-b) \in S \Rightarrow a-b \in S$.

Again, since S is closed under multiplication

So, $a, b \in S \Rightarrow a \cdot b \in S$.

Conversely, suppose S is non-empty subset of R

such that,
$a, b \in S \Rightarrow a-b \in S$ and $a.b \in S$
We have to show S is a sub ring of R.

Since, S is non-empty subset of R so let $a \in$ then by condition (i)
$a, -a \in S \Rightarrow a-a \in S$ i.e. $0 \in S$.
So, S has additive identity.

Let $a \in S$ then again by condition (i)
$0, a \in S \Rightarrow 0-a \in S$ i.e $-a \in S$. So, every element of S has additive inverse in S.

Let ~~$a \in S$~~ $a, b \in S$ then $a, -b \in S$ again by (i) condition.
$a, -b \in S \Rightarrow a-(-b) \in S \Rightarrow a+b \in S$
closure is satisfied.
The binary operation addition (+) is associative and commutative throughout R so it is also associative and commutative on the subset S.
Now, by condition a) $a, b \in S \Rightarrow a.b \in S$, so, multiplicative closure is satisfied.

Since, the multiplication (.) is associative and distributive over addition. So, it also satisfies on the subset S.
Hence, S is a sub-ring of R.

Property 2/ Theorem 2.

The intersection of two sub-rings of a ring is also a sub-ring.

Proof:

Let S and T are sub-rings of ring R. Then we have to prove $S \cap T$ is a subring of R.

Since, $S \leq T$ are sub-rings so $0 \in S$ and $0 \in T$

$\Rightarrow$ i.e. $0 \in S \cap T$.

$\therefore S \cap T$ is a non-empty subset of R.

Let $a, b \in S \cap T$ then, $ab \in S$ and $a, b \in T$.

Since S and T are sub-rings of R, so, $a, b \in S$

$\Rightarrow a-b \in S$ and $a \cdot b \in S$ and $a, b \in T \Rightarrow a-b \in T$ and $a.b \in T$.

$\therefore a-b \in S \cap T$ and $a.b \in S \cap T$.

Hence, $S \cap T$ is sub-ring of R.

Property 3/ Theorem 3.

Every field is an integral domain.

Proof

Let F be a field. Since field F is commutative ring with unit element so to prove F is an integral domain, it is sufficient to show F has non-zero divisor.

Suppose $a, b \in F$ with $a \neq 0$ such that $a.b = 0$.

Since, $a \in F$ and $a \neq 0$ so $\exists\ a^{-1} \in F$ such that $a^{-1}a = aa^{-1} = 1$.

Now, $a.b = 0$

$\Rightarrow a^{-1}.(ab) = a^{-1}.0$

$\Rightarrow (a^{-1}.a)b = a^{-1}.0$

$\Rightarrow 1.b = a^{-1}.0$

$\Rightarrow 1.b = 0$

$\Rightarrow b = 0$.

Similarly, if $a, b \in F$ and $b \neq 0$ and $a.b = 0$ then we can show $a = 0$.

$\Rightarrow a.b = 0 \Rightarrow a = 0$ or $b = 0$ $\forall a, b \in F$

$\Rightarrow$ Hence, F has non-zero divisor. Hence, F is an integral domain.

But the converse of the above theorem may not be true.

i.e. An integral domain may not be field.

Property 4 / Theorem 4.

A skew field (division ring) has no zero divisors.

Proof

Let S be a skew field. Suppose $a, b \in S$ with $a \neq 0$ such that $a.b = 0$.

Since S is a skew field so $a \in S, a \neq 0$ $\exists a^{-1} \in S$ such that $a.a^{-1} = a^{-1}.a = 1$

Now, $a.b = 0$

$\Rightarrow a^{-1}.(ab) = a^{-1}.0$

$\Rightarrow (a^{-1}a)b = 0 \Rightarrow 1.b = 0 \Rightarrow b = 0$

Similarly, if $a, b \in S, b \neq 0$ and $a.b = 0$ then we can show $a = 0$.

$\therefore a.b = 0 \Rightarrow a = 0$ or $b = 0$ $\forall a, b \in S$.

Hence, S has no zero divisor.

Ideals

Ideal is a subring/subset of a mathematical ring with certain absorption properties.

Ex- The set of even ~~numbers~~ integers is an ideal in the ring of integers.

Left Ideal: Let R be a ring and I is non-empty subset of R. Then I is said to be a left ideal of R if)

(i) $a-b \in I \; \forall \; a,b \in I$

(ii) $ra \in I \; \forall \; r \in R, a \in I$

Right Ideal: Let R be a ring and I be a non-empty subset of R. Then I is said to be a right ideal of R if:

(i) $a-b \in I \; \forall \; a,b \in I$

(ii) $ar \in I \; \forall \; a \in I, r \in R.$

Ideal: (Two sided ideal): Let I be a non-empty subset of R then I is said to be an ideal of R if

(i) $a-b \in I \; \forall \; a,b \in I$

(ii) $ar, ra \in I \; \forall \; a \in I, r \in R.$

Example

(i) Let $E = \{0, \pm 2, \pm 4, \ldots\}$ then E is an ideal of Z, for since E is sub ring of Z and $\forall a \in Z$ and $r \in E$. We have $ar, ra \in E$. So, E is ideal of Z.

(ii) R = Set of real numbers $(R, +, \cdot)$ and $(E, +, \cdot)$ is subring of R but E is not an ideal of R.

Page No.:
Date : / /

Properties / theorems of ~~Rings~~ Ideals:

Property 1 / Theorem 1.

An Ideal I of a ring R is a sub ring of R.

Proof:

Let I be an ideal of a ring by R. By definition of ideal I is a non-empty subset of R. Let $a, b \in R$ then we have $a-b \in I$.

Again let $a, b \in I$ then $b \in R$ $(I \subset R)$

Hence, by definition of $a, b \in I \Rightarrow a.b \in I$.

Hence, I is a subring of R.

Property 2 / Theorem 2

The intersection of two ideal of a ring is again an ideal.

Proof:

Let H and K be two ideals of a ring R since $0 \in H \cap K$ so $H \cap K \neq \phi$.

So $H \cap K$ is non-empty set. Let $a, b \in H \cap K$ then $a, b \in H$ and $a, b \in K$.

Since H & K be two ideals so, $a, b \in H \Rightarrow a-b \in H$ and $ar, ra \in H$ for $r \in R$.

Similarly, $a-b \in K$ and $ar, ra \in K \ \forall r \in R$.

Hence, for $a, b \in H \cap K$ and $r \in R$, we have $a-b \in H \cap K$ and $ar, ra \in H \cap K$. Hence, $H \cap K$ is an ideal of R.

Note: The arbitrary intersection of ideals of R is also an ideal.

Page No.:
Date : / /

Property 3/ Theorem 3
The Commutative ring with unit element having {0} and R are only ideals in a field.

Proof:
Let us define a set $Ra = \{ra : r \in R\}$.
Let $x, y \in Ra$ then $x = r_1 a$ and $y = r_2 a$, for some $r_1, r_2 \in R$. Then $x - y = (r_1 - r_2)a \in Ra$ for $(r_1 - r_2) \in R$.

Again $rx = r(r_1 a) = (rr_1)a \in Ra$ for $r, r_1 \in R$. Since R is commutative ring so $xr \in Ra$.
Hence, R is an ideal of R.

We have, $Ra = \{0\}$ or R since $0 \neq a = 1 \cdot a \in Ra$. So $Ra \neq \{0\}$. So we must have $R = Ra$ i.e. every element R is a multiple of 'a' by some element of R. If $I \in R$ so $\exists\, a^{-1} \in R$ s.t. $aa^{-1} = 1$.
Hence, R is a field.

Sum and Product of Ideal

Let H and K be ideal of R. The sum of ideals is denoted by $H + K$ and defined by $H + K = \{x + y : x \in H, y \in K\}$

Similarly, the product of the ideal is denoted by HK and given by

$$HK = \left\{ \sum_{i=1}^{n} x_i y_i : x_i \in H, y_i \in K, n \in N \right\}$$

Date : / /

Quotient Ring

Let R be a ring and I be an ideal of R. Let $R' = \frac{R}{I} = \{a+I : a \in R\}$ be the set of all cosets of I in R then R/I forms a ring with respect to addition and multiplication defined by

$(a+I)+(b+I) = (a+b)+I$

$(a+I)\cdot(b+I) = a\cdot b+I$

This ring R/I is called quotient ring.

Theorem

Show that $\frac{R}{I}$ is a ring.

First well defined:

Let $a+I, a'+I, b+I, b'+I \in \frac{R}{I}$

Then we need to show $(a+I)+(b+I) = (a'+I)+(b'+I)$ and $(a+I)\cdot(b+I) = (a'+I)\cdot(b'+I)$

&

Since, $a+I = a'+I$ so $a-a' \in I$

Since, $b+I = b'+I$ so $b-b' \in I$

$\Rightarrow (a-a')+(b-b') \in I \Rightarrow (a+b)-(a'+b') \in I$

$\Rightarrow (a+b+I) = (a'+b'+I)$

$\Rightarrow (a+I)(b+I) = (a'+I)(b'+I)$

Since, $a, a', b, b' \in R$ and $a-a', b-b' \in I$ so $a'(b-b'), (a-a')b, (a-a')\cdot(b-b') \in I$

Now,

$(a.b-a.b') = a'(b-b')+(a-a')b+(a-a').(b-b') \in I$

i.e. $a.b-a.b' \in I$

$\Rightarrow a.b+I = a'b'+I$

Date : / /

$\Rightarrow (a+I)(b+J) = (a'+I)(b'+I)$

Hence, well defined.

Then we have to show R/I is a ring:

(i) Let $(a+I), (b+I) \in R/I$, since R is a ring

For all $a, b \in R \exists -a, -b \in R$.

