2 LINEAR ALGEBRA

1. Linear Algebra : Matrices, Vectors, Determinants, Linear Systems of Equations

Linear algebra—Includes the theory and applications of linear systems of equations, linear transformations and eigen value problems.

Matrix—A rectangular arrays of numbers. They are useful because they enable us to consider an array of many numbers as a single object and help us to perform calculations with these single object in a very compact form. 'A mathematical 'Shorthand.'

• Basic Concepts : Matrix Addition, Scalar Multiplication

Matrix—A rectangular arrays of numbers (or functions) enclosed in brackets. These numbers (or functions) are called entries or elements of the matrix.

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} \ldots\ldots a_{1n} \\ a_{21} & a_{22} \ldots\ldots a_{2n} \\ \vdots & \\ a_{m1} & a_{m2} \ldots\ldots a_{mn} \end{bmatrix}$$

In the double subscript notation a_{ij}, the first subscript denotes the row and second subscript the column, in which the given entry stands.

Order of matrix—$(m \times n)$ matrix : m-rows and n-columns.

Square matrix—If $m = n$, then A is $n \times n$ square matrix.

Diagonal (main)/ principal diagonal—The diagonal containing $a_{11}, a_{22}, \ldots\ldots a_{nn}$.

Rectangular matrix—A matrix which is not square.

Vectors—*Row vector* : matrix having one row $(1 \times n)$

Column vector : matrix having one column $(m \times 1)$

Transposition—Interchanging row and columns. If A is $m \times n$ matrix $[a_{ij}]$

Then transpose of A, A^T is $n \times m$ matrix $[a_{ji}]$

Symmetric matrix—A square matrix :

$A^T = A$

Skew-symmetric matrix—A square matrix :

$A^T = -A$

(1) $A = [a_{ij}]$, square matrix.

A is symmetric iff $a_{ij} = a_{ji}\ \forall\ i, j$

A is skew-symmetric iff $a_{ij} = -a_{ji}, \forall\ i, j$

A is skew-symmetric $\Rightarrow a_{ii} = 0$. Diagonal elements are zero

(2) For every square matrix A, the matrix $A + A^T$ is symmetric, the matrix $A - A^T$ is skew-symmetric.

(3) Every square matrix can be written as a sum of skew-symmetric and symmetric matrices.

Equality of matrix—Two matrices $A = [a_{ij}]$ and $B = [b_{ij}]$ are equal *i.e.*, A = B,

if—

(i) They are of same order

(ii) The corresponding entries are equal,

$a_{ij} = b_{ij}\ \forall\ i, j$

Matrix addition—The addition of two matrices $A = [a_{ij}]$ and $B = [b_{ij}]$ is A + B,

if—

(i) They are of same order

(ii) $A + B = [a_{ij} + b_{ij}]$, *i.e.*, adding corresponding entries.

Scalar multiplication—The product of any matrix $A = [a_{ij}]$ by a scalar c is $cA = c[a_{ij}] = [ca_{ij}]$, *i.e.*, multiplying each entry by c.

Zero matrix—A matrix with all entries zero.

Some Important Theorem

1. For the matrix A, B, C of same order.

$$A + B = B + A$$ abelian

Associative $$(A + B) + C = A + (B + C) = A + B + C$$

$$A + 0 = A$$ – Identity

$$A + (-A) = 0$$ – Inverse.

2. Multiplying by scalar c, k

$$c(A + B) = cA + cB$$

$$(c + k)A = cA + kA$$

$$(ck)A = c(kA) = ckA$$

$$1A = A.$$

3. $(A + B)^T = A^T + B^T$

$$(cA)^T = cA^T.$$

- **Matrix Multiplication :** $[a]_{m\times n}$ $[b_{ij}]_{n\times p}$

(1) The product C = AB of two matrix A and B is defined iff number of columns of A = number of rows of B.

(2) If $A = [a_{ij}]$ is $m \times p$

$B = [b_{ij}]$ is $p \times n$ then, $C = [c_{ij}]$ is $(m \times n)$

where, $C_{ij} = \sum_{l=1}^{p} a_{il}\, b_{lj}$

$i = 1……m$

$j = 1……n.$

(3) i-row of A and j-column of B will produce c_{ij} entry.

(4) Matrix multiplication is not commutative, AB ≠ BA in general.

(5) AB = 0 does not necessary implies A = 0 or B = 0 or BA = 0.

(6) AC = AD does not necessary implies C = D (even when A ≠ 0).

(7) In C = AB

A is postmultiplied by B.

B is premultiplied by A.

Some Important Results

1. $k(AB) = (kA)B = A(kB)$, for some scalar k
2. $A(BC) = (AB)C$
3. $(A + B)C = AC + BC$ } distributive
4. $C(A + B) = CA + CB$

Triangular matrix—

Upper triangular matrix— A square matrix that have all entries below diagonal are zero. $a_{ij} = 0$, $i > j$.

Lower triangular matrix— A square matrix that have all entries above diagonal are zero, $a_{ij} = 0$, $i < j$.

Diagonal matrix—Square matrix having non-zero entries only on diagonal any entry above and below diagonal are zero.

$$\text{diag}\,(a_{11}, a_{22}, a_{33}, \ldots\ldots a_{nn}),\ (a_{ij} = 0,\ i \neq j)$$

Scalar matrix—If all the entries of main diagonal matrix are equal (say) c.

$$\text{diag}\,(a_{11}, a_{22}, a_{33}, \ldots, a_{nn})$$

$$\text{where } a_{ij} = \begin{cases} 0 & i \neq j \\ c & i = j \end{cases}$$

Identity matrix (Unit matrix)—Scalar matrix, whose entries of main diagonal are all one.

AI = IA = A.

Transpose of a product—$(AB)^T = B^T A^T$.

Inner product—If $a = [a_1 \ldots a_n]$ and $b = [b_1 \ldots b_n]^T$

$$a \cdot b = \sum_{l=1}^{n} a_l\, b_l = a_1\, b_1 + a_2\, b_2 + \ldots\ldots + a_n\, b_n.$$

Product in terms of row and column vectors—

$A = [a_1 \ldots a_n]$, where $a_i = [a_{i1}, a_{i2}, \ldots\ldots a_{ip}]$

$B = [b_1 \ldots b_n]^T$, where $b_j = [b_{1j}, b_{2j}, \ldots\ldots b_{pj}]^T$

$C = AB = [c_{ij}]$ $c_{ij} = a_i \cdot b_j$

Idempotent matrix : $A^2 = A$

Nilpotent matrix : $A^m = 0$ for some integer m.

2. Linear Systems of Equations

Linear system of m equations in n unknowns $x_1, \ldots x_n$ is the set of equations

$$a_{11}\, x_1 + a_{12}\, x_2 + \ldots\ldots + a_{1n}\, x_n = b_1$$
$$a_{21}\, x_1 + a_{22}\, x_2 + \ldots\ldots + a_{2n}\, x_n = b_2$$
$$\vdots \qquad\qquad \vdots$$
$$a_{m1}\, x_1 + a_{m2}\, x_2 + \ldots\ldots + a_{mn}\, x_n = b_m$$

Here a_{ij} are called coefficients (which are given numbers)

(1) If all b_j ($j = 1, \ldots m$) are zero then **homogeneous** system.

(2) If atleast one b_j ($j = 1, \ldots m$) is not zero then **non-homogeneous.**

(3) **Solution**—Set of numbers $x_1 \ldots\ldots x_n$, which satisfies all m-equations.

(4) **Solution vector**—Ordered Set of numbers $[x_1 \ldots\ldots x_n]$ which satisfies all m-equations.

(5) If the above is homogeneous system, then it has atleast one trival solution.

$$x_1 = x_2 = x_3 = \ldots\ldots = x_n = 0$$

Matrix representation—$Ax = b$

$$\text{where,} \quad A = \begin{bmatrix} a_{11} \ldots\ldots a_{in} \\ : \quad\quad : \\ a_{m1} \ldots\ldots a_{mn} \end{bmatrix}_{(m \times n)}$$

$$x = [x_1 \ldots x_n]^T \text{ and } b = [b_1 \ldots b_m]^T$$

Augmented matrix—

$$\tilde{A} = \begin{bmatrix} a_{11} \ldots\ldots a_{in} & b_1 \\ : & : \\ a_{m1} \ldots a_{mn} & b_m \end{bmatrix}$$

$$= [a_{ij}, b_i]$$

The Augumented matrix $\tilde{A}$ determines the system completely because it contains all given numbers given in linear system of equations.

3. Rank of Matrix : Linear Independence and Dependence

Let $\bar{a}_1, \bar{a}_2, \ldots\ldots, \bar{a}_m$ are m-vectors, then

Linear combination of m-vectors: $c_1\bar{a}_1 + c_2 \bar{a}_2 + \ldots\ldots + c_m \bar{a}_m = \sum_{i=1}^{m} c_i \bar{a}_i$.

where, $c_1 \ldots\ldots c_m$ are any scalars.

Linearly independent vectors— If $\sum_{i=1}^{m} c_i \bar{a}_i = \bar{0}$, when all c_i's are zero. then $(\bar{a}_1, \ldots\ldots, \bar{a}_m)$ are linearly independent vectors.

Linearly dependent vectors— If $\sum_{i=1}^{m} c_i \bar{a}_i = \bar{0}$, for some c_i's may be zero, then $(\bar{a}_1, \ldots\ldots, \bar{a}_m)$ are linearly dependent vectors.

Sub-matrix—A matrix obtained from a matrix, by omitting rows and columns.

Rank of a matrix—The maximum number of linearly independent row vectors of a matrix $A = [a_{jk}]$ is called the rank of A or (rank A).

Nullity of a matrix : If A is a square matrix of order n then nullity of matrix A,

$$N(A) = n - \text{rank } A.$$

Some Important Theorems

1. The rank of a matrix A equals the maximum number of linearly independent columns vectors of A.
2. Matrix A and its transpose A^T have same rank.
3. Row-equivalent matrix have the same rank.
4. p-vectors $\bar{a}_1, \bar{a}_2, \ldots\ldots, \bar{a}_p$ are linearly independent if the matrix with row vectors $(\bar{a}_1, \bar{a}_2, \ldots\ldots, \bar{a}_p)$ has rank p. The vectors are linearly dependent if that rank is less than p.
5. Rank $(A^T B^T)$ = Rank (BA)
6. Rank of the product of two matrices cannot exceed the rank of either factor.

4. Solutions of Linear Systems

Given a linear system (non-homogeneous system) of m-equations in n-unknowns $x_1 \ldots\ldots x_n$.

$$a_{11} x_1 + a_{12} x_2 + \ldots\ldots\ldots + a_{1n} x_n = b_1$$
$$a_{21} x_1 + a_{22} x_2 + \ldots\ldots\ldots + a_{2n} x_n = b_2$$
$$: \qquad\qquad :$$
$$a_{m1} x_1 + a_{m2} x_2 + \ldots\ldots\ldots + a_{mn} x_n = b_m$$

(A) Existence of solution—This system has solution iff the coefficient matrix A and augmented matrix $\tilde{A}$ of it have same rank.

$$A = \begin{bmatrix} a_{11} \ldots\ldots a_{1n} \\ : \\ a_{m1} \ldots\ldots a_{mn} \end{bmatrix}, \text{ and}$$

$$\tilde{A} = \begin{bmatrix} a_{11} \ldots a_{1n} & : b_1 \\ : & : \; : \\ : & : \; : \\ a_{m1} \ldots a_{mn} & : b_m \end{bmatrix}$$

i.e. Rank A = Rank $\tilde{A}$.

(B) Uniqueness of solution—This system has precisely one solution iff

$$\text{Rank } A = \text{Rank } \tilde{A} \Rightarrow r = n$$

(C) Infinitely many solutions—If this rank, $r < n$, the system have infinitely many solutions. These can be obtained by determining r-suitable unknown in terms of remaining $n-r$ unknowns, to which arbitrary values can be assigned.

(D) Homogeneous system—If all b_i's ($i = 1 \ldots m$) are zero. Otherwise non-homogeneous.

(a) A homogeneous system has the *trival solution* $x_1 = 0, \ldots\ldots, x_n = 0$, if rank A = n.

(b) A homogeneous system has the *non-trival solution* iff rank A < n.

(c) A homogeneous linear system with fewer equations then unknowns always has non-trival solutions.

(D') Non-Homogeneous system—If a non-homogeneous linear system have a solution, then all the solutions are of the form $\bar{x} = \bar{x}_0 + \bar{x}_A$,

where x_0 is any fixed solution and $\bar{x}_A$ are all the solutions obtained from homogeneous linear systems.

5. Determinants

The ***n*-order determinant** of a square matrix $A = [a_{ij}]$ of order n, is a number,

$$\begin{aligned} \text{det. } A &= |A| = |a_{ij}| \\ &= a_{j1}\, c_{j1} + \ldots\ldots + a_{jn}\, c_{jn}, \quad j = 1, 2, \ldots \text{ or } n \\ &= a_{1k}\, c_{1k} + \ldots\ldots + a_{nk}\, c_{nk}, \quad k = 1, 2, \ldots \text{ or } n \end{aligned}$$

where, $c_{jk} = (-1)^{j+k} M_{jk}$

$= $ *Co-factor* of a_{ik} in $|A|$

and, $m_{jk} =$ Determinant of order $(n-1)$, obtained by deleting the rows and columns of entry a_{jk} (*i.e.* j-th row and k-th column).

$=$ *minor* of a_{jk} in $|A|$.

Geometrically,

det A = ± volume of the n-dimensional parallelopiped spanned by the column (or row) vectors of A.

For $n = 2$

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}\, a_{22} - a_{12}\, a_{21}$$

For $n = 3$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

For Triangular Matrix—

$$|A| = |a_{ij}| = a_{11}\, a_{22} \ldots\ldots a_{nn}$$

i.e., product of diagonal entries.

Some Properties of Determinants

Let A be a determinant of order n

1. det A^T = det A
2. $|AB| = |A|\,|B|$
3. det $A^{-1} = 1/\text{det } A$
4. det I = 1
5. det $(xA) = x^n$ det A
6. det A $= \lambda_1 \ldots\ldots \lambda_n$ = product of eigen values.
7. If all elements of a row (or column) are multiplied by constant k, then determinant is multiplied by k.
8. Exchange of two rows (or columns) change the sign of the determinant.
9. Determinant does not change if one row (or column) multiplied by a constant is added to another row (or column)
10. Determinant equals to zero, if
    (a) All elements of a row (column) are zero, or
    (b) Two rows (columns) coincide.

Rank of a matrix in terms of determinant—An $m \times n$ matrix $A = [a_{ij}]$ has rank $r \geq 1$ iff A has $r \times r$ sub-matrix with non-zero determinant.

If A is square matrix of order n, its rank is n iff det A ≠ 0.

Cramer's Theorem (Solution of linear system by determinants)

(a) If a linear system of n-equations has the same number of unknowns $x_1, x_2, \ldots\ldots, x_n$.

$$\begin{aligned} a_{11}\, x_1 + a_{12}\, x_2 + \ldots\ldots\ldots + a_{1n}\, x_n &= b_1 \\ a_{21}\, x_1 + a_{22}\, x_2 + \ldots\ldots\ldots + a_{2n}\, x_n &= b_2 \\ &\vdots \\ a_{n1}\, x_1 + a_{n2}\, x_2 + \ldots\ldots\ldots + a_{nn}\, x_n &= b_n \end{aligned}$$

$$\Leftrightarrow \bar{A}\,\bar{x} = \bar{b}$$

$A = \text{diag}(a_{11}, a_{22} \ldots a_{nn})$

$A^{-1} = \text{diag}\left(\frac{1}{a_{11}}, \frac{1}{a_{22}} \ldots \frac{1}{a_{nn}}\right)$ $\bar{A}^T = A^{-1}$ unitary

has a non-zero coefficient determinant D = det A, the system has precisely one solution. This solution is given by the formulas

$$x_1 = \frac{D_1}{D}, x_2 = \frac{D_2}{D}, \ldots, x_n = \frac{D_n}{D} \text{ (Cramer's Rule)}$$

where D_k is the determinant obtained from D by replacing in D the k-th column by the column with entries $b_1 \ldots\ldots b_n$.

If the system is homogeneous and $D \neq 0$, then it has only the trival solution $x_1 = 0, x_2 = 0, \ldots\ldots, x_n = 0$.

If D = 0, the homogeneous system also have non-trival solutions.

6. Inverse of Matrix

If A is a square matrix, then inverse of A, A^{-1} exist if $AA^{-1} = A^{-1}A = I$.

A^{-1} exist $\Leftrightarrow$ det $A \neq 0$

$\Leftrightarrow$ A is non-singular matrix

$\Leftrightarrow$ Columns (rows) of A are linearly independent.

Calculation of A^{-1}

(a) $A^{-1} = \frac{1}{\det A}[A_{ij}]^T$, where A_{ij} is the cofactor of a_{ij} in det A

(b) By Gauss Jordan method

$$[AI] = \begin{bmatrix} a_{11}\ldots & a_{1n} & 1\,0\,0\ldots0 \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ a_{n1}\ldots & a_{nn} & \ldots\ldots\ldots1 \end{bmatrix} \sim \begin{bmatrix} 1\,0\,0\ldots & b_{11}\ldots & b_{1n} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \ldots\ldots\ldots1 & a_{n1}\ldots & b_{nn} \end{bmatrix}$$

$$= [I\,B]$$

then $B = A^{-1}$

(c) If $A = \text{diag}(a_{11}, \ldots\ldots a_{nn})$

then $A^{-1} = \text{diag}\left(\frac{1}{a_{11}}, \ldots\ldots, \frac{1}{a_{nn}}\right)$

7. Symmetric, Skew-Symmetric and Orthogonal Matrix

Symmetric matrix—A real square matrix is symmetric, if—

$$A^T = A, \text{ i.e. } a_{kj} = a_{jk}$$

Skew-symmetric matrix—A real square matrix is skew-symmetric, if—

$$A^T = -A, \text{ i.e. } a_{kj} = -a_{jk}$$

Orthogonal matrix—A real square matrix is orthogonal, if—

$$A^T = A^{-1}.$$

Some Important Theorems

1. Matrix A is symmetric $\Rightarrow$
   (a) All eigen values are real
   (b) Eigen vectors corresponding to different eigen values are orthogonal.
2. Matrix A is skew-symmetric
   $\Rightarrow$ Eigen values are pure, imaginary or zero.
   $\Rightarrow$ Main diagonal entries are zero.
3. Matrix A is orthogonal $\Rightarrow$
   Eigen values are real or complex conjugates in pairs and have absolute value 1.

Hermitian, Skew-Hermitian, unitary—

If $A = [a_{jk}]$ is a complex matrix, its *Complex Conjugate* is $\bar{A} = [\bar{a}_{jk}]$

Hermitian matrix—A square matrix $A = [a_{kj}]$ is hermitian, if—

$$\bar{A}^T = A, \text{ i.e., } \bar{a_{kj}} = a_{jk}$$

Skew-hermitian—A square matrix $A = [a_{kj}]$ is skew-Hermitian,

$$\bar{A}^T = -A, \text{ i.e., } \bar{a_{kj}} = -a_{jk}$$

Unitary—A square matrix A is unitary, if–

$$\bar{A}^T = A^{-1}$$

Some Important Results

1. Matrix A is Hermitian $\Rightarrow$ main diagonal entries are real.
2. Matrix A is skew-Hermitian $\Rightarrow$ main diagonal entries are pure imaginary or zero.
3. Eigen values for—
   (a) Hermitian and symmetric matrix are real.
   (b) Skew-Hermitian and skew-symmetric are pure imaginary or zero.
   (c) Unitary and orthogonal matrix have absolute value.

$A^{-1} = diag(\frac{1}{a_{11}}, \frac{1}{a_{22}} \cdots \frac{1}{a_{nn}})$. $\bar{A}^T = A^{-1}$ unitary

has a non-zero coefficient determinant D = det A, the system has precisely one solution. This solution is given by the formulas

$$x_1 = \frac{D_1}{D}, x_2 = \frac{D_2}{D}, \ldots, x_n = \frac{D_n}{D} \text{ (Cramer's Rule)}$$

where D_k is the determinant obtained from D by replacing in D the k-th column by the column with entries $b_1 \ldots\ldots b_n$.

If the system is homogeneous and $D \neq 0$, then it has only the trival solution $x_1 = 0, x_2 = 0, \ldots\ldots, x_n = 0$.

If D = 0, the homogeneous system also have non-trival solutions.

6. Inverse of Matrix

If A is a square matrix, then inverse of A, A^{-1} exist if $AA^{-1} = A^{-1}A = I$.

A^{-1} exist $\Leftrightarrow$ det $A \neq 0$

$\Leftrightarrow$ A is non-singular matrix

$\Leftrightarrow$ Columns (rows) of A are linearly independent.