Then $(a+I) - (b+I) = (a+I) + (-b+I)]$

$= (a+(-b)+I)$

$= a - b + I$

Hence $(a+I) - (b+I) \in R/I$

Again, $(a+I) \cdot (b+I) = (a \cdot b + I)$

This shows that $(a \cdot b + I) \in R/I$

This shows that R/I is a ring.

4.4 Homomorphism of Rings

Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be two rings $f: R \to R'$ be function. Then the function f is said to be a ring homomorphism if

(i) $f(a+b) = f(a) + f(b)$

(ii) $f(ab) = f(a) \cdot f(b)$ $\forall a, b \in R$

Then binary operation '+' and '·' on the left are the binary operation of R and + and · on the right right one of R'.

Example

Let $f: R \to M_2(R)$ be a mapping defined by $f(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ $\forall a \in R$, then f is a ring homomorphism.

Proof

(i) Let $a, b \in R$ then $f(a+b) = \begin{pmatrix} a+b & 0 \\ 0 & a+b \end{pmatrix}$

$= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$

$= f(a) + f(b)$

$\therefore f(a+b) = f(a) + f(b)$

(ii) $f(a \cdot b) = \begin{pmatrix} a \cdot b & 0 \\ 0 & a \cdot b \end{pmatrix}$

and

$f(a) \cdot f(b) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$

$= \begin{pmatrix} a \cdot b + 0 \cdot 0 & a \cdot 0 + 0 \cdot b \\ 0 \cdot b + a \cdot 0 & 0 \cdot 0 + a \cdot b \end{pmatrix}$

$= \begin{pmatrix} a.b & 0 \\ 0 & a.b \end{pmatrix}$

$= f(a.b)$

$\therefore f(ab) = f(a).f(b)$

So $f: R \to M_2(R)$ is a ring homomorphism.

Theorem

If $f: R \to R'$ be a ring homomorphism then

(i) $f(0) = 0'$ where 0 and $0'$ are additive identity of R and R' respectively.

(ii) $f(-a) = -f(a)$.

Proof:

(i) Let $f: R \to R'$ be ring homomorphism. 0 & $0'$ are additive identity of R and R' respectively.

Then for any $a \in R$; $a+0$; $f(a+0) = f(a)$

$\Rightarrow f(a) + f(0) = f(a)$ ($\because$ f is a ring homomorphism)

$\Rightarrow f(a) + f(0) = f(a) + 0'$

$\Rightarrow f(0) = 0'$.

(ii) Let $f: R \to R'$ be ring homomorphism, 0 & $0'$ are additive identity of R and R' respectively then for any $a \in R$

$a + (-a) = 0$

$\therefore f[a + (-a)] = f(a)$

$\Rightarrow f(a) + f(-a) = f(0)$

$\Rightarrow f(a) + f(-a) = 0'$ [$f(0) = 0'$]

This shows that $f(a)$ is the additive inverse of $f(a)$. So, $f(a) = -f(a)$.

Page No.:
Date : / /

Kernel of Ring homomorphism

Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be two rings, $f: R \to R'$ be ring homomorphism, then the set K_f defined by

$K_f = \{x : x \in R \text{ and } f(x) = 0'\}$ is called Kernel of ring homomorphism.

Image of Ring Homomorphism

Let $f: R \to R'$ be a ring homomorphism, then the set $f(R) = \{f(a) : a \in R\}$ is called image of ring homomorphism.

Page No.:
Date : / /

4.5 Integral Domain (ID), Principal Ideal Domain (PID), Euclidean Domain (ED), Unique Factorization Domain (UFD)

Integral Domain (ID)

An integral domain is a non-zero commutative ring in which the product of any two non-zero elements is non-zero.

or, An integral domain is a commutative ring with an identity ($1 \neq 0$) with no zero-divisors.

Alternatively, a commutative ring R with unity is called an integral domain if for all $a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

or in other words $a \neq 0, b \neq 0 \Rightarrow ab \neq 0 \ \forall a, b \in R$

Examples

i) The set I of Integers under usual addition and multiplication is an integral domain for any two integers a, b, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

ii) Consider a ring $R = \{0, 1, 2, 3, 4, 5, 6, 7\}$ under the addition and subtraction modulo 8. This ring is commutative but it is not an integer domain because $2 \in R, 4 \in R$ are two non-zero elements such that $2.4 \equiv 0 \pmod 8$.

Principal Ideal Domain (PID)

A principal ideal domain (PID) is an integral domain in which every proper ideal can be generated by a single element.

A ring R is a principal ideal domain if,

i) It is an integral domain (hence in particular a commutative ring)

ii) Every ideal in R is a principle ideal.

Examples

- K, any field
- Z: the ring of integers
- K[x]: rings of polynomials
- Z[i]: ring of Gaussian integers.
- any Euclidean domain.

Euclidean Domain (ED)

An Euclidean domain (also called an Euclidean ring) is an integral domain that can be endowed with an Euclidean function which allows a suitable generalization of the Euclidean division of the Integers.

An Euclidean domain is an integral domain R with a norm 'n' such that for any $a, b \in R$, there exist q, r such that $a = q.b + r$ with $n(r) < n(b)$.

The element 'q' is called and 'r' is called remainder.

Euclidean domains further have an Euclidean

algorithm for finding a common divisor of two elements.

Examples of Euclidean Domain:

- Any field. Define $f(x) = 1$ for all non-zero x.
- $\mathbb{Z}$, the ring of integers. Define $f(n) = |n|$.
- $\mathbb{Z}[i]$, the ring of Gaussian integers, define $f(a+bi) = a^2+b^2$.
- $K[x]$, the ring of polynomials over field K.

Unique Factorization Domain (UFD)

A UFD is a commutative ring in which every element can be uniquely written as a product of prime elements, analogous to the fundamental theorem of arithmetic. UFDs are sometimes called factorial rings.

An integral domain R with identity is called unique factorization domain if it satisfies the following:

(i) Every non-zero non unit element a can be factorized into irreducible.

(ii) If $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, where p_i's and q_i's are irreducible then p_i's and q_i's are associates in some order and $m = n$.

Example

- Every field F is a UFD because each non-zero

element of a field is a unit.

- The Gaussian integers, $Z[i] := \{a+bi / a, b \in Z\}$
- The polynomial ring $K[x_1, \ldots, x_n]$ is UFD.
-

Date : / /

Unit-5

Vector Spaces

Page No.:
Date : / /

5.1. Definition and examples of vector spaces

Definition

Let V be a non-empty set of objects and F be a given field. Suppose vector addition and vector multiplication is defined in V. Then we say V is a vector space over the field F if it satisfies the following properties:

A.1: Closure - for any $u, v \in V \Rightarrow u+v \in V$

A.2: Associativity - for any $u, v, w \in V \Rightarrow (u+v)+w = u+(v+w)$

A.3: Existence of additive inverse:- There is an element $0 \in V$ such that $u+0=u \ \forall u \in V$

A.4: Existence of additive inverse - For each $u \in V$, $-u \in V$ such that $u+(-u)=0$.

A.5: Commutative - for each $u, v \in V$, $u+v=v+u$

M1: Closure - for any $\alpha \in F, u \in V \Rightarrow \alpha u \in V$

M2: Distributivity for vector addition - for any $\alpha \in F$ $u, v \in V \Rightarrow \alpha(u+v) = \alpha u + \alpha v$.

M3: Distributivity for scalar addition - For any $\alpha, \beta \in F$, and $u \in V, (\alpha+\beta)u = \alpha u + \beta u$

M4: Associativity for scalar multiplication :- For any $\alpha, \beta \in F$ and $u \in V, \alpha(\beta u) = \alpha(\beta)u = \beta(\alpha u)$

M5: Existence of unity in field - For each $u \in V, 1 \in F$ such that $1 \cdot u = u$

Page No.:
Date: / /

Note - The elements of V are called vectors and elements of F are called scalars.

Examples

Ex-1: The set of real numbers ($\mathbb{R}$) is a vector space over the field F of real numbers ($\mathbb{R}$) with usual addition and multiplication of real numbers.

Ex-2: The set of all 2×3 matrix forms a vector space over the field of real numbers with usual addition of matrix addition and multiplication of matrix by a scalar.

Properties of Vector Spaces

1. If $\alpha \in F$ and $0 \in V$ then $\alpha 0 = 0$.
2. If $0 \in F$ and $u \in V$ then $0 \cdot u = 0$
3. If $\alpha \in F$, $u \in V$ and αu of $\alpha u = 0 \Rightarrow \alpha = 0$, $u = 0$ or both.
4. $(-1) \cdot u = -u$.

5.2 Subspaces

A non-empty subset W of a vector space V over the field F is said to be a subspace of V if W itself is a vector space with respect to vector addition and scalar multiplication defined in V.

Example

Ex-1 The space $\mathbb{R}$ of real numbers is subspace of the vector space C, of the set of complex numbers over the field of real number.

Ex-2 : Let $V = \mathbb{R}^3$ be a vector space over $\mathbb{R}$ then, $W = \{x, y, 0 : x, y \in \mathbb{R}\}$ is a subspace of V.

Let $\alpha, \beta \in \mathbb{R}$ and $u = (x_1, y_1, 0)$, $v = (x_2, y_2, 0) \in V$ then,

$\alpha u + \beta v = \alpha(x_1, y_1, 0) + \beta(x_2, y_2, 0)$

$= (\alpha x_1 + \beta x_2, \alpha y_1 + \beta y_2, 0)$ is a point on xy-plane.

$\therefore \alpha u + \beta v \in W$

So, W is a subspace of V.

Page No.:
Date: / /

Theorems of Vector Spaces and Subspaces:

Theorem 1

The non-empty subset W of a vector space V is a subspace of V iff for any scalars $\alpha, \beta \in F$ and $u, v \in W \Rightarrow \alpha u + \beta v \in W$.

Proof:

Let W be a subspace of V.