Calculation of A^{-1}

(a) $A^{-1} = \frac{1}{\det A}[A_{ij}]^T$, where A_{ij} is the cofactor of a_{ij} in det A

(b) By Gauss Jordan method

$$[AI] = \begin{bmatrix} a_{11}\ldots & a_{1n} & 1\,0\,0\ldots 0 \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ a_{n1}\ldots & a_{nn} & \ldots\ldots\ldots 1 \end{bmatrix} \sim \begin{bmatrix} 1\,0\,0\ldots & b_{11}\ldots & b_{1n} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \ldots\ldots\ldots 1 & a_{n1}\ldots & b_{nn} \end{bmatrix}$$

$$= [I\ B]$$

then $B = A^{-1}$

(c) If $A = \text{diag}(a_{11}, \ldots\ldots a_{nn})$

then $A^{-1} = \text{diag}\left(\frac{1}{a_{11}}, \ldots\ldots, \frac{1}{a_{nn}}\right)$

7. Symmetric, Skew-Symmetric and Orthogonal Matrix

Symmetric matrix—A real square matrix is symmetric, if—

$$A^T = A, \text{ i.e. } a_{kj} = a_{jk}$$

Skew-symmetric matrix—A real square matrix is skew-symmetric, if—

$$A^T = -A, \text{ i.e. } a_{kj} = -a_{jk}$$

Orthogonal matrix—A real square matrix is orthogonal, if—

$$A^T = A^{-1}.$$

Some Important Theorems

1. Matrix A is symmetric $\Rightarrow$
   (a) All eigen values are real
   (b) Eigen vectors corresponding to different eigen values are orthogonal.
2. Matrix A is skew-symmetric
   $\Rightarrow$ Eigen values are pure, imaginary or zero.
   $\Rightarrow$ Main diagonal entries are zero.
3. Matrix A is orthogonal $\Rightarrow$
   Eigen values are real or complex conjugates in pairs and have absolute value 1.

Hermitian, Skew-Hermitian, unitary—

If $A = [a_{jk}]$ is a complex matrix, its *Complex Conjugate* is $\bar{A} = [\bar{a}_{jk}]$

Hermitian matrix—A square matrix $A = [a_{kj}]$ is hermitian, if—

$$\bar{A}^T = A, \text{ i.e., } \bar{a_{kj}} = a_{jk}$$

Skew-hermitian—A square matrix $A = [a_{kj}]$ is skew-Hermitian,

$$\bar{A}^T = -A, \text{ i.e., } \bar{a_{kj}} = -a_{jk}$$

Unitary—A square matrix A is unitary, if–

$$\bar{A}^T = A^{-1}$$

Some Important Results

1. Matrix A is Hermitian $\Rightarrow$ main diagonal entries are real.
2. Matrix A is skew-Hermitian $\Rightarrow$ main diagonal entries are pure imaginary or zero.
3. Eigen values for—
   (a) Hermitian and symmetric matrix are real.
   (b) Skew-Hermitian and skew-symmetric are pure imaginary or zero.
   (c) Unitary and orthogonal matrix have absolute value.

8. Characteristic Value and Characteristic Vectors

Let $A = [\bar{a}_{jk}]$ is square matrix of order n, and given a equation $A\bar{x} = \lambda\bar{x}$, where vector $\bar{x}$ and scalar λ are unknown.

(a) Zero vector $\bar{x} = 0$, is solution for all λ.

(b) When $\bar{x} \neq 0$, The value of λ for which $A\bar{x} - \lambda\bar{x} = \bar{0} \Leftrightarrow (A - \lambda)\,\bar{x} = \bar{0}$ has the solution is called *characteristic value* (or root) of A and corresponding $\bar{x} \neq \bar{0}$ is called *Characteristic vector of* A, corresponding to λ.

The characteristic equation—

λ is an eigen value of A $\Leftrightarrow$ det $(A - \lambda I)$

$$= \begin{vmatrix} a_{11}-\lambda a_{12}\ldots\ldots\ldots a_{1n} \\ a_{21} \quad a_{22}-\lambda\ldots\ldots a_{2n} \\ \vdots \\ a_{n1}\ldots\ldots\ldots\ldots a_{mn}-\lambda \end{vmatrix} = 0,$$

det $A = \lambda_1 \ldots \lambda_n$ (product of all eigen values)

trace $A = \lambda_1 \ldots + \lambda_n$ (sum of all eigen values).

9. Quadratic Forms

Given $A = [a_{ij}]$, a square matrix of order n and $\bar{x} = (x_1, \ldots\ldots, x_n)$, then the *quadratic form for* A is

$$Q(\bar{x}) = \bar{x}^T A \bar{x}.$$

$Q(\bar{x}) = \bar{x}^T A \bar{x}$ is

(a) Positive definite, if $Q(\bar{x}) > 0, \bar{x} \neq 0$ $\Leftrightarrow$ all eigen values $\lambda > 0 \Leftrightarrow |A| > 0$.

(b) Positive semi-definite, if $Q(\bar{x}) \geq 0 \Leftrightarrow$ all eigen values $\lambda \geq 0$.

(c) Indefinite, if Q assumes positive and negative values $\Leftrightarrow$ A has positive and negative eigen values.

(d) Negative definite $\Leftrightarrow Q(\bar{x}) < 0, \bar{x} \neq 0 \Leftrightarrow$ all eigen values $\lambda > 0 \Leftrightarrow -Q(\bar{x})$ are positive definite.

10. Basis of Eigen Vectors

Linear independence of eigen vectors—Let $\lambda_1\ldots\ldots, \lambda_k$ be k-distinct eigen-values of square matrix of order n, then corresponding eigen vectors $x_1, \ldots\ldots, x_k$ form a linearly independent set.

Basis of eigen vectors—If n-order square matrix has n-distinct eigen values, then A has a basis of eigen vectors for $\mathbb{C}^n$ (or $\mathbb{R}^n$). Where $\mathbb{C}$ (and $\mathbb{R}$) are set of complex (and real) numbers.

Diagonalization of matrix—If n-order square matrix A has a basis of eigen vector, then $D = X^{-1} A X$ is diagonal, with the eigen values of A as the entries on the main diagonal. Here X is the matrix with these eigen vectors as column vectors.

11. Linear Spaces

Vector spaces—A set L of elements $\bar{x}, \bar{y}, \bar{z}, \ldots\ldots$ are called linear space or vector space (on $\mathbb{L}$) if addition and multiplication by scalars are defined so that the following laws are satisfied for all $\bar{x}, \bar{y}, \bar{z} \in L$ and $\lambda, \mu \in \mathbb{R}$.

I. (i) $\bar{x}, \bar{y} \in L \Rightarrow \bar{x} + \bar{y} \in L$

(ii) $\bar{x} + \bar{y} = \bar{y} + \bar{x}$ (Abelian law)

(iii) $(\bar{x} + \bar{y}) + \bar{z} = \bar{x} + (\bar{y} + \bar{z})$ (Associative)

(iv) $\exists\, \bar{0} : \bar{x} + \bar{0} = \bar{x}$ (Identity with add.)

(v) $\exists -\bar{x} : \bar{x} + (-\bar{x}) = \bar{0}$ (Inverse)

II. (i) $\lambda\bar{x} \in L$

(ii) $\lambda(\mu\bar{x}) = (\lambda\mu)\,\bar{x}$

(iii) $(\lambda + \mu)\,\bar{x} = \lambda\bar{x} + \mu\bar{x}$

(iv) $\lambda(\bar{x} + \bar{y}) = \lambda\bar{x} + \lambda\bar{y}$

(v) $1\bar{x} = \bar{x}$

(vi) $\overline{0x} = \bar{0}$

(vii) $\lambda\,\bar{0} = \lambda$

Test for subspace—A non-empty subset M of L is a linear space itself, if—

1. $\bar{x}, \bar{y} \in M \Rightarrow \bar{x} + \bar{y} \in M$
2. $\bar{x} \in M, \lambda \in \mathbb{R} \Rightarrow \lambda\bar{x} \in M$

Linear combinations, basis—

1. The vector $\bar{y}$ is a linear combination of vectors $\bar{x}_1, \ldots, \bar{x}_n$, if $\bar{y} = \lambda_1\bar{x}_1 + \lambda_2\bar{x}_2 + \ldots\ldots + \lambda_n\bar{x}_n$ for some scalars $\lambda_1 \ldots \lambda_n$.

2. The linear hull LH $(x_1 \ldots\ldots x_n)$ is $\{y : y = \lambda_1 x_1 \ldots\ldots + \lambda_n x_m, \lambda_i \in \mathbb{R}\}$

3. Vectors $\bar{x}_1 \ldots\ldots \bar{x}_n$ are

(a) Linearly independent, if $\lambda_1\bar{x}_1 + \lambda_2\bar{x}_2 + \ldots + \lambda_n \bar{x}_n = \bar{0} \Rightarrow \lambda i = 0$, all i

(b) Linearly dependent, if $\exists\ \lambda_1 \ldots\ldots \lambda_n$ not all zero :

$\lambda_1\bar{x}_1 + \lambda_2\bar{x}_2 + \ldots + \lambda_n \bar{x}_n = \bar{0}$

($\Leftrightarrow$ some $\bar{x}_i$ is a linear combination of the other)

4. $\bar{e}_1, \bar{e}_1 \ldots \bar{e}_n$ is a basis of the linear space L and L is n-dimensional, if—

(i) $\bar{e}_1, \ldots\ldots, \bar{e}_n$ are linearly independent.

(ii) Every $\bar{x} \in$ L can be written uniquely,

$x = x_1\bar{e}_1 + x_2\bar{e}_2 + \ldots\ldots + x_n\bar{e}_n$

12. Scalar Product

1. Let L be a linear space, A scalar product $(\bar{x}, \bar{y})$ is a function L $\times$ L$\rightarrow \mathbb{R}$ with the following properties holding for all $\bar{x}, \bar{y}, \bar{z} \in$ L and $\lambda, \mu \in \mathbb{R}$—

(a) $(\bar{x}, \bar{y}) = (\bar{y}, \bar{x})$

(b) $(\bar{x}, \lambda\bar{y} + \mu\bar{z}) = \lambda(\bar{x}, \bar{y}) + \mu(\bar{x}, \bar{z})$

(c) $(\bar{x}, \bar{x}) \geq 0, (\bar{x}, \bar{x}) = 0 \Leftrightarrow \bar{x} = 0$

2. Length of $\bar{x}$: $|\bar{x}| = \sqrt{(\bar{x}, \bar{x})}$,

$|c\bar{x}| = (c)|\bar{x}|$ (c scalar)

3. $|(\bar{x}, \bar{y})| \leq |\bar{x}|\ |\bar{y}|$ (Cauchy-Schwarz inequality).

4. $|\bar{x} + \bar{y}| \leq |\bar{x}| + |\bar{y}|$ (Triangle inequality).