Let $\alpha, \beta \in F$ & $u, v \in W$. Since W itself is a vector space, so $\alpha u \in W$ & $\beta v \in W$.

Conversely, if $\alpha u + \beta v \in W$

Let $\alpha = 1$, $\beta = 1$

Then, $1 \cdot u + 1 \cdot v = u + v \in W$

Let $\alpha = 0$, $\beta = 0$

Then,

$0 \cdot u + 0 \cdot v = 0 \in W$

Let, $\alpha = -1$, $\beta = 0$

$-1 \cdot u + 0 \cdot v = -u \in W$

Let, $\beta = 0$

$\alpha u + 0 \cdot v = \alpha u \in W$.

Since, remaining properties are satisfied throughout V, they are also satisfied in subset W of V.

Hence, W is a subspace of V.

Page No.:
Date : / /

Theorem 2

The intersection of any two subspace of a vector space is also a subspace.

Proof

Let V be a vector space over field F.
Let W_1 & W_2 are subspace of V.
So, $\alpha, \beta \in F$ & $u, v \in W_1$ & W_2
$\Rightarrow \alpha u + \beta v \in W_1$ & $\alpha u + \beta v \in W_2$

Since, $\alpha u + \beta v \in W_1$ & $\alpha u + \beta v \in W_2$
$\Rightarrow \alpha u + \beta v \in W_1 \cap W_2$
~~So, $W_1 \cap W_2$ is~~
So, $W_1 \cap W_2$ is a subspace of V.

Theorem 3

The linear sum of two subspaces also a subspace.

Proof

Let V be a vector space ~~of order~~ over field F. U & W be two subspace of V.
Then,
$U + W = \{u + w, u \in V$ & $v \in W\}$
Since, U & W are subspace of V so, $0 \in U$ & $0 \in W$
$\Rightarrow 0 + 0 \in U + W$
$\Rightarrow 0 \in U + W$
So, $U + W$ is a non-empty subspace of V.
Let,
$\alpha, \beta \in F$ & $v_1 = u_1, v_2 = u_2 + w_2 \in U + W$
Now,
$\alpha v_1 + \beta v_2 = \alpha(u_1 + w_1) + \beta(u_2 + w_2)$
$= (\alpha u_1 + \alpha w_1) + (\beta u_2 + \beta w_2)$

$= \alpha u_1 + \alpha w_1 + \beta u_2 + \beta w_2$

$= \alpha u_1 + \beta u_2 + \alpha w_1 + \beta w_2$

Since, U & W are subspace of V

So $\alpha u_1 + \beta v_2 \in U$ & $\alpha w_1 + \beta w_2 \in W$

$\therefore \alpha v_1 + \beta v_2 \in U + W$

Hence the linear sum of two subspace also a subspace.

5.3 Linear Combination : linear independence and linear dependence

Linear Combination

Let V be a vector space over the field F. $u_1, u_2 \cdots u_n$ be any vectors in V (i.e. $u_1, u_2, \cdots u_n \in V$) for any scalars $\alpha_1, \alpha_2 \cdots \alpha_n \in F$.

Then,

$\alpha_1 u_2 + u_2 u_2 + \cdots + \alpha_n u_n$ is called linear combination of vectors $(u_1, u_2 \cdots u_n)$ of V.

Linearly dependent Vectors

Let V be a vector space of the field F. Then the vectors $u_1, u_2 \cdots u_n$ of V are said to be linearly dependent if $\exists$ scalar $\alpha_1, \alpha_2 \cdots \alpha_n \in F$, at least one side of them being non-zero such that $\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n = 0$.

In this case the set $S = \{u_1, u_2, \cdots u_n\}$ of vector is said to be set of linearly dependent vector.

Examples

Ex-1

Let $V = R^3$ and $u_1 = (3,3)$, $u_2 = (1,1)$ for each $1, -3 \in F$.

$$u_1 + (-3)u_2 = (3,3) + -3(1,1)$$
$$= (3-3, 3-3)$$
$$= (0,0) = 0.$$

Ex-2 The matrix $u = \begin{pmatrix} -3 & -1 & -2 \\ -1 & 2 & 4 \end{pmatrix}$ and $v = \begin{pmatrix} 6 & 2 & 4 \\ 2 & -4 & -8 \end{pmatrix}$

Page No.:
Date : / /

Then, $2u+v = 2\begin{pmatrix} -3 & -1 & -2 \\ -1 & 2 & -4 \end{pmatrix} + \begin{pmatrix} 6 & 2 & 4 \\ 2 & -4 & -8 \end{pmatrix}$

$= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

$\therefore$ u & v are linear dependent.

Linearly Independent Vectors

Let V be the vector space over the field F. Then the vector $u_1, u_2, \ldots u_n$ of V are said to be linearly independent whenever

$\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n = 0$.

$\Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = \ldots = \alpha_n = 0$.

(All the scalar must be zero).

Example

Let $V = \mathbb{R}^2$

$u_1 = (1, 1)$

$u_2 = (2, 1) \in V$

Suppose, $\alpha_1 u_1 + \alpha_2 u_2 = 0 \quad \alpha_1, \alpha_2 \in F$

$\Rightarrow \alpha_1(1,1) + \alpha_2(2,1) = (0,0)$

$\Rightarrow (\alpha_1 + 2\alpha_2, \alpha_1 + \alpha_2) \Rightarrow (0,0)$

$\Rightarrow \alpha_1 + 2\alpha_2 = 0$ and $\alpha_1 + \alpha_2 = 0$

$\Rightarrow -\alpha_2 + 2\alpha_2 = 0 \qquad \Rightarrow \alpha_1 = -\alpha_2$

$\Rightarrow \alpha_2 = 0. \qquad \Rightarrow \alpha_1 = 0$

So, u_1, u_2 are linearly independent.

Date : / /

5.4 Basis and dimension of a Vector Space

Basis

A Set $S = \{v_1, v_2 \cdots v_n\}$ of vectors is said to be a basis of vector space V if

(i) S generate V.

(ii) $v_1, v_2 \cdots v_n$ are linearly independent vectors.

Example

Let $V = R^2 = \{(x,y) : (x,y) \in R\}$

$v_1 = (1,1)$, $v_2 = (2,1)$

Then prove that $S = (v_1, v_2)$ forms a basis of V.

Proof

Let $V = R^2$ and $v_1 = (1,1)$, $v_2 = (2,1)$

and let $\alpha_1, \alpha_2 \in F$

(i) S generates V.

~~$\Rightarrow (x,y) = \alpha_1(1,1) + \alpha_2(2,1)$~~

Let $v = (x,y) \in V$ and $v = \alpha_1 v_1 + \alpha_2 v_2$

$\Rightarrow (x,y) = \alpha_1(1,1) + \alpha_2(2,1)$

$\Rightarrow (x,y) = (\alpha_1 + 2\alpha_2, \alpha_1 + \alpha_2)$

$\Rightarrow \alpha_1 + 2\alpha_1 = x$ and $\alpha_1 + \alpha_2 = y$

$\Rightarrow \alpha_1 = y - \alpha_2$

Then, $y - \alpha_2 + 2\alpha_2 = x$

$\Rightarrow \alpha_2 = x - y$

and $\alpha_1 = y - (x-y) = y - x + y = 2y - x$

$(x,y) = \alpha_1(1,1) + \alpha_2(2,1)$

$(x,y) = (2y-x)(1,1) + (x-y)(2,1)$

This shows that $\{v_1, v_2\}$ generates V.

Secondly, we have to show v_1, v_2 are linearly independent.

Page No.:
Date : / /

Suppose $\alpha_1 v_1 + \alpha_2 v_2 = 0$ $\quad \alpha_1, \alpha_2 \in F$

$\alpha_1(1,1) + \alpha_2(2,1) = 0$

$\Rightarrow (\alpha_1, \alpha_1) + (2\alpha_2, \alpha_2) = 0$

$\Rightarrow (\alpha_1 + 2\alpha_2, \alpha_1 + \alpha_2) = (0,0)$

$\Rightarrow \alpha_1 + 2\alpha_2 = 0$ & $\alpha_1 + \alpha_2 = 0$

$\Rightarrow \alpha_1 = -\alpha_2$

$\alpha_1 + 2\alpha_2 = 0$

$\Rightarrow -\alpha_1 + 2\alpha_2 = 0$

$\Rightarrow \alpha_2 = 0$ and $\alpha_1 = 0$.

Hence, v_1 and v_2 are linearly independent, so $\{v_1, v_2\}$ forms a basis.

Dimension of Vector Space:

Let V be a vector space over field F and then the number of vectors in ~~be~~ basis of V is called the dimension of V.

e.g. $V = \mathbb{R}^2$, $v_1 = (1,1)$, $v_2 = (2,1)$

$\beta_2 = \{v_1, v_2\}$ is a basis of V. So, dimension of $V = 2$.

Date : / /

Unit-6
Linear Transformation

Page No.:
Date : / /

6.1 Definition and examples of linear transformations

Let V and W be two vector spaces over the same field F. Then the mapping $T: V \to W$ is said to be a linear transformation (Homomorphism of Vector Spaces) if

(i) $T(v_1 + v_2) = T(v_1) + T(v_2) \quad \forall v_1, v_2 \in V$

(ii) $T(\alpha v) = \alpha T(v) \quad \forall \alpha \in F, v \in V.$

Note

1. A linear transformation from vector space V to itself is called linear operator.

2. Taking $\alpha = 0$ in (ii) we get $T(0v) = 0T(v)$ or $T(0) = 0$. Thus the linear transformation takes 0 to 0.

Examples of linear transformation:

Eg 1

Let $I: V \to V$ be a identity function defined by $I(v) = v \quad \forall v \in V$.

Then prove that I is linear transformation.

Soln:

Let $v_1, v_2 \in V$ then $I(v_1 + v_2) = v_1 + v_2$

and $I(v_1) + I(v_2) = v_1 + v_2$

$\therefore I(v_1 + v_2) = I(v_1) + I(v_2)$

again $\alpha \in F$ and $v \in V$ then $I(\alpha v) = \alpha v = \alpha I(v)$

$\therefore$ I is a linear transformation.

Page No.:
Date : / /

Ex-2

The zero mapping $0: V \to W$ defined by $0(v) = 0 \ \forall v \in V$ linear transformation.

Sol:

Let $v_1, v_2 \in V$ and then $0(v_1+v_2) = 0$

and $0(v_1) + 0(v_2) = 0 + 0 = 0$

$\therefore 0(v_1+v_2) = 0(v_1) + 0(v_2)$

Also, let $\alpha \in F$ and $v \in V$ then

$0(\alpha v) = 0$ and $\alpha(v) = \alpha \cdot 0 = 0$

i.e. $0(\alpha v) = \alpha 0(v)$

Hence, 0 is a linear transformation.

Page No.:
Date : / /

Theorems / Properties of linear transformation

Theorem 1

Let V and W be two vector spaces over the same field F then the mapping $T: V \to W$ is linear if and only if

$T(\alpha v_1 + \beta v_2) = \alpha T(v_1) + \beta T(v_2) \quad \forall \alpha, \beta \in F;\ v_1, v_2 \in V$

Proof

First suppose T is linear.

Let $\alpha, \beta \in F$ and $v_1, v_2 \in V$ then

$\alpha v_1, \beta v_2 \in V \Rightarrow \alpha v_1 + \beta v_2 \in V$

Now, $T(\alpha v_1 + \beta v_2) = T(\alpha v_1) + T(\beta v_2)$ from (i) condition

$= \alpha T(v_1) + \beta T(v_2)$ ... from (ii) condition.

Conversely, suppose $T(\alpha v_1 + \beta v_2) = \alpha T(v_1) + \beta T(v_2)$

$\forall \alpha, \beta \in F$ ...(i) $\forall v_1, v_2 \in V$

Then we have to show T is linear.

Taking $\alpha = \beta = 1$ in (i) we get

$T(v_1 + v_2) = T(v_1) + T(v_2) \quad \forall v_1, v_2 \in V$

Taking $\beta = 0$ in (i)

~~$T\alpha(v_1) = \alpha T(v_1) \quad \forall \alpha \in F, v \in V$~~

$T\alpha(v_1) + T0(v_2) = \alpha T(v_1) + 0T(v_2)$

$\Rightarrow T\alpha(v_1) + 0 = \alpha T(v_1) \quad \forall \alpha \in F, v \in V.$

(∵ T is linear).

Page No.:
Date: / /

Theorem 2

Let $T: V \to W$ be a linear transformation from V to W. If $\{v_1, v_2, \ldots, v_n\}$ is linearly independent in V then $\{T(v_1), \ldots, T(v_n)\}$ is also linearly independent in W.

Proof

Let $v_1, v_2, \ldots, v_n$ are linearly independent in V then scalar $\alpha_1, \alpha_2, \ldots \alpha_n \in F$ such that

$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0 \in V \quad [\alpha_1 = \alpha_2 = \cdots \alpha_n = 0]$

i.e. $T = T(\alpha_1 v_1 + \cdots + \alpha_n v_n)$

$0 = \alpha_1 T(v_1) + \cdots + \alpha_n T(v_n)$

Then shows that $T(v_1), T(v_2) \ldots, T(v_n)$ are linearly independent in W.

Note: Let $T: V \to W$ be a linear transformation and $v_1, v_2, \ldots v_n$ be any vectors of V. If $T(v_1), T(v_2) \ldots, T(v_n)$ are linearly independent in W then $v_1, v_2, \ldots v_n$ are linearly independent in V.

Proof:

Since, $T(v_1), T(v_2), \ldots T(v_n)$ are linearly independent in W. Then $\exists \alpha_1, \alpha_2, \ldots \alpha_n \in F$ such that

$\alpha_1 T(v_1) + \alpha_2 T(v_2) + \cdots + \alpha_n T(v_n) = 0$

$\Rightarrow \alpha_1 = \alpha_2 \cdots = \alpha_n = 0$

$T(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) = 0 = T(0)$

$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$ ①

$\Rightarrow \alpha_1 = \alpha_2 = \cdots \alpha_n = 0$

$\therefore v_1, v_2, \ldots v_n$ are linearly independent in V.

Page No.:
Date : / /

6.2 Kernel and Image of Linear Transformation

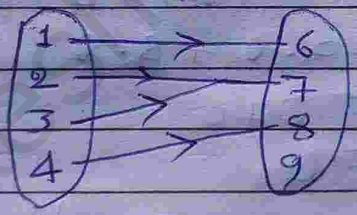
Let V and W be two vector spaces over the same field F, and $T: V \to W$ is a linear transformation. Then the kernel of T is the set of all elements $v \in V$ such that $T(v) = 0$. It is denoted by ker T.

$\therefore \ker T = \{v \in V : T(v) = 0\}$

The image of T is the set of all images of elements of V. It is denoted by $I(V)$ and given be,

$I(V) = \{w \in W : w = T(v) \text{ for some } v \in V\}$

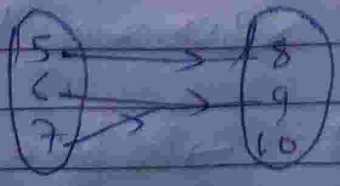
Example 1



$6 = T(1), \ 7 = T(2) \ \& \ T(3), \ 8 = T(4)$

$I(V) = \{6, 7, 8\}$

Example 2



$T(5) = 8, \ T(6) = T(7) = 9$

$I(V) = \{8, 9\}$.

Page No.:
Date : / /

Theorems / properties related to Kernel and Image of Linear Transformation:

Theorem 1 / Property 1

If $T: V \to W$ be a linear Transformation then, $\ker T$ is a subspace of V.

Proof

Let, $T: V \to W$ is a linear Transformation and $\ker T = \{v \in V : T(v) = 0\}$

Since $T(0) = 0 \in \ker T$

$\therefore \ker T$ is non-empty subset of V.

Let $v_1, v_2 \in \ker T$ and $\alpha, \beta \in V$. Then,

$T(v_1) = 0$ and $T(v_2) = 0$

Now,

$T(\alpha v_1 + \beta v_2) = \alpha T(v_1) + \beta T(v_2)$ ($\because T$ is linear)

$= \alpha \cdot 0 + \beta \cdot 0$

$= 0 + 0$

$= 0$

Now, $\alpha v_1 + \beta v_2 \in \ker T$. Hence $\ker T$ is subspace of V.

Theorem 2 / Property 2

Let $T: V \to W$ be a linear Transformation, then image of T is subspace of V.

Proof:

We have, $T: V \to W$ be a linear Transformation.

$\text{Im } T$ or $I(T) = \{w \in W : w = T(v)$ for some $v \in V\}$

Since, $0 \in W$ and $0 = T(0)$ So, $0 \in \text{Im } T$.

$\therefore \text{Im } T$ is non-empty subset of W.

Page No.:
Date : / /

Let, $w_1, w_2 \in ImT$ and $\alpha, \beta \in F$

Then,

$w_1 = T(v_1)$ and $w_2 = T(v_2)$ for some $v_1, v_2 \in V$

Now,

$$\alpha w_1 + \beta w_2 = \alpha T(v_1) + \beta T(v_2)$$
$$= T\alpha(v_1) + T\beta(v_2)$$
$$= T(\alpha(v_1) + \beta(v_2))$$

Since, $\alpha v_1 + \beta v_2 \in V$. So $T(\alpha v_1 + \beta v_2) \in ImT$

i.e. $\alpha w_1 + \beta w_2 \in ImT$

$\therefore ImT$ is a subspace of W. Hence, proved.

Page No.:
Date : / /

6.3 Algebra of linear transformations

Let V and W be two vector spaces over the same field F. T_1 and T_2 are two linear transformations from V to W. Let $v \in V$ and k be a scalar then.

(i) The sum $T_1 + T_2$ defined as $(T_1 + T_2)v = T_1(v) + T_2(v)$

(ii) The product kT_1 is defined as

$(kT_1)v = kT_1(v)$.

Page No.:
Date : / /

Explain and prove the algebraic properties of linear transformation.

Theorem 1

The sum of two linear tranformations is also linear.

Proof

Let V and W be two vector spaces over the same field F. T_1 and T_2 be two linear transformations from V to W. Then we have to show T_1+T_2 is linear.

Now,

Let $v_1, v_2 \in V$ then $(T_1+T_2)(v_1+v_2)$

$= T_1(v_1+v_2) + T_2(v_1+v_2)$ (by defn)

$= T_1(v_1) + T_1(v_2) + T_2(v_1) + T_2(v_2)$

(since, T_1, T_2 are linear)

$= T_1(v_1) + T_2(v_1) + T_1(v_2) + T_2(v_2)$

$= (T_1+T_2)v_1 + (T_1+T_2)v_2$

Again,

Let $\alpha \in F$ and $v \in V$

then, $(T_1+T_2)\alpha v = T_1\alpha(v) + T_2\alpha(v)$

$= \alpha T_1(v) + \alpha T_2(v)$

$= \alpha[T_1(v)+T_2(v)]$

$= \alpha(T_1+T_2)(v)$

$\therefore T_1+T_2$ is a linear transformation.

Page No.:
Date : / /

Theorem 2

The product of a scalar k and the linear Transformation $T: V \to W$ is a linear Transformation.

Proof

Let V and W be two vector spaces over the same field F. Let

Let $T: V \to W$ be a linear transformation and $k \in F$, a scalar. Then we have to show that kT is a linear.