13. Orthonormal Basis

Let L be an n-dimensional linear space with scalar product (Euclidean space)

1. A basis $\bar{e}_1, \ldots, \bar{e}_n$ is called orthonormal basis, if— $\bar{e}_i.\bar{e}_j = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$

2. $\bar{e}_1, \ldots \bar{e}_n$ are orthonormal basis,

$$\bar{x} = \sum_{k=1}^{n} x_k \bar{e}_k \text{ and } \bar{y} = \sum_{k=1}^{n} y_k \bar{e}_k$$

then

$$x_k = \bar{x} \cdot \bar{e}_k$$

$$|\bar{x}|^2 = \sum_{k=1}^{n} x_k^2$$

$$\bar{x} \cdot \bar{y} = \sum_{k=1}^{n} x_k y_k$$

14. Orthogonal Component

M subspace of L : $M^{\perp} = \{\bar{y} \in L : (\bar{x}, \bar{y}) = 0$, all $\bar{x} \in M\}$

Orthogonal projection—M subspace, $\bar{e}_1, \ldots \bar{e}_m$ orthonormal basis of M

x^{-1} is the orthogonal projection of $\bar{x}$ on M, if—

$\bar{x} = \bar{x}' + \bar{x}'', \bar{x}' \in M, x'' \in M^{\perp}$.

15. The Space $\mathbb{R}^n$

The set of all column vectors $\bar{x} = (x_1 \ldots x_n)^T$ is called $\mathbb{R}^n$, The natural choice of orthonormal basis of $\mathbb{R}^n$ is the set of vectors $\bar{e}_1 = (1, 0, 0, \ldots)^T$, $\bar{e}_2 = (0, 1, 0, \ldots\ldots 0)^T \ldots\ldots \bar{e}_n = (0, 0, \ldots, 0, 1)^T$ *i.e.*

$\bar{x} = x_1\bar{e}_1 + x_2\bar{e}_2 + \ldots\ldots + x_n\bar{e}_n$, x_n any scalar.

Addition $\bar{x} + \bar{y} = (x_1 \ldots x_n)^T + (y_1 \ldots y_n)^T = (x_1 + y_1, x_2 + y_2, \ldots\ldots, x_n + y_n)^T$.

Multiplication by a scalar $c\bar{x} = c(x_1, x_2, \ldots x_n)^T = (cx_1, cx_2, \ldots c\, x_n)^T$

Scalar product $\bar{x} \cdot \bar{y} = x_1 y_1 + x_2 y_2 + \ldots\ldots + x_n y_n = \bar{x}^T \bar{y}$.

Length or Norm $|\bar{x}| = \sqrt{x^T x} = \sqrt{x_1^2 + \ldots\ldots x_n^2}$

$|c\bar{x}| = |c|\, |\bar{x}|$

Pythagoras theorem

$\bar{x} \cdot \bar{y} = 0 \Leftrightarrow |\bar{x} + \bar{y}|^2 = |x|^2 + |y|^2$

Cauchy's Schwarz' inequality

$|\bar{x} \cdot \bar{y}| \leq |\bar{x}| + |\bar{y}|$

The triangle inequality $|\bar{x} + \bar{y}| \leq |\bar{x}| + |\bar{y}|$

Angle between $\bar{x}$ and $\bar{y}$: $\cos\theta = \dfrac{\bar{x} \cdot \bar{y}}{|\bar{x}|\ |\bar{y}|}$

PART–B
LINEAR ALGEBRA (1)

1. Let A be the matrix of order $m \times n$, then the determinant of A exist iff—
(A) $m > n$ (B) $m < n$
(C) $m \neq n$ (D) $m = n$

2. If matrix A and B commute, then—
(A) $(AB)^n = A^nB^n$ (B) $(AB)^n = AB$
(C) $(AB)^n = B^n$ (D) None of these

3. If I is an identity matrix, then—
(A) $I^n = I$ (B) $I^n = 0$
(C) $I^n = 1/I$ (D) None of these

4. If A and B are two matrix of same order, then the follow operation does not holds.
(A) $A + B = B + A$
(B) $AB = BA$
(C) $A - B = - B + A$
(D) $(A + B)I = A + B$

5. A real quadratic form $X^T A X$ is positive definite, if—
(A) All eigen values of $A > 0$
(B) All eigen values of $A < 0$
(C) All eigen values of $A = 0$
(D) None of these

6. A real quadratic form $X^T A X$ is positive semidefinite, if—
(A) All eigen values of $A \geq 0$
(B) All eigen values of $A \leq 0$
(C) All eigen values of $A = 0$
(D) None of these

7. The eigen values of the matrix $\begin{bmatrix} 1 & 1 & 3 \\ 1 & 5 & 1 \\ 3 & 1 & 1 \end{bmatrix}$ is—
(A) +2, 3, 6 (B) 2, 6, 7
(C) – 2, 3, 6 (D) None of these

8. If A is a square matrix, then A^{-1} exist iff—
(A) $|A| = 0$ (B) $|A| \neq 0$
(C) $|A| > 0$ (D) $|A| < 0$

9. The matrix $A = [a_{ij}]$ is Hermitian iff—
(A) $a_{ij} = -\bar{a}_{ji}$ for all i, j
(B) $a_{ij} = \bar{a}_{ji}$ for all i, j
(C) $a_{ij} = a_{ji}$ for all i, j
(D) None of these

10. The diagonal elements of Hermitian matrix are—
(A) Complex number
(B) Real numbers
(C) Natural numbers
(D) None of these

11. The diagonal elements of Skew-Hermitian matrix are—
(A) Pure real numbers or zero
(B) Pure imaginary or zero
(C) Complex number
(D) None of these

12. The matrix $\begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$ is a—
(A) Hermitian matrix
(B) Skew-Hermitian matrix
(C) Symmetric matrix
(D) Skew-Symmetric matrix

13. The matrix $\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ is a—
(A) Hermitian matrix
(B) Skew-Hermitian
(C) Skew-Symmetric
(D) Symmetric

14. If A is a Hermitian matrix, then iA is—
(A) Hermitian (B) Skew-Hermitian
(C) Symmetric (D) Skew-Symmetric

15. If A is a square matrix, and $A^2 = A$, then A is—
(A) Hermitian matrix
(B) Idempotent matrix
(C) Symmetric matrix
(D) None of these

16. If A and B are idempotent matrix, then AB is idempotent, if—
(A) $AB = BA$ (B) $(AB)^T = B^T A^T$
(C) $AB \neq BA$ (D) None of these

17. If A is Skew-Hermitian matrix, then iA is—
(A) Hermitian (B) Skew-Hermitian
(C) Symmetric (D) Skew-Symmetric

18. If A and B are idempotent matrix, then A + B will be idempotent, iff—
(A) AB = BA = zero matrix
(B) AB = zero matrix
(C) BA = zero matrix
(D) None of these

19. The square matrix A is nilpotent if—
(A) $A^m = I$, m any positive integer
(B) $A^m = 0$ for any +ve integer
(C) $A^m = A$
(D) None of these

20. The square matrix A is involutary matrix if—
(A) $A^2 = I$ (B) $A^2 = 0$
(C) $A^2 = A$ (D) None of these

21. A square matrix A is Orthogonal if—
(A) $AA^T \neq I$ (B) $AA^T = A^T A = I$
(C) $AA^T = O$ (D) None of these

22. The square real matrix A is called unitary if—
(A) $AA^T = A^T A = I$ (B) $AA^T \neq I$
(C) $A^T A = O$ (D) None of these

23. The diag (1, 1, ……1) is—
(A) Idempotent matrix
(B) Rectangular matrix
(C) Non-Symmetric matrix
(D) None of these

24. If A is non-singular matrix, then—
(A) $(A^{-1})^{-1} = I$ (B) $(A^{-1})^{-1} = A^{-1}$
(C) $(A^{-1})^{-1} = A$ (D) None of these

25. The following statement is true—
(A) $(A^T)^{-1} = (A^{-1})^T$ (B) $(A^T)^{-1} = (A^T)$
(C) $(A^T)^{-1} = A^{-1}$ (D) None of these

26. The Conjugate matrix of matrix $\begin{bmatrix} 1-i & 2 \\ i & 1+i \end{bmatrix}$ is—
(A) $\begin{bmatrix} 1-i & 2 \\ 1+i & i \end{bmatrix}$ (B) $\begin{bmatrix} 1+i & 2 \\ -i & 1-i \end{bmatrix}$
(C) $\begin{bmatrix} 2 & 1-i \\ 1+i & i \end{bmatrix}$ (D) $\begin{bmatrix} 1+i & i \\ 2 & 1-i \end{bmatrix}$

27. The Tranjugate of a matrix $\begin{bmatrix} 1+i & i \\ 2 & 1-i \end{bmatrix}$ is—
(A) $\begin{bmatrix} 1-i & 2 \\ -i & 1+i \end{bmatrix}$ (B) $\begin{bmatrix} 1+i & 2 \\ i & 1-i \end{bmatrix}$
(C) $\begin{bmatrix} i & 2 \\ 1-i & 1+i \end{bmatrix}$ (D) $\begin{bmatrix} 1-i & 2 \\ 3 & 2-i \end{bmatrix}$

28. If in a matrix A, two columns are interchanged and we obtain matrix B, then—
(A) $|A| = |B|$ (B) $|A| = -|B|$
(C) $|A| = \frac{1}{|B|}$ (D) None of these

29. If A^T is a transpose of square matrix A, then—
(A) $|A^T| = 1/|A|$ (B) $|A^T| = -|A|$
(C) $|A^T| = |A|$ (D) None of these

30. If two rows of a matrix A are identical, then—
(A) $|A| = 0$ (B) $|A| = 1$
(C) $|A| \neq 0$ (D) None of these

31. If A is any n-order square matrix and k is any scalar, then—
(A) $|kA| = k^n |A|$ (B) $|kA| = k|A|$
(C) $|kA| = k^2|A|$ (D) None of these

32. Expansion of the matrix $\begin{vmatrix} 1 & z & -y \\ -z & 1 & x \\ y & -x & 1 \end{vmatrix}$ gives?
(A) $1 + x + y + z$ (B) $1 + x^2 + y^2 + z^2$
(C) $1 + xyz$ (D) None of these