(i) Let $v_1, v_2 \in V$ then,

$$kT(v_1+v_2) = k T(v_1+v_2) = k[T(v_1)+T(v_2)]$$
$$= kT(v_1) + kT(v_2)$$
$$= kT(v_1) + kT(v_2)$$

(ii) Let $\alpha \in F$ and $v \in V$.

$$kT(\alpha v) = kT(\alpha v) = k\alpha T(v) \quad (\because T \text{ is linear})$$
$$= \alpha k T(v)$$
$$= \alpha (kT)(v)$$

Hence, $kT(v_1+v_2) = kTv_1 + kTv_2$

$$kT(\alpha v) = \alpha (kT)(v)$$

Therefore, kT is linear Transformation.

6.4 Matrix representation of linear transformation

Let V and W be two vector spaces over the same field F. $T: V \to W$ be a linear transformation.

Suppose $\{u_1, u_2, \dots u_n\}$ be a basis of V and $\{w_1, w_2, \dots w_m\}$ be a base of W.

Then, for any $u_i \in V$; $T(u_i) \in W$.

So, scalars $a_{ij} \in F$ such that

$$\left.\begin{aligned} T(u_1) &= a_{11}w_1 + a_{12}w_2 + \dots + a_{1m}w_m \\ T(u_2) &= a_{21}w_1 + a_{22}w_2 + \dots + a_{2m}w_m \\ T(u_3) &= a_{31}w_1 + a_{32}w_2 + \dots + a_{3m}w_m \\ &\vdots \\ T(u_n) &= a_{n1}w_1 + a_{n2}w_2 + \dots + a_{nm}w_m \end{aligned}\right\} \quad \dots (i)$$

Then the transpose of coefficient matrix of (i) is called the matrix representation of linear transformation T with respect to given bases.

Example 1

Find the matrix representation by the linear transformation $T: R^2 \to R^2$ defined by $T(x,y) = (x, 2y)$ with respect to standard bases.

Soln:

We have $\{(1,0), (0,1)\}$ is the standard bases.

$T(1,0) = (1,0) = 1 \cdot w_1 + 0 w_2$

$T(0,1) = (0,1) = 0 \cdot w_1 + 0.2 w_2$

∴ The coefficient of matrix is $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$

Page No.:
Date : / /

∴ The matrix representation of linear transformation is $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}^T = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1m} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2m} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nm} \end{bmatrix}$$

→ Matrix representation of linear transformation

6.5 Eigen Values and Eigen Vectors

Let, V be a vector space over the field F. $T: V \to V$ be a linear transformation (or operator). Then the scalar $\lambda \in F$ is said to be Eigen value of T, if $\exists$ a non-zero vector $v \in V$ such that $T(v) = \lambda v$.

If λ is a ~~eigen~~ Eigen value of T then any vector $v \in V$ such that $T(v) = \lambda v$ is called Eigen vector of T associated with Eigen value λ. The collection of all Eigen vector $v \in V$ such that $T(v) = \lambda v$ is called Eigen space associated with Eigen value λ.

Example

Let, ~~V be~~ $I: V \to V$ be a linear transformation defined by $I(v) = v \ \forall v \in V$.

If we take $\lambda = 1$ then $I(v) = 1 \cdot v = \lambda v \ \forall v \in V$.

So, 1 is the Eigen value of I and all vectors $v \in V$ are Eigen vector associated with Eigen value $\lambda (= 1)$.

Note: We Consider square matrix of order n as a linear transformation from F^n to F^n. The eigen value of the matrix are the eigen value of matrix as a linear transformation.

- If A is a square matrix of order n then $A - \lambda I$, when I is a square unit matrix of order n called characteristics matrix of A.
- The determinant $|A - \lambda I|$ is called characteristics polynomial of A.

Page No.:
Date : / /

. The equation $|A-\lambda I|=0$ is called characteristic equation.
. The roots of characteristic equation are called eigen values of matrix A.

Note: Eigen values are also called latent root or proper value or spectral value. Eigen vectors are also called latent vectors or proper vectors or spectral vector.

Q1. Find the eigen values and eigen vectors of the matrix $A=\begin{pmatrix}3 & -1\\ 1 & 1\end{pmatrix}$.

Soln:
The characteristic equation of matrix A is $|A-\lambda I|=0 \Rightarrow \left|\begin{bmatrix}3 & -1\\ 1 & 1\end{bmatrix}-\lambda\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right|=$

$\Rightarrow \left|\begin{bmatrix}3-1\\ 1\ 1\end{bmatrix}-\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}\right|=0 \Rightarrow \begin{vmatrix}3-\lambda & -1\\ 1 & 1-\lambda\end{vmatrix}=0$

$\Rightarrow (3-\lambda)(1-\lambda)+1=0$
or, $3-3\lambda-\lambda+\lambda^2+1=0$
or, $\lambda^2-4\lambda+4=0$
or, $\lambda^2-2\lambda-2\lambda+4=0$
or, $\lambda(\lambda-2)-2(\lambda-2)=0$
or, $(\lambda-2)(\lambda-2)=0$
$\therefore \lambda=2$ and $\lambda=2$
The eigen value of A are 2 and 2.

Let $v=\begin{pmatrix}x\\ y\end{pmatrix}$ be a eigen vector
Then, $Av=\lambda v$, where $V=[x\ y]=\begin{bmatrix}x\\ y\end{bmatrix}$

Date : / /

$$\text{or, } \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 2 \begin{pmatrix} x \\ y \end{pmatrix} \quad [\text{where } \lambda = 2]$$

$$\text{or, } \begin{pmatrix} 3x-y \\ x+y \end{pmatrix} = \begin{pmatrix} 2x \\ 2y \end{pmatrix}$$

$\Rightarrow 3x-y = 2x$ and $x+y = 2y$
or, $3x-2x-y=0$ and $x+y-2y=0$
or, $x-y=0$ and $x-y=0$
$\Rightarrow x=y$ and $x=y$.

Thus implies if $x=y$ then $y=x$.
So, the eigen value is 2 and eigen vectors are $(1,1), (2,2)$ ---- etc.

Qe. Find the eigen values and eigen vector of the following matrix $\begin{pmatrix} 5 & 4 \\ 1 & 2 \end{pmatrix}$

Soln:
We have, $A = \begin{pmatrix} 5 & 4 \\ 1 & 2 \end{pmatrix}$

The characteristic equation is $|A - \lambda I| = 0$

$$\Rightarrow \left| \begin{pmatrix} 5 & 4 \\ 1 & 2 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right| = 0$$

$$\Rightarrow \left| \begin{pmatrix} 5 & 4 \\ 1 & 2 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right| = 0$$

$$\text{or, } \begin{vmatrix} 5-\lambda & 4 \\ 1 & 2-\lambda \end{vmatrix} = 0$$

$\Rightarrow (5-\lambda)(2-\lambda) - 4 = 0$
$\Rightarrow 10 - 5\lambda - 2\lambda + \lambda^2 = 0$

Date : / /

or, $\lambda^2 - 7\lambda + 6 = 0$

or, $\lambda^2 - 6\lambda - \lambda + 6 = 0$

or, $\lambda(\lambda-6) - 1(\lambda-6) = 0$

or, $(\lambda-6)(\lambda-1) = 0$

Either, $\lambda = 6$ or, $\lambda = 1$

∴ Eigen values are 1 and 6.

for $\lambda = 1$

Let, $V = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ be an eigen Vector.

Then, $AV = \lambda V$

$$\begin{pmatrix} 5 & 4 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 2\begin{pmatrix} x \\ y \end{pmatrix}$$

or, $\begin{pmatrix} 5x+4y \\ x+2y \end{pmatrix} = \begin{pmatrix} 2x \\ 2y \end{pmatrix} \Rightarrow 5x+4y = 2x$ and $x+2y = y$

$\Rightarrow x = -y$ and $x = -y$

So, the eigen vector associated with eigen value $\lambda = 1$ is $V = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

Again, for $\lambda = 6$

$AV = \lambda V$

or, $\begin{pmatrix} 5 & 4 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 6\begin{pmatrix} x \\ y \end{pmatrix} \Rightarrow \begin{pmatrix} 5x+4y \\ x+2y \end{pmatrix} = \begin{pmatrix} 6x \\ 6y \end{pmatrix}$

or, $5x+4y = 6x$ and $x+2y = 6y$

$\Rightarrow x = 4y$ and $x = 4y$

So the eigen vector associated with eigen value $\lambda = 6$ is $V = \begin{pmatrix} 4 \\ 1 \end{pmatrix}$

Date : / /

Q3. Find the eigen value and eigen vector of the matrix $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Soln:

Given, $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

The characteristic equation of A is $|A - \lambda I| = 0$

$$\text{or, } \left| \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right| = 0$$

$$\text{or, } \left| \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix} \right| = 0.$$

$$\text{or, } \begin{vmatrix} -\lambda & 1 & 0 \\ 1 & -\lambda & 0 \\ 0 & 0 & 1-\lambda \end{vmatrix} = 0$$

$$\text{or, } -\lambda \begin{vmatrix} -\lambda & 0 \\ 0 & 1-\lambda \end{vmatrix} - 1 \begin{vmatrix} 1 & 0 \\ 0 & 1-\lambda \end{vmatrix} + 0 \begin{vmatrix} 1 & -\lambda \\ 0 & 0 \end{vmatrix} = 0$$

$$\text{or, } -\lambda(-\lambda + \lambda^2 - 0) - 1(1 - \lambda - 0) + 0 = 0$$

$$\text{or, } \lambda^2 - \lambda^3 - 1 + \lambda = 0$$

$$\text{or, } \lambda^3 - \lambda^2 - \lambda + 1 = 0$$

$$\text{or, } \lambda^2(\lambda - 1) - 1(\lambda - 1) = 0$$

$$\text{or, } (\lambda - 1)(\lambda^2 - 1) = 0$$

$$\text{or, } (\lambda - 1)(\lambda + 1)(\lambda - 1) = 0$$

$\because (\lambda^2 - 1) = (\lambda + 1)(\lambda - 1)$

Either,

$\lambda - 1 = 0$ or $\lambda + 1 = 0$ or $\lambda - 1 = 0$

or $\lambda = 1$ or, $\lambda = -1$ or, $\lambda = 1$

Thus, the eigen values are $-1, 1, 1$. for $\lambda = 1$

Next for eigen vector,

Let, $v = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ be an eigen vector

Then, $AV = \lambda v$

or, $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = -1 \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ [Taking $\lambda = -1$]

or, $\begin{bmatrix} 0 + y + 0 \\ x + 0 + 0 \\ 0 + 0 + z \end{bmatrix} = -1 \begin{bmatrix} x \\ y \\ z \end{bmatrix}$

or, $\begin{bmatrix} y \\ x \\ z \end{bmatrix} = \begin{bmatrix} -x \\ -y \\ -z \end{bmatrix}$

Comparing both, we get

$y = -x \Rightarrow x + y = 0$ —(i)

$x = -y \Rightarrow x + y = 0$ —(ii)

$z = -z \Rightarrow z + z = 0 \Rightarrow 2z = 0 \Rightarrow z = 0$ —(iii)

~~So, the eigen vectors associated with~~

So, If $x = 1$ then $y = -1$

If $y = 1$ then $x = -1$.