33. The value of the determinant $\begin{vmatrix} 0 & c & b \\ -c & 0 & a \\ -b & -a & 0 \end{vmatrix}$ is—

(A) Zero (B) bc

(C) abc (D) None of these

34. If the matrix B is obtained from the matrix A by interchanging two rows, then—

(A) $|B| = |A|$ (B) $|B| = -|A|$

(C) $|B| = \frac{1}{|A|}$ (D) None of these

35. If B is the matrix obtained from A, by changing rows into columns and columns into row, then—

(A) $|A| = |B|$ (B) $|A| \neq |B|$

(C) $|A| = -|B|$ (D) None of these

36. If row vectors of a square matrix A are linearly dependent, then—

(A) $|A| = 0$ (B) $|A| \neq 0$

(C) $|A| = C$ (D) None of these

37. If A is a square matrix, then—

(A) (adj A) A = |A| I, where I an identity matrix

(B) (adj A) A = |A|

(C) (adj A) A = I

(D) None of these

38. If $|A| \neq 0$, then—

(A) $|\text{adj } A| = |A|^{n-1}$ (B) $|\text{adj } A| = |A|^n$

(C) $|\text{adj } A| = 0$ (D) None of these

39. A square matrix A is singular if—

(A) $|A| = 0$ (B) $|A| \neq 0$

(C) $|A| = 1$ (D) None of these

40. If A, B, C are three matrix, then—

(A) $|ABC| = |A|\ |B|\ |C|$

(B) $|ABC| = |AB|\ C$

(C) $|ABC| = |A|\ |BC|$

(D) None of these

41. If row vectors of a non-zero square matrix A are linearly independent, then—

(A) $|A| = 0$ (B) $|A| \neq 0$

(C) $|A| = n$ (D) None of these

42. If A and B are two square matrix of same order—

(A) $|AB| = |BA|$ (B) $|AB| \neq |B|\ |A|$

(C) $|AB| \neq |BA|$ (D) None of these

43. If I_n is an identity matrix of order n, and k any scalar—

(A) $\text{adj}(kI_n) = kI_n$

(B) $\text{adj}(k\,I_n) = k^n\,I_n$

(C) $\text{adj}(k\,I_n) = k^{n-1}\,I_n$

(D) None of these

44. If A is a Symmetric matrix, then—

(A) adj A is a Non-Symmetric matrix

(B) adj A is a Symmetric matrix

(C) adj A is does not exist

(D) None of these

45. Let I_n be an Identity matrix of order n, then—

(A) $\text{adj } I_n = I_n$ (B) $\text{adj } I_n = 0$

(C) $\text{adj } I_n = n\,I_n$ (D) None of these

46. Every Skew-Symmetric matrix of odd order is—

(A) Singular (B) Non-singular

(C) Identity (D) None of these

47. If matrix A have inverse B and C, then—

(A) $B \neq C$

(B) $B = C$

(C) $B = nC$, for any n

(D) None of these

48. The square matrix A have an inverse iff—

(A) $|A| \neq 0$ (B) $|A| = 0$

(C) $|A| > 1$ (D) $|A| < 1$

49. If A and B are two non-singular matrix of same order, then—

(A) $(AB)^{-1} = B^{-1} A^{-1}$

(B) $(AB)^{-1} = A^{-1} B^{-1}$

(C) $(AB)^{-1} = AB$

(D) None of these

50. The following vectors $\left(\frac{1}{4}, 0, -\frac{1}{4}\right), \left(\frac{1}{3}, -\frac{1}{3}, 0\right)$ and $\left(0, \frac{1}{2}, -\frac{1}{2}\right)$ are—

(A) Linearly independent

(B) Linearly dependent

(C) Constant

(D) None of these

51. The following vectors (1, 9, 9, 8), (2, 0, 0, 8) and (2, 0, 0, 3) are—

(A) Linearly dependent

(B) Linearly independent

(C) Constant
(D) None of these

52. The following vectors (– 4, 2), (9, 1) and (5, 3) are—
(A) Linearly dependent
(B) Linearly independent
(C) Constant
(D) None of these

53. The following vectors (0, 5, –1), (–3, 8, 16) and (9, 56, –64) are—
(A) Linearly independent
(B) Linearly dependent
(C) Constant
(D) None of these

54. Let $m \equiv$ rank of matrix A and $n \equiv$ number of linearly independent columns vector of matrix A, then—
(A) $m < n$ (B) $m > n$
(C) $m \le n$ (D) None of these

55. If two vectors $\bar{a_1}$ and $\bar{a_2}$ are linearly dependent, then—
(A) $\bar{a_1} = c\bar{a_2}$, for some c
(B) $\bar{a_1} \neq c\bar{a_2}$, for some c
(C) $\bar{a_1} > c\bar{a_2}$, for some c
(D) None of these

56. If any of the vector from m-vectors $\bar{a_1}, \bar{a_2}, \ldots \ldots \bar{a_m}$, can be expressed as linear combination of the rest $(m-1)$ vectors, then m-vectors are—
(A) Linearly independent
(B) Linearly dependent
(C) Constant
(D) None of these

57. The unit vector are—
(A) Linearly dependent
(B) Linearly independent
(C) Zero vectors
(D) None of these

58. Let A and B are two equivalent matrix, then—
(A) Rank A = rank B
(B) Rank A ≠ rank B
(C) Rank A > rank B
(D) None of these

59. Let A be a matrix of order $m \times n$ and non-singular matrix of order n, then—
(A) Rank (RA) ≠ rank (A)
(B) Rank (RA) ≥ rank (A)
(C) Rank (RA) ≤ rank (A)
(D) Rank (RA) = rank (A)

60. Given $A\bar{x} = \bar{b}$, then the solution of system exists, if—
(A) Rank (A) ≠ rank [A, b]
(B) Rank A = rank b
(C) Rank (A) = rank [A; b]
(D) None of these

61. For given $A\bar{x} = \bar{b}$, where order of A is n have unique solution, if—
(A) Rank A ≠ rank [A; b] = n
(B) Rank A = rank [A; b] ≠ n
(C) Rank A = rank [A; b] = n
(D) None of these

62. If A is a $(n \times 1)$ non-zero matrix and B $(1 \times n)$ non-zero matrix, then—
(A) Rank (AB) = 1 (B) Rank (AB) = n
(C) Rank (AB) = 0 (D) None of these

63. The rank of the matrix $A = \begin{bmatrix} 0 & i & -i \\ -i & 0 & i \\ i & -i & 0 \end{bmatrix}$ is—
(A) 1 (B) 2
(C) 3 (D) 4

64. The rank of the matrix $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 2 & 1 & 2 \end{bmatrix}$ is—
(A) 1 (B) 2
(C) 3 (D) 4

65. The rank of matrix, whose every element is unity, is—
(A) Greater than one (B) Equals to one
(C) Zero (D) None of these

66. Let A be a square matrix of order n, then nullity of A is—
(A) n-rank A (B) Rank A – n
(C) n + rank A (D) None of these

67. If I is an unit matrix of order n, then—
(A) Rank (I) = n (B) Rank (I) ≥ n
(C) Rank (I) ≤ n (D) None of these

4 ALGEBRA

1. Numbers

Counting numbers (Natural numbers)—1, 2, 3, 4,...

Even numbers—Divisible by 2, 2, 4, 6, 8,...

Old numbers—Not divisible by 2, 1, 3, 5, 7, 9,...

Prime numbers—Number greater than one and whose only divisors are one and number itself, 2, 3, 5, 7, 11, 13,...

Composite numbers—4, 6, 8, 9, 10, 12,...

The integers in this chapter are denoted by a, b, c, d, n, m etc.

2. Fundamental Theorems of Arithmetic

Principle of induction—If $\mathbf{Z}$ is a set of integers such that

(a) $1 \in \mathbf{Z}$

(b) $n \in \mathbf{Z} \Rightarrow n + 1 \in \mathbf{Z}$ then

(c) All integers ≥ 1 belongs to $\mathbf{Z}$.

Well ordering principle—If A is a non-empty set of positive integers, then A contains a smallest member.

Divisibility—$d|n$ (d divides n) $\Rightarrow n = cd$, for some c.

Common divisor—If $d|a$ and $d|b$ then d is common divisor of a and b.

Greatest common divisor—If $d|a$ and $d|b$ and for every $e|a$ and $e|b \Rightarrow e|d$ then d is greatest common divisor of a and b, denoted by $(a, b) = d$.

Relative prime—a and b are relative prime if $|(a, b) = 1$.

Prime number—An integer n is prime if $n>1$ and if the only positive divisors of n are 1 and n.

Composite number—If $n > 1$ and n is not prime, then n is composite number.

Some Important Theorems

1. Divisibility has the following properties : For integers n, m, d, a and b
   - (a) $n|n$ (reflexive)
   - (b) $d|n$ and $n|m \Rightarrow d|m$ (transitive)
   - (c) $d|n$ and $d|m \Rightarrow d|(an + bm)$, for some a, b (linearity)
   - (d) $d|n \Rightarrow ad|an$ (multiplication property)
   - (e) $ad|an$ and $a \neq 0 \Rightarrow d|n$ (cancellation)
   - (f) $1|n$ (one divides every integer)
   - (g) $n|0$ (every integer divides zero)
   - (h) $0|n \Rightarrow n = 0$ (zero divides only zero)
   - (i) $d|n$ and $n \neq 0 \Rightarrow |d| \leq |n|$ (comparison)
   - (j) $d|n$ and $n|d \Rightarrow |d| = |n|$
   - (k) $d|n$ and $d \neq 0 \Rightarrow (n/d)|n$
2. Given any two integers a and b, there is common divisor d of a and b of the form $d = ax + by$, where x and y are integers. Moreover every common divisor of a and b divides this d.
3. Given integer a and b, there is one and only one number d such that
   - (a) $d \geq 0$
   - (b) $d|a$ and $d|b$
   - (c) $e|a$ and $e|b \Rightarrow e|d$
4. The gcd has the following properties :
   - (a) $(a, b) = (b, a)$
   - (b) $(a, (b, c)) = ((a, b), c)$
   - (c) $(ac, bc) = |c|\,(a, b)$
   - (d) $(a, 1) = (1, a) = 1$
     $(a, 0) = (0, a) = |a|$
5. **Euclid's lemma**—If $a|bc$ and if $(a, b) = 1$, then $a|c$.
6. Every integer $n > 1$ is either a prime number or a product of prime numbers.
7. **Euclid**—There are infinitely many prime numbers.
8. If prime p does not divides a than $(p, a) = 1$.
9. If prime p divides ab then $p|a$ or $p|b$.
10. If prime p divides a product $a_1\, a_2 \ldots a_n$ then p divides atleast one of the factors.
11. **Fundamental theorem of arithmetic**—Every integer $n > 1$ can be represented as a product of prime factors in only one way, apart from the order of the factors.
12. **Division algorithm**—Given integers a and b with $b > 0$, there exists a unique pair of integers q and r such that $a = bq + r$, $0 \leq r < b$. moreover $r = 0$ iff $b|a$, here q is quotient and r remainder.

3. Linear Diophantine Equations

A linear equation $ax + by = c$, with $a \neq 0$, $b \neq 0$ and c integers is called a linear Diophantine equation in two unknown x and y.

Solution of linear Diophantine equation—A pair of integers x_0, y_0 is called a solution of $ax + by = c$ if $ax_0 + by_0 = c$.