$\therefore$ The eigen vector associated with eigen value $\lambda = -1$ is

Date : / /

$$V = \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} \text{ or } \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}$$

Again, For $\lambda = 1$

~~The eigen vector is~~

$$AV = \lambda v$$

$$\text{or } \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 1 \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$$\text{or, } \begin{pmatrix} y \\ x \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

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

So, the eigen vector associated with $\lambda = 1$ is

$$V = \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \text{ or } \begin{bmatrix} 2 \\ 2 \\ 2 \end{bmatrix}.$$

Page No.:
Date : / /

Find ~~the~~ eigen values and eigen vector

(a) $A = \begin{bmatrix} 2 & -2 & 2 \\ 1 & 1 & 1 \\ 1 & 3 & -1 \end{bmatrix}$

(b) $A = \begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix}$

(c) $A = \begin{bmatrix} 3 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 1 & -1 \end{bmatrix}$

a.

Soln:

Given,

$$A = \begin{bmatrix} 2 & -2 & 2 \\ 1 & 1 & 1 \\ 1 & 3 & -1 \end{bmatrix}$$

The characteristic equation of A is

$$|A - \lambda I| = 0$$

or $$\left| \begin{bmatrix} 2 & -2 & 2 \\ 1 & 1 & 1 \\ 1 & 3 & -1 \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right| = 0$$

or $$\left| \begin{bmatrix} 2 & -2 & 2 \\ 1 & 1 & 1 \\ 1 & 3 & -1 \end{bmatrix} - \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix} \right| = 0$$

Date : / /

$$\text{or, } \begin{vmatrix} 2-\lambda & -2 & 2 \\ 1 & 1-\lambda & 1 \\ 1 & 3 & -1-\lambda \end{vmatrix} = 0$$

$$\text{or, } (2-\lambda)\begin{vmatrix} 1-\lambda & 1 \\ 3 & -1-\lambda \end{vmatrix} - (-2)\begin{vmatrix} 1 & 1 \\ 1 & -1-\lambda \end{vmatrix} + 2\begin{vmatrix} 1 & 1-\lambda \\ 1 & 3 \end{vmatrix} = 0$$

$$\text{or, } (2-\lambda)\left[-(1-\lambda)(1-\lambda)-3\right] + 2(-1-\lambda-1) + 2(3-1+\lambda) = 0$$

$$\text{or, } (2-\lambda)(\lambda^2-1-3) + 2(-2-\lambda) + 2(2+\lambda) = 0$$

$$\text{or, } (2-\lambda)(\lambda^2-4) - 4 - 2\lambda + 4 + 2\lambda = 0$$

$$\text{or, } 2\lambda^2 - 8 - \lambda^3 + 4\lambda = 0$$

$$\text{or, } \lambda^3 - 2\lambda^2 - 4\lambda + 8 = 0$$

$$\text{or, } \lambda^2(\lambda-2) - 4(\lambda-2) = 0$$

$$\text{or, } (\lambda-2)(\lambda^2-4) = 0$$

$$\text{or, } (\lambda-2)(\lambda+2)(\lambda-2) = 0$$

Either,

$\lambda - 2 = 0$ or, $\lambda + 2 = 0$ or $\lambda - 2 = 0$

$\Rightarrow \lambda = 2$ $\Rightarrow \lambda = -2$ $\Rightarrow \lambda = 2$

~~Now,~~ ∴ Eigen values are $2, -2$.

~~∴ The Eigen vector associated with eigen value $\lambda = 2$ is~~

Next for eigen vector

~~Let~~ Taking $\lambda = 2$

$$AV = \lambda V \quad \left[\text{where } V = \begin{bmatrix} x \\ y \\ z \end{bmatrix}\right]$$

$$\text{or, } \begin{bmatrix} 2 & -2 & 2 \\ 1 & 1 & 1 \\ 1 & 3 & -1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 2\begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

Page No.:
Date : / /

e, $\begin{bmatrix} 2x-2y+2z \\ x+y+z \\ x+3y-z \end{bmatrix} = \begin{bmatrix} 2x \\ 2y \\ 2z \end{bmatrix}$

Comparing both, we get

$2x-2y+2z = 2x \Rightarrow 2y-2z=0 \Rightarrow y-z=0$ — (I)

$x+y+z=2y \Rightarrow x-y+z=0$ — (II)

$x+3y-z=2z \Rightarrow x+3y-3z=0$ — (III)

Now,

Coefficient of x	Coeff. of y	Coeff. of z	Constant
0	1	-1	0
1	-1	1	0
1	3	-3	0

$$D = \begin{vmatrix} 0 & 1 & -1 \\ 1 & -1 & 1 \\ 1 & 3 & -3 \end{vmatrix} = -1 \begin{vmatrix} 1 & 1 \\ 1 & -3 \end{vmatrix} - 1 \begin{vmatrix} 1 & -1 \\ 1 & 3 \end{vmatrix} = 0$$

$$D_1 = \begin{vmatrix} 0 & 1 & -1 \\ 0 & -1 & 1 \\ 0 & 3 & -3 \end{vmatrix} = -1 \begin{vmatrix} 0 & 1 \\ 0 & -3 \end{vmatrix} - 1 \begin{vmatrix} 0 & -1 \\ 0 & 3 \end{vmatrix} = 0$$

$$D_2 = \begin{vmatrix} 0 & 0 & -1 \\ 1 & 0 & 1 \\ 1 & 0 & 3 \end{vmatrix} = -1 \begin{vmatrix} 1 & 0 \\ 1 & 0 \end{vmatrix} = 0$$

$$D_3 = \begin{vmatrix} 0 & 1 & 0 \\ 1 & -1 & 0 \\ 1 & 3 & 0 \end{vmatrix} = -1 \begin{vmatrix} 1 & 0 \\ 1 & 0 \end{vmatrix} = 0$$

Date : / /

$\therefore x = \frac{D_1}{D} = \frac{0}{0}$, $y = \frac{D_2}{D} = \frac{0}{0}$, $z = \frac{D_3}{D_1} = \frac{0}{0}$

So, the eigen vector associated with $\lambda = 2$ is

$$V = \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Now,
Taking $\lambda = -2$
Eigen vector is

$$AV = \lambda V$$

$$\text{or, } \begin{bmatrix} 2 & -2 & 2 \\ 1 & 1 & 1 \\ 1 & 3 & -3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = -2 \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

$$\text{or, } \begin{bmatrix} 2x - 2y + 2z \\ x + y + z \\ x + 3y - z \end{bmatrix} = \begin{bmatrix} -2x \\ -2y \\ -2z \end{bmatrix}$$

Comparing both, we get

$2x - 2y + 2z = -2x \Rightarrow 4x - 2y + 2z = 0 \Rightarrow 2x - y + z = 0$ (i)

$x + y + z = -2y \Rightarrow x + 3y + z = 0$ (ii)

$x + 3y - z = -2z \Rightarrow x + 3y + z = 0$ (iii)

Now,

Coeff of x	Coeff of y	Coeff of z	Constant
2	-1	1	0
1	3	1	0
1	3	1	0

Date : / /

$$D = \begin{vmatrix} 2 & -1 & 1 \\ 1 & 3 & 1 \\ 1 & 3 & 1 \end{vmatrix} = 2\begin{vmatrix} 3 & 1 \\ 3 & 1 \end{vmatrix} - (-1)\begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} + 1\begin{vmatrix} 1 & 3 \\ 1 & 3 \end{vmatrix}$$

$$= 2(3-3) + 1(1-1) + 1(3-3)$$

$$= 2(0) + 0 + 0$$

$$\therefore D = 0$$

$$D_1 = \begin{vmatrix} 0 & -1 & 1 \\ 0 & 3 & 1 \\ 0 & 3 & 1 \end{vmatrix} = 0 - (-1)\begin{vmatrix} 0 & 1 \\ 0 & 1 \end{vmatrix} + 1\begin{vmatrix} 0 & 3 \\ 0 & 3 \end{vmatrix}$$

$$= 1(0-0) + 1(0-0)$$

$$\therefore D_1 = 0$$

$$D_2 = \begin{vmatrix} 2 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{vmatrix} = 2\begin{vmatrix} 0 & 1 \\ 0 & 1 \end{vmatrix} - 0 + 1\begin{vmatrix} 1 & 0 \\ 1 & 0 \end{vmatrix}$$

$$\therefore D_2 = 0$$

$$D_3 = \begin{vmatrix} 2 & -1 & 0 \\ 1 & 3 & 0 \\ 1 & 3 & 0 \end{vmatrix} = 2\begin{vmatrix} 3 & 0 \\ 3 & 0 \end{vmatrix} + 1\begin{vmatrix} 1 & 0 \\ 1 & 0 \end{vmatrix} + 0$$

$$\therefore D_3 = 0$$

$$\therefore x = \frac{D_1}{D} = \frac{0}{0}, \quad y = \frac{D_2}{D} = \frac{0}{0}, \quad z = \frac{D_3}{D} = \frac{0}{0}$$