1. Let $a \neq 0$, $b \neq 0$ and c be any three integers and $d = (a, b)$. The linear Diophantine equation $ax + by = c$ has a solution iff $d|c$.
2. If x_0, y_0 is any particular solution of $ax + by = c$ then any other solution of this equation is $x' = x_0 - \frac{b}{d}t$, $y' = y_0 + \frac{a}{d}t$, t being any integer.
3. The Diophantine equation $y^2 = x^3 + k$ has no solution if k has the form $k = (4n - 1)^3 - 4m^2$, where m and n are integers such that no prime $p \equiv -1 \pmod 4$ divides m.

4. Congruences

$a \equiv b \pmod m$—Given integers a, b, m with $m > 0$, a is congruent to b modulo m, $[a \equiv b \pmod m]$, if m divides the difference $a - b$. The number m is called modulus of the congruence.

1. $a \equiv 0 \pmod m$ iff $m|a$.
2. $a \equiv b \pmod m$ iff $(a - b) \equiv 0 \pmod m$.
3. Congruence is an equivalence relation.
   - (a) $a \equiv a \pmod m$ (reflexivity).
   - (b) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ (symmetry)
   - (c) $a \equiv b \pmod m$ and $b \equiv c \pmod m$ $\Rightarrow a \equiv c \pmod m$ (transitivity).
4. If $a \equiv b \pmod m$ and $\alpha \equiv \beta \pmod m$ then
   - (a) $ax + \alpha y \equiv bx + \beta y \pmod m$ for all integers x and y.
   - (b) $a\alpha \equiv b\beta \pmod m$.
   - (c) $a^n \equiv b^n \pmod m$ for every positive integer n.
   - (d) $f(a) \equiv f(b) \pmod m$ for every polynomial f with integer coefficients.
5. If $c > 0$ then $a \equiv b \pmod m$ iff $ac \equiv bc \pmod{mc}$.
6. **Cancellation law**—If $ac \equiv bc \pmod m$ and $d = (m, c)$ then $a \equiv b \left(\mathrm{mod}\ \frac{m}{d}\right)$.
7. Assume $a \equiv b \pmod m$. If $d|m$ and $d|a$ then $d|b$.
8. If $a \equiv b \pmod m$ then $(a, m) = (b, m)$.
9. If $a \equiv b \pmod m$ and if $0 \leq |b - a| < m$ then $a = b$.
10. $a \equiv b \pmod m$ iff a and b give the same remainder when divided by m.
11. $a \equiv b \pmod m$ and $a \equiv b \pmod n$ where $(m, n) = 1$, $a \equiv b \pmod{mn}$.

Residue class a modulo m—

$\hat{a} = \{x \mid x \equiv a \pmod m\}$.

Complete residue system modulo m—A set of m representatives, one from each of the residue classes $\hat{1}, \hat{2}, \ldots, \hat{m}$.

Some Important Theorems

1. For some given modulus m,
   - (a) $\hat{a} = \hat{b}$ iff $a \equiv b \pmod m$
   - (b) Two integers x and y are in some residue class iff $x \equiv y \pmod m$
   - (c) The m residue classes $\hat{1}, \hat{2}, \ldots, \hat{m}$ are disjoint and their union is the set of all integers.

2. Assume $(k, m) = 1$. If $(a_1, \ldots, a_m)$ is a complete residue system modulo m, so is $\{ka_1, \ldots, ka_m\}$.

5. Linear Congruences

Solution of congruence—A integer x satisfying a polynomial congruence $f(x) \equiv 0 \pmod{m}$ is called a solution of the congruence.

1. Assume $(a, m) = 1$. Then the linear congruence $ax \equiv b \pmod{m}$ has exactly one solution.
2. Assume $(a, m) = d$. Then the linear congruence $ax \equiv b \pmod{m}$ has solution iff $d|b$.
3. Assume $(a, m) = d$ and $d|b$. Then the linear congruence $ax \equiv b \pmod{m}$ has exactly d solutions modulo m. These are given by
$t, t + \frac{m}{d}, t + \frac{2m}{d}, \ldots, t + (d-1)\frac{m}{d}$, where t is the solution, unique modulo m/d, of the linear congruence $\frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right)$.
4. If $(a, b) = d$ there exist integers x and y such that $ax + by = d$.

6. Reduced Residue System

Reduced residue system modulo m—It is a set of $\phi(m)$ integers, incongruent modulo m, each of which is relatively prime to m.

Here $\phi(m)$ is Euler's totient.

Some Important Theorems

1. If $\{a_1, a_2, \ldots, a_{\phi(m)}\}$ is a reduced residue system modulo m and if $(k, m) = 1$, then $\{ka_1, ka_2, \ldots, ka_{\phi(m)}\}$ is also a reduced residue system modulo m.
2. **Euler-Fermat theorem**—Assume $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.
3. If a prime p does not divide a then
$$a^{p-1} \equiv 1 \pmod{p}.$$
4. **Little Fermat theorem**—For any integer a and any prime p we have $a^p \equiv a \pmod{p}$.
5. If $(a, m) = 1$ the solution (unique mod m) of the linear congruence $ax \equiv b \pmod{m}$ is given by $x \equiv b\, a^{\phi(m)-1} \pmod{m}$.

Lagrange's Theorem

1. **Lagrange's theorem**—Given a prime p, let
$$f(x) = c_0 + c_1 x + \ldots\ldots + c_n x^n$$
be a polynomial of degree n with integer coefficients such that $c_n \not\equiv 0 \pmod{p}$. Then the polynomial congruence, $f(x) \equiv 0 \pmod{p}$, has at most n solutions.
2. If $f(x) = c_0 + c_1 x + \ldots + c_n x^n$ is a polynomial of degree n with integer coefficients, and if the congruence $f(x) \equiv 0 \pmod{p}$, has more than n solutions, where p is prime, then every coefficient of f is divisible by p.
3. For any prime p all the coefficients of the polynomial
$f(x) = (x-1)(x-2)\ldots(x-p+1) - x^{p-1} + 1$
are divisible by p.
4. **Wilson's theorem**—For any prime p, $(\lfloor p-1) \equiv (-1) \pmod{p}$.
5. **Wolstenholme's theorem**—For any prime $p \geq 5$, we have
$$\left(\sum_{k=1}^{p-1} \frac{\lfloor p-1}{k}\right) \equiv 0 \pmod{p^2}$$

7. Chinese Remainder Theorem

1. **Chinese Remainder theorem**—Assume $m_1, m_2, \ldots, m_r$ are positive integers, relatively prime in pairs : $(m_i, m_k) = 1$ if $i \neq k$.
Let $b_1, b_2, \ldots, b_r$ be arbitrary integers. Then the system of congruences
$$x \equiv b_1 \pmod{m_1}$$
$$\vdots$$
$$x \equiv b_r \pmod{m_r}$$
has exactly one solution modulo the product $m_1 \ldots m_r$.
2. Assume $m_1, \ldots, m_r$ are relatively prime in pairs. Let $b_1, \ldots, b_r$ be arbitrary integers and let $a_1, \ldots, a_r$ satisfy $(a_k, m_k) = 1$ for $k = 1, 2, \ldots, r$. Then the linear system of congruences
$$a_1 x \equiv b_1 \pmod{m_1}$$
$$\vdots$$
$$a_r x \equiv b_r \pmod{m_r}$$
has exactly one solution modulo $m_1 m_2 \ldots m_r$
3. Let f be a polynomial with integer coefficients, let $m_1, m_2, \ldots, m_r$ be positive integers relatively prime in pairs and let $m = m_1 m_2 \ldots m_r$. Then the congruence
$$f(x) \equiv 0 \pmod{m} \quad \ldots(i)$$
has a solution iff each of the congruences,
$$f(x) \equiv 0 \pmod{m_i},\ i = 1, 2, \ldots, r \quad \ldots(ii)$$
has a solution. Moreover if $v(m)$ and $v(m_i)$ denote the number of solutions of (i) and (ii) respectively, then $v(m) = v(m_1)\, v(m_2) \ldots v(m_r)$.
4. The set of lattice points in the plane visible from the origin contains arbitrarily large square gaps. That is, given any integer $k > 0$, there exists a lattice point (a, b) such that none of the lattice points,
$(a + r, b + s)$, $0 < r \leq k$, $0 < s \leq k$
is visible from the origin.

8. Quadratic Residues

Quadratic residue mod p—If congruence $x^2 \equiv n \pmod{p}$ has a solution then n is a quadratic residue mod p denoted by (nRp).

If $x^2 \equiv n \pmod{p}$ has no solution, then n is quadratic nonresidue mod p denoted by $(n\bar{R}p)$.

Legendre's symbol—Let p be an odd prime. If $n \not\equiv 0 \pmod{p}$ then Legendre's symbol, $(n|p)$ is
$$(n|p) = \begin{cases} +1 & \text{if } nRp \\ -1 & \text{if } n\bar{R}p \end{cases}$$
If $\quad n \equiv 0 \pmod{p}$ then $(n|p) = 0$

Jacobi symbols—If P is a positive odd integer with prime factorization $P = \prod_{i=1}^{r} p_i^{a_i}$. Then Jacobi symbol $(n|P)$ for all integer is
$$(n|P) = \prod_{i=1}^{r} (n|p_i)^{a_i},$$
where $(n|p_i)$ is Legendre symbol and $(n|1) = 1$.

Some Important Theorems

1. If p is an odd prime. Then every reduced residue system mod p contains exactly $(p-1)/2$ quadratic residues and exactly $(p-1)/2$ quadratic nonresidues mod p. The quadratic residues belong to the residue classes containing the numbers,
$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$
2. **Euler's criterion**—If p is an odd prime. Then for all n we have $(n|p) \equiv n^{(p-1)/2} \pmod{p}$.
3. Legendre's symbol $(n|p)$ is a completely multiplicative function of n.
4. For every odd prime p,
$$(-1|p) = (-1)^{(p-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv 3 \pmod{4} \end{cases}$$
5. For every odd prime p,
$$(2|p) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8} \\ -1, & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$
6. **Gauss lemma**—Assume $n \not\equiv 0 \pmod{p}$ and consider the least positive residues mod p of the following $(p-1)/2$ multiples of n :
$$n, 2n, 3n, \ldots, \frac{p-1}{2}n.$$
If m denotes the number of these residues which exceed $p/2$ then $(n|p) = (-1)^m$.
7. If m is the number defined in Gauss lemma, then
$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] + (n-1)\frac{p^2-1}{8} \pmod{2}$$
If n is odd then
$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] \pmod{2}.$$
8. **Quadratic reciprocity law**—If p and q are distinct odd primes, then
$(p|q)(q|p) = (-1)^{(p-1)(q-1)/4}$.
9. If P and Q are odd positive integers, then
   (a) $(m|P)(n|P) = (mn|P)$
   (b) $(n|P)(n|Q) = (n|PQ)$
   (c) $(m|P) = (n|P)$ whenever $m \equiv n \pmod{P}$
   (d) $(a^2 n|P) = (n|P)$ whenever $(a, P) = 1$.
10. If P is an odd positive integer, then
$(-1|P) = (-1)^{(P-1)/2}$ and $(2|P) = (-1)^{(P^2-1)/8}$.
11. **Reciprocity law for Jacobi symbols**—If P and Q are positive odd integers with $(P, Q) = 1$, then $(P|Q)(Q|P) = (-1)^{(P-1)(Q-1)/4}$.

9. Gauss Sum

$$G(n, \chi) = \sum_{r \bmod p} \chi(r)\, e^{2\pi i n r/p}$$

where $\chi(r) = (r|p)$ is the quadratic character mod p.

Some Important Theorems

1. If p is an odd prime and $\chi(r) = (r|p)$ then $G(1, \chi)^2 = (-1|p)p$.
2. If p and q be distinct odd primes and let χ be the quadratic character mod p. Then the quadratic reciprocity law
$$(q|p) = (-1)^{(p-1)(q-1)/4}\,(p|q)$$
is equivalent to congruence
$$G(1, \chi)^{q-1} \equiv (q|p) \pmod q.$$
3. If p and q are distinct odd primes and if χ is the character mod p, then
$$G(1, \chi)^{q-1} = (q|p) \sum_{r_1 \bmod p} \cdots \sum_{r_q \bmod p} (r_1 \ldots r_q|p)$$
$$r_1 + r_2 + \ldots\ldots + r_q \equiv q \pmod p.$$
4. If the product ma is even, then
$$S(a, m) = \sqrt{\frac{m}{a}}\left(\frac{1+i}{\sqrt{2}}\right)\overline{S(m, a)}$$
where $S(a, m) = \sum_{r=0}^{m-1} e^{\pi i a r^2/m}$ and bar denotes complex conjugate.

10. Representation of Integers as Sum of Squares

Sum of two squares—

1. No integer of the form $4k + 3$ is the sum of two squares.
2. If each m and n are sum of two squares, then there product mn is also a sum of two squares.
3. **Thue's lemma**—Let p be a prime and a an integer, which is coprime to p. Then the linear congruence $ax \equiv y \pmod p$ has the solution (x_0, y_0) such that $0 < |x_0| < \sqrt{p}$ and $0 < |y_0| < \sqrt{p}$.
4. **Fermat's lemma**—An odd prime p can be represented as a sum of two squares iff $p \equiv 1 \pmod 4$.
5. A positive integer $n > 1$ can be represented as sum of two squares iff either n has no prime factor congruent to 3 (mod 4) or if it has a prime factor congruent to 3(mod 4) then it occurs to an even power in the prime factorization of n.
6. Every odd prime is the difference of two squares in one and only one way.

Sum of three or more squares—

1. Any integer of the form $4^n(8m + 7)$ integers $m, n \geq 0$ is not a sum of three squares.
2. If p is a prime number. Then there exist integers a, b, c atleast of which are non-zero such that
$$a^2 + b^2 + c^2 \equiv 0 \pmod p.$$
3. **Eulers lemma**—If each of two positive integers m and n is a sum of four squares, then their product mn is also a sum of four squares.
4. Any prime number p can be written as sum of four non-negative squares.
5. **Lagranges theorem**—Every integer > 1 can be represented as the sum of four non-negative squares.
6. **Aubry theorem**—There are infinitely many primes each of which is a sum of three distinct squares.

Arithmetical function—A real or complex valued function defined on the positive integers is called an arithmetical function.

Möbius function—The Möbius function μ is defined as
$$\mu(1) = 1$$
If $n > 1$, write $n = p_1^{a_1} \ldots\ldots p_k^{a_k}$, then
$$\mu(n) = (-1)^k \text{ if } a_1 = a_2 = \ldots = a_k = 1$$
$$\mu(n) = 0, \text{ otherwise.}$$

1. $\mu(n) = 0$ iff n has a square factor > 1.
2. If $n \geq 1$, we have
$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1 \end{cases}$$

Euler totient function—If $n \geq 1$, the Euler totient $\phi(n)$, is the number of positive integers not exceeding n which are relative prime to n;

1. If $n \geq 1$, $\sum_{d|n} \phi(d) = n$.
2. **Relation between ϕ and μ :**
$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$
3. **Product formula for $\phi(n)$:**
For $n \geq 1$, $\phi(n) = n \prod_{p|n}\left(1 - \frac{1}{p}\right)$.
4. $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ for prime p and $\alpha \geq 1$.
5. $\phi(mn) = \phi(m)\,\phi(n)\,(d/\phi(d))$, where $d = (m, n)$.
6. $\phi(mn) = \phi(m)\,\phi(n)$ if $(m, n) = 1$.
7. $\phi(n)$ is even for $n \geq 3$.
8. If n has r distinct odd prime factors, then $2^r | \phi(n)$.
9. $a|b \Rightarrow \phi(a) | \phi(b)$.

Dirichlet product of arithmetical functions—If f and g are two arithmetical functions then their Dirichlet product (Dirichlet convolution) is an arithmetic function
$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

1. If $h = f * g$ then $h(n) = (f * g)(n)$.
2. Dirichlet product is commutative and associative, i.e., for any arithmetic functions, f, g, k, we have
$$f * g = g * f$$
$$f * (g * k) = (f * g) * k.$$

Identity function—An arithmetic function
$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

Unit function—An arithmetic function $u(n) = 1$ for all n.

Dirichlet inverse—If f is an arithmetic function with $f(1) = 0$ then there is a unique arithmetic function f^{-1}, called Dirichlet inverse of f such that
$$f * f^{-1} = f^{-1} * f = I$$
Moreover, f^{-1} is given by recursion formula,
$$f^{-1}(1) = \frac{1}{f(1)},$$
$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \quad \text{for } n > 1.$$

Möbius inversion—
$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d)\,\mu\left(\frac{n}{d}\right).$$

Mangoldt function—For every integer $n > 1$, Mangoldt function,
$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^m \text{ for some prime } p \text{ and some } m \geq 1 \\ 0, & \text{otherwise} \end{cases}$$

1. If $n \geq 1$, $\log n = \sum_{d|n} \Lambda(d)$
2. If $n \geq 1$, $\Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right)$
$$= -\sum_{d|n} \mu(d) \log d.$$

Multiplicative function—An arithmetical function f is multiplicative if f is not identically zero and if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$.

Completely multiplicative function—A multiplicative function such that
$$f(mn) = f(m)f(n) \text{ for all } m, n$$

1. If f is multiplicative then $f(1) = 1$.
2. Given f with $f(1) = 1$. Then
   (a) f is multiplicative iff $f(p_1^{a_1} \ldots p_r^{a_r}) = f(p_1^{a_1}) \ldots f(p_r^{a_r})$.
   for all primes p_i and all integers $a_i \geq 1$.
   (b) f is multiplicative, then f is completely multiplicative iff $f(p^a) = f(p)^a$ for all primes p and all integers $a \geq 1$.
3. If f and g are multiplicative, so is their Dirichlet $f * g$.
4. If both g and f are multiplicative, then f is also multiplicative.
5. If g is multiplicative, so is g^{-1}, (its Dirichlet inverse).
6. If f is multiplicative, then f is completely multiplicative iff
$$f^{-1}(n) = \mu(n)f(n) \text{ for all } n \geq 1.$$
7. If f is multiplicative, then
$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n}(1 - f(p)).$$

Liouville's function—The Liouville's function $\lambda(1) = 1$ and if $n = p_1^{a_1} \ldots p_k^{a_k}$
$$\lambda(n) = (-1)^{a_1 + a_2 + \ldots + a_k}$$

1. For every $n \geq 1$,
$$\sum_{d|n} \lambda(d) = \begin{cases} 1, & \text{if } n \text{ is square} \\ 0, & \text{otherwise} \end{cases}$$
2. $\lambda^{-1}(n) = |\mu(n)|$ for all n.

The tau (τ) and sigma (σ) function—For each positive integer n, the tau function $\tau(n)$ is the number of positive divisors of n and sigma function $\sigma(n)$ is sum of positive divisors of n, i.e.,
$$\tau(n) = \sum_{\substack{d|n \\ d \geq 1}} 1 \quad \text{and} \quad \sigma(n) = \sum_{\substack{d|n \\ d \geq 1}} d$$

Some Important Theorems

1. If $n = p_1^{s_1}.p_2^{s_2}...p_r^{s_r}$, p_i distinct primes and integers $s_i > 1$: then
   (a) For each $r \geq 1$,
   (i) $\tau(n) = (s_1 + 1)(s_2 + 1)...(s_r + 1)$ and
   (ii) $\sigma(n) = \frac{p_1^{s_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{s_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{s_r+1} - 1}{p_r + 1}$
   (b) $\tau(n) = \tau(p_1^{s_1}).\tau(p_2^{s_2})...\tau(p_r^{s_r})$
   $\sigma(n) = \sigma(p_1^{s_1}).\sigma(p_2^{s_2})...\sigma(p_r^{s_r})$
2. Let n be an integer > 1, then
   (a) $\tau(n)$ is odd iff n is perfect square.
   (b) $\sigma(n)$ is odd iff n is perfect square or twice a perfect square.
   (c) $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$
   (d) $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$

Greatest integer function—Let x be a real number then $[x]$, the greatest integer function denotes the largest integer that does not exceed x.

Some Important Theorems

1. $[x] \leq x \leq [x] + 1$.
2. $[x + m] = [x] + m$, m any integer.
3. $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$
4. $[x] + [-x] = \begin{cases} 0, & \text{if } x \text{ is an integer} \\ -1, & \text{otherwise} \end{cases}$
5. $\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$ if m is a positive integer.
6. If p is a prime number and n a positive integer. Then the exponent e such that

$$p^e | \underline{n} \text{ is almost } \sum_{i=1}^{\infty} \left[\frac{n}{p_i}\right].$$

11. Group

A non empty set of elements, G is said to form a group if in G there is defined a binary operator $*$ called product such that

(a) $a, b \in G \Rightarrow a * b \in G$. (Closed)

(b) $a, b, c \in G \Rightarrow a * (b * c) = (a * b) * c$. (Associative)

(c) There exist $e \in G : a * e = e * a = a$, for all $a \in G$. (Existence of identity)

(d) For every $a \in G$, there exist $a^{-1} \in G$: $a * a^{-1} = a^{-1} * a = e$. (Existence of inverse)

Abelian group—A group G is Abelian (Commutative) if for every $a, b \in G, a * b = b * a$.