So, the Eigen vector associated with $\lambda = -2$ is

$$V = \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Date : / /

b) $A = \begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix}$

Soln:

Given matrix

$$A = \begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix}$$

The characteristic equation of A is

$$|A - \lambda I| = 0$$

or, $$\left| \begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right| = 0$$

or, $$\left| \begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix} - \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix} \right| = 0$$

or, $$\begin{vmatrix} -1-\lambda & 2 & 2 \\ 2 & 2-\lambda & 2 \\ 3 & -6 & -6-\lambda \end{vmatrix} = 0.$$

or, $$(-1-\lambda)\begin{vmatrix} 2-\lambda & 2 \\ -6 & -6-\lambda \end{vmatrix} - 2\begin{vmatrix} 2 & 2 \\ 3 & -6-\lambda \end{vmatrix} + 2\begin{vmatrix} 2 & 2-\lambda \\ 3 & -6 \end{vmatrix} = 0$$

or, $(-1-\lambda)[(-6-\lambda)(2-\lambda)+12] - 2[2(-6-\lambda)-6] + 2[-12-3(2-\lambda)] = 0$

or, $(-1-\lambda)(-12+6\lambda-2\lambda+\lambda^2+12) - 2(-12-2\lambda-6) + 2(-12-6+3\lambda) = 0$

Date : / /

$\Rightarrow (-1-\lambda)(\lambda^2+4\lambda) - 2(-18-2\lambda) + 2(-18+3\lambda) = 0$

$\Rightarrow -\lambda^2 - 4\lambda - \lambda^3 - 4\lambda^2 + 36 + 12\lambda - 36 + 6\lambda = 0$

$\Rightarrow -\lambda^3 - 5\lambda^2 + 8\lambda = 0$

$\Rightarrow \lambda^3 + 5\lambda^2 + 8\lambda = 0$

$\Rightarrow \lambda^2 + 5\lambda + 6 = 0$

$\Rightarrow \lambda^2 + 3\lambda + 2\lambda + 6 = 0$

$\Rightarrow \lambda(\lambda+3) + 2(\lambda+3) = 0$

$\Rightarrow (\lambda+3)(\lambda+2) = 0$

Either, $\lambda+3 = 0$ or, $\lambda+2 = 0$

$\therefore \lambda = -3$ or, $\therefore \lambda = -2$

$\therefore$ Eigen Values are -2 and -3.

Next, for Eigen Vector.

Taking $\lambda = -2$

$AV = \lambda V$ [Where $V = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$]

$$\Rightarrow \begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = -2 \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} -x+2y+2z \\ 2x+2y+2z \\ 3x-6y-6z \end{bmatrix} = \begin{bmatrix} -2x \\ -2y \\ -2z \end{bmatrix}$$

Comparing both, we get

$-x+2y+2z = -2x \Rightarrow x+2y+2z = 0$ — (I)

$2x+2y+2z = -2y \Rightarrow 2x+4y+2z = 0$ — (II)

$3x-6y-6z = -2z \Rightarrow 3x-6y-4z = 0$ — (III)

Now,

Coeff of x	Coeff of y	Coeff of z	Constant
1	2	2	0
2	4	2	0
3	-6	-4	0

$$D = \begin{vmatrix} 1 & 2 & 2 \\ 2 & 4 & 2 \\ 3 & -6 & -4 \end{vmatrix} = 1\begin{vmatrix} 4 & 2 \\ -6 & -4 \end{vmatrix} - 2\begin{vmatrix} 2 & 2 \\ 3 & -4 \end{vmatrix} + 2\begin{vmatrix} 2 & 4 \\ 3 & -6 \end{vmatrix}$$

$$= 1(-16+12) - 2(-8-6) + 2(-12-12)$$
$$= -4 + 28 - 48$$
$$= -24$$

$$D_1 = \begin{vmatrix} 0 & 2 & 2 \\ 0 & 4 & 2 \\ 0 & -6 & -4 \end{vmatrix} = 0 - 2\begin{vmatrix} 0 & 2 \\ 0 & -4 \end{vmatrix} + 2\begin{vmatrix} 0 & 4 \\ 0 & -6 \end{vmatrix}$$
$$= 0 - 0 + 0$$
$$= 0$$

$$D_2 = \begin{vmatrix} 1 & 0 & 2 \\ 2 & 0 & 2 \\ 3 & 0 & -4 \end{vmatrix} = 1\begin{vmatrix} 0 & 2 \\ 0 & -4 \end{vmatrix} - 0 + 2\begin{vmatrix} 2 & 0 \\ 3 & 0 \end{vmatrix}$$
$$= 0$$

$$D_3 = \begin{vmatrix} 1 & 2 & 0 \\ 2 & 4 & 0 \\ 3 & -6 & 0 \end{vmatrix} = 1\begin{vmatrix} 4 & 0 \\ -6 & 0 \end{vmatrix} - 2\begin{vmatrix} 2 & 0 \\ 3 & 0 \end{vmatrix} + 0$$
$$= 0$$

$\therefore x = \frac{D_1}{D} = \frac{0}{-24} = 0$

$y = \frac{D_2}{D} = \frac{0}{-24} = 0$

$z = \frac{D_3}{D} = \frac{0}{-24} = 0$

$\therefore$ So, the Eigen vector associated with eigen

Date : / /

value $\lambda = -2$ is $V = \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$.

Again.
Taking $\lambda = -3$

$AV = \lambda V$

$$\Rightarrow \begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = -3 \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} -x+2y+2z \\ 2x+2y+2z \\ 3x-6y-6z \end{bmatrix} = \begin{bmatrix} -3x \\ -3y \\ -3z \end{bmatrix}$$

Comparing both, we get

$-x+2y+2z = -3x \Rightarrow 2x+2y+2z = 0 \Rightarrow x+y+z = 0$ — (i)

$2x+2y+2z = -3y \Rightarrow 2x+5y+2z = 0$ — (ii)

$3x-6y-6z = -3z \Rightarrow 3x-6y-3z = 0 \Rightarrow x-2y-z = 0$ — (iii)

Coeff of x	Coeff of y	Coeff of z	Constant
1	1	1	0
2	5	2	0
1	-2	-1	0

$$D = \begin{vmatrix} 1 & 1 & 1 \\ 2 & 5 & 2 \\ 1 & -2 & -1 \end{vmatrix} = 1 \begin{vmatrix} 5 & 2 \\ -2 & -1 \end{vmatrix} - 1 \begin{vmatrix} 2 & 2 \\ 1 & -1 \end{vmatrix} + 1 \begin{vmatrix} 2 & 5 \\ 1 & -2 \end{vmatrix}$$

$$= 1(-5+4) - 1(-2-2) + 1(-4-5)$$

$$= -1+4-9 = -6$$

$$D_1 = \begin{vmatrix} 0 & 1 & 1 \\ 0 & 5 & 2 \\ 0 & -2 & -1 \end{vmatrix} = 0 - 1\begin{vmatrix} 0 & 2 \\ 0 & -1 \end{vmatrix} + 1\begin{vmatrix} 0 & 5 \\ 0 & -2 \end{vmatrix}$$

$$= 0 - 0 + 0$$

$$= 0$$

$$D_2 = \begin{vmatrix} 1 & 0 & 1 \\ 2 & 0 & 2 \\ 1 & 0 & -1 \end{vmatrix} = 1\begin{vmatrix} 0 & 2 \\ 0 & -1 \end{vmatrix} - 0 + 1\begin{vmatrix} 2 & 0 \\ 1 & 0 \end{vmatrix}$$

$$= 0$$

$$D_3 = \begin{vmatrix} 1 & 1 & 0 \\ 2 & 5 & 0 \\ 1 & -2 & 0 \end{vmatrix} = 1\begin{vmatrix} 5 & 0 \\ -2 & 0 \end{vmatrix} - 1\begin{vmatrix} 2 & 0 \\ 1 & 0 \end{vmatrix} + 0$$

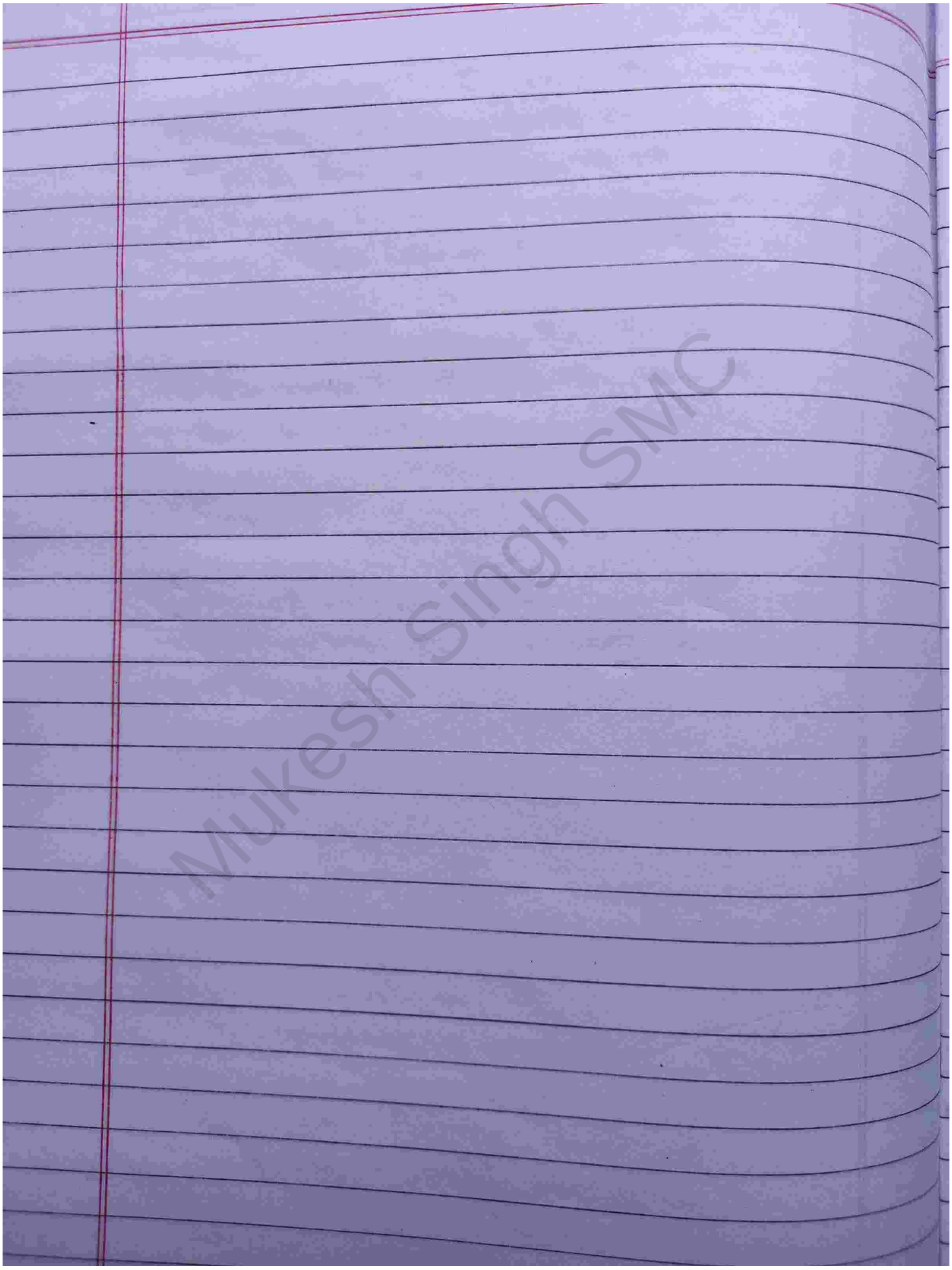
$$= 0$$

$$\therefore x = \frac{D_1}{D} = \frac{0}{-6} = 0$$

$$\therefore y = \frac{D_2}{D} = \frac{0}{-6} = 0$$

$$\therefore z = \frac{D_3}{D} = \frac{0}{-6} = 0$$

So, the Eigen vector associated with eigen value $\lambda = -3$ is $V = \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$.



Unit-7
Field Theory

Page No.:
Date : / /

7.1 Introduction

A commutative division ring is called a field.

OR, A commutative ring $(R, +, \cdot)$ with unit element is said to be a field if every non-zero element $a \in R$ has multiplicative inverse $a^{-1} \in R$.

Examples

1. $(R, +, \cdot)$ is field.
2. $(Q, +, \cdot)$ is field.
3. $(C, +, \cdot)$ is also field (set of all complex numbers.)
4. $(Z, +, \cdot)$ is not field.
5. The set of all 2×2 non-singular matrices is not field because it is not commutative.

Q. Show that J_5 of residue classes of integers modulo 5 is a field. (TU 2057)

Soln:

We have $J_5 = \{0, 1, 2, 3, 4\} \pmod 5$. So,

$+_{J_5}$	0	1	2	3	4
0	0	1	2	3	4
1	0	2	3	4	5
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

From the above table addition modulo 5 satisfies closure, associative and commutative properties.

Also 0 is an additive identity element. The

Date : / /

additive inverse of 1, 2, 3 and 4 are 4, 3, 2 and 1 respectively. So, $(J_5, +)$ is an abelian group.

Again,

$\times_{J_5}$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

From the above table, the multiplication modulo 5 satisfies associative and distributive properties. So, $(J_5, +, \times)$ form a ring. Also it is a commutative ring with unit element 1 and 1, 2, 3, 4 are the multiplicative inverse of 1, 3, 2, 4 respectively. Hence, J_5 is a field.

7.2 Subfield

A non-empty subset H of a field F is called a subfield of F if H itself forms a field with respect to the operations defined of F.

The field R of real numbers is a subfield of field of complex numbers and the field Q of rational numbers is also a subfield of real numbers.

~~The subfield~~

Example

Q is a subfield of R.
R is subfield of C.

Proper Subfield:

A subfield Q of a field F is called proper subfield of F if Q ≠ F.

7.3 Prime field

A field F is called prime field if it has no proper subfields.

If E be an extension of a field F, then obviously, E is a vector space over F. The dimension of E over F is usually denoted by [E:F].

If [E:F] is finite then E is called finite extension of F otherwise E is called an infinite extension field.

Example

$\mathbb{C}$ except imaginary number $= \mathbb{R}$.

$\therefore \mathbb{R}$ is prime field of $\mathbb{C}$ except imaginary number.

7.4 Fidd extension and degree of field ~~extension~~ extension

Field extension / Extension field:

The super field of a field is called an extension field of the field.

For example:

The field of complex numbers is an extension field of field of rational numbers and field of real numbers.

The subfield $\mathcal{G}$ of field F is called a proper subfield of F if $\mathcal{G} = F$.

Degree ~~/dimension~~ of ~~ext~~ field extension

Number of ~~member~~/elements in a field is called degree of field extension.

Examples of Degree of field extension:

① $\mathcal{G} = \{\frac{1}{2}, \frac{3}{4}, 1, -5, -\frac{7}{5}\}$ ② $F = \{1, 2, 5, 7, 10, 15, 20\}$

$d(F) = 7$ (finite)

$d(\mathcal{G}) = 5$ (finite)

3) $\mathcal{G} = \{\frac{1}{2}, \frac{3}{2}, \frac{5}{2} \cdots\}$ 4) $F = \{1, 2, 5, \cdots\}$

$d(\mathcal{G}) = \infty$ (infinite) $d(F) = \infty$ (infinite)

Page No.:
Date: / /

Dimension = degree:

E is vector space over F.
The dimension of E over F $\Rightarrow [E:F]$

If E is finite, $[E:F]$, E is finite dimension over F.

If E is infinite, $[E:F]$, E is infinite dimension over F.

Page No.:
Date : / /

Prove the theorems of Extension of field:

Theorem 1

The necessary and sufficient conditions for a non-empty subset H of field F to be a subfield of F are:

(i) $a-b \in H \ \forall\ a,b \in H$

(ii) $ab^{-1} \in H \ \forall\ a, b(\neq 0) \in H$

Proof:

Let H be a subfield of F then.

H is a ~~sub~~group under addition.

If $a,b \in H \Rightarrow a-b \in H \Rightarrow$

By closure property, $a+(-b) = a-b \in H$.

Since, H is a group then if $a \in H \Rightarrow a^{-1} \in H$

By closure property, $a.b^{-1} \in H$

Conversely,

H is non-empty subset of F and $a-b \in H$ & $ab^{-1} \in H \ \forall\ a,b \in H$.

Let, $a \in H$, $a-a \in H \Rightarrow 0 \in H$. (identity)

Since, $-a \in H \Rightarrow 0+(-a) = -a \in H$ (inverse)

Let $a,b \in H$ then $-b \in H \Rightarrow a+(-b) = a+b \in H$ (closure)

Since, the commutativity of associativity are satisfied in F. So, they are also satisfied in H.

Thus, H is abelian group.

Page No.:
Date : / /

Now, let $(a \neq 0) \in H$, then ~~$b \in H$~~ $aa^{-1} \in H$
$\Rightarrow$ $1 \in H$ (identity) · multiplicative identity
If $a = 1$ then $aa^{-1} \in H \Rightarrow 1a^{-1} \in H \Rightarrow a^{-1} \in H$
multiplicative (inverse)

Let $a, b (\neq 0) \in H$. So, $b^{-1} \in H \Rightarrow a(b^{-1})^{-1} = ab \in H$
(closure satisfied)

Since, the commutativity, associativity and distributivity are satisfied in F. So they are also satisfied in H.
Hence H is a subfield of F.

Theorem 2
L be a finite extension of F and H is subfield of L which contains F then $[H:F] / [L:F]$.

~~Proof~~
Let L, H, F are three fields satisfying $F \subseteq H \subseteq L$.
Let, $[L:F]$ is finite (say n).
Let $\{v_1, v_2, \ldots, v_n\}$ be a basis of L over F.
Then $\{v_1, v_2, \ldots, v_n\}$ generates L over F.

Since $F \subseteq H$ then any linear combination of $v_1, v_2, \ldots, v_n$ over F will also be a linear combination of $v_1, v_2, \ldots, v_n$ over H.
This shows that $\{v_1, v_2, \ldots v_n\}$ also generates L over H i.e. L_K also a finite dimensional vector space over H. And $[L:H]$ is finite.

Page No.:
Date : / /

Hence, $[L:F] = [H:F] \Rightarrow [H:F] \mid [L:F]$.

$= [H:F]$ $[F \subseteq H \subseteq L]$

i.e $[L:F] = [H:F] \Rightarrow [H:F] [L:F]$

7.5 Algebraic and transcendal elements

Algebraic element of a field

An element $u \in E$ (where E is an extension of a field F) is said to be algebraic over F if there is a non-zero polynomial $f(x) \in F[x]$ such that $f(u) = 0$.

OR

Let, $u \in E$, $[E:F]$ ∃ non-zero polynomial $f(x) \in F(x)$ such that $f(u) = 0$, then u is called algebraic element of F.

Transcendal element of a field:

If the element u is not algebraic then it is called transcendal element.

Example

$[c:R]$, if $0 \in C$ then, $f(x) = 3x^2 + 2x \in F(x)$ is

If $f(0) = 3x.0^2 + 2x0 = 0$

$\therefore 0$ is algebraic element.

Otherwise,

Transcendal element.

e.g. $[R:\mathbb{Q}]$ has transcendal element.