If G is a non-empty set and $*$ is any binary operation defined on G, then $(G, *)$ is—

(a) **Quasi-group**—$a, b \in G \Rightarrow a * b \in G$.

(b) **Semi-group**—$a, b \in G \Rightarrow a * b \in G$ and $(a * b) * c = a * (b * c)$, $a, b, c \in G$.

(c) **Monoid**—$a, b \in G \Rightarrow a \cdot b \in G$, $(a * b) * c = a * (b * c)$, $a, b, c \in G$ and there exist $e \in G$ identity : $a * e = e * a = a$.

i.e. semi-group is a *quasi-group* with associativity.

Monoid is a *semi-group* with identity.

Group is a *monoid* with inverse.

Abelian group is a *group* with commutativity.

Order of group—The number of elements in G, $o(G)$.

Cyclic group—$a^i \in G$ and $O(G) = n$:

$$a^i = \begin{cases} a^0 = a^n = e, & i = 0, n \\ a^i & i < n \\ a^{i-n} & i > n \end{cases}$$

Lemma—(a) The identity element of G is unique.

(b) $\forall a \in G$, its inverse a^{-1} is unique.

(c) $a \in G \Rightarrow (a^{-1})^{-1} = a$

(d) $a, b \in G \Rightarrow (a * b)^{-1} = b^{-1} * a^{-1}$

(e) $a * b = a * c \Rightarrow b = c$

$b * a = c * a \Rightarrow b = c$

12. Subgroup

A non empty subset H of G, is a subgroup of group G, if H is a group on the operator of G.

Right and left cosets—H is a subgroup of group G, $a \in G$ then

Right coset of H in G is $Ha = \{ha : h \in H\}$

Left coset of H in G is $aH = \{ah : h \in H\}$

Index of subgroup—If H is a subgroup of G, the index of H in G is the number of distinct right cosets of H in G.

Order (period) of element—If G is a group, $a \in G$, the order of a (period of a), is the least positive integer $m : a^m = e$, $o(a) = m$.

Product subgroups—$HK = \{x \in G : x = hk; h \in H, k \in K\}$, H, G are subgroup of G.

Lemma—A non-empty subset H of a group G is a subgroup of G iff,

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

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

Lemma—If H is a non-empty finite subset of G and H is closed then H is a subgroup of G.

Lemma—$\forall a \in G$

$$Ha = \{x \in G : a \equiv x \bmod H\}.$$

Lemma—There is one-to-one correspondence between two right cosets of H in G.

Some Important Theorems

1. If G is a finite group and H is a subgroup of G, then $o(H)$ divides $o(G)$.
2. If G is a finite group and $a \in G \Rightarrow o(a)/o(G)$.
3. If G is a finite group and $a \in G \Rightarrow a^{o(G)} = e$.
4. **Fermat**—If p is a prime number and a is any integer, then $a^p \equiv a \bmod p$.
5. If G is a finite group whose order is a prime number p, then G is a cyclic group.
6. HK is a subgroup of G iff HK = KH.
7. If HK are subgroups of the Abelian group G, then HK is a subgroup of G.
8. If H and K are finite subgroups of G of orders $o(H)$ and $o(G)$ respectively then

$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)}.$$

9. If H and K are subgroups of G and $o(H) > \sqrt{o(G)}$ and $o(K) > \sqrt{o(G)}$, then $H \cap K \neq \{e\}$.

13. Normal Subgroups and Quotient Groups

Normal subgroup—A subgroup N of G is normal subgroup if $\forall g \in G$ and $n \in N$, $gng^{-1} \in N$.

Quotient group—If G is a group, N is normal subgroup of G, then group G|N is called quotient (factor) group.

Lemma—N is a normal subgroup of G iff $gNg^{-1} = N$, for $\forall g \in G$.

Lemma—N is a normal subgroup of G iff $Na = aN$, $\forall a \in G$.

Lemma—N is a normal subgroup of G iff $(Na)(Nb) = Nab$.

Lemma—N is a normal subgroup of G, G is finite group then

$$o(G|N) = o(G)/o(N).$$

14. Homomorphism

Homomorphism—A mapping ϕ from group G into a group $\bar{G}$ is said to be a homomorphism if $\forall a, b \in G, \phi(ab) = \phi(a)\phi(b)$.

Kernel—If ϕ is a homomorphism of G into $\bar{G}$, the kernel of ϕ, K_ϕ is defined by $K_\phi = \{x \in G : \phi(x) = \bar{e}$, $\bar{e}$ an identity element in $\bar{G}\}$.

Isomorphism—A homomorphism ϕ from G into $\bar{G}$ is an isomorphism if ϕ is one-to-one.

Isomorphic—Two groups G and $G*$ are isomorphic if there is an isomorphism of G onto G^*, $(G \cong G^*)$.

Lemma—N is a normal subgroup of G ; $\phi : G \to G/N : \phi(x) = Nx$, $\forall x \in G$. Then ϕ is homomorphism of G onto G/N.

Lemma—If ϕ is homomorphism of G into $\bar{G}$, then

(a) $\phi(e) = \bar{e}$, the identity element of $\bar{G}$.

(b) $\phi(x^{-1}) = \phi(x)^{-1}$, $\forall x \in G$.

Lemma—If ϕ is homomorphism of G into $\bar{G}$ with Kernel K, then K is a normal subgroup of G.

Lemma—If ϕ is a homomorphism of G into $\bar{G}$ with kernel K, then the set of all inverse images of $\bar{g} \in \bar{G}$ under ϕ is given by Kx, where x is any particular inverse image of $\bar{g} \in \bar{G}$.

Lemma—A homomorphism ϕ of G into $\bar{G}$ with kernel K_ϕ is isomorphism of G into $\bar{G}$ iff $K_\phi = (e)$.

Some Important Theorems

1. If ϕ is a homomorphism of G onto $\bar{G}$ with kernel K, then $G/K \approx \bar{G}$.

2. **Cauchy's theorem for Abelian group**—If G is a finite Abelian group and any prime number $p|o(G)$ there exist $a \neq e \in G : a^p = e$.
3. **Sylow's theorem for Abelian group**—If G is a finite Abelian group and p any prime such that $p^{\alpha}|o(G)$, $p^{\alpha+1} \nmid o(G)$, then G has a subgroup of order p^{α}.
4. If G is Abelian group of order $o(G)$ and $p^{\alpha}|o(G)$, $p^{\alpha+1} \nmid o(G)$, then there is unique subgroup of G of order p^{α}.
5. If ϕ is homomorphism of G into $\bar{G}$ with kernel K, and $\bar{N}$ is a normal subgroup of $\bar{G}$, N = $\{x \in G | \phi(x) = \bar{N}\}$.

   Then $G/N = \bar{G} | \bar{N}$ and $G|N = (G|K)\ (N|K)$.

15. Automorphism

Automorphism—A homomorphism of a group G onto itself.

Theorems

1. If G is a group, A(G), a set of automorphism is also a group.
2. Let G be a group and ϕ an automorphism of G.

   If $a \in G$ and $o(a) > 0$, then $o(\phi(a)) = o(a)$.

16. Cayley's Theorem

1. **Caylery**—Every group is isomorphic to a subgroup of A(S) for some appropriate S.
2. If H is a subgroup of G, S is a set of all right cosets of H in G, then there is a homomorphism o of G into A(S) and the kernel of o is the largest normal subgroup of G, which is contained in H.
3. If G is a finite group, $H \neq G$ is a subgroup of $G : o(G) \nmid i(H)!$ then H must contain non-trivial normal subgroups of G.

17. Permutation Groups

Even permutation—A permutation $\theta \in S_n$ is said to be an even permutation if it can be represented as a product of an even number of transpositions.

Lemma—Every permutation is the product of its cycles.

Lemma—Every permutation is a product of 2-cycles (transposition).

Lemma—S_n has as a normal subgroup of index 2, the alternating group A_n, consisting of all even permutations.

18. Conjugate and Normalizer

Conjugate—If $a, b \in G$, b is conjugate to a if there exist $c \in G : b = c^{-1}\,ac$.

Normalizer—$a \in G$, N(a) the normalizer of a in G is $N(a) = \{x \in G : x\,a = ax\}$.

Lemma—Conjugacy is an equivalence relation on G.

Lemma—N(a) is a subgroup of G.

Some Important Theorems

1. If G is a finite group $\Rightarrow o(G)|o(N(a))$
2. $a \in Z(G)$, the centre of a group iff $N(a) = G$. If G is finite, $a \in Z$ iff $o(N(a)) = o(G)$.
3. If $o(G) = p^n$, p is a prime number $\Rightarrow Z(G) \neq (e)$.
4. If $o(G) = p^2$, p is a prime number $\Rightarrow$ G is Abelian.
5. **Cauchy**—If p is prime number and $p|o(G)$ then G has an element of order p.

19. Sylow's Theorem

1. If p is a prime number and $p^{\alpha}|o(G)$, then G has a subgroup of order p^{α}.
2. If $p^m|o(G)$, $p^{m+1} \nmid o(G)$, then G is a subgroup of order p^m.
3. If A and B are finite subgroups of G then

$$o(A \times B) = \frac{o(A)\,o(B)}{o(A \cap x B x^{-1})}$$

20. Direct Product

Internal direct product—If G is a group and $N_1, N_2, \ldots, N_n$ are normal subgroup of G :

(a) $G = N_1, N_2 \ldots\ldots, N_n$

(b) $g \in G$, $g = m_1\ m_2 \ldots m_n$, $m_i \in N_i$ in a unique way, then G is internal direct product of N_1 $N_2 \ldots N_n$.

1. If G is internal direct product of $N_1 \ldots N_n$, then for $i \neq j$, $N_i \cap N_j = (e)$ and if $a \in N_i, b \in N_j$ then $ab = ba$.
2. If G is internal direct product of $N_1, \ldots, N_n$, and if $T = N_1 \times N_2 \times \ldots\ldots \times N_n$, then G and T are isomorphic.

21. Finite Abelian Group

Invariants of G—If G is an Abelian group of order p^n, p a prime

$G = A_1 \times A_2 \times \ldots \times A_m$, $\forall\ A_i$ is cyclic of order p^{n_i}, $n_i \leq n_{i+1}$, then $n_1, \ldots, n_k$ are invariants of G.

Theorem—The number of non-isomorphic Abelian groups of order p^n are equals to the number of partitions of n.

22. Associative Ring

A non-empty set R is said to be a ring if in R, there are defined two operators + and · respectively : $a, b, c \in R$.

(a) $a + b \in R$
(b) $a + b = b + a$
(c) $(a + b) + c = a + (b + c)$
(d) $0 \in R : a + 0 = a$, $\forall a \in R$
(e) $-a \in R : a + (-a) = 0$

} Abelian group with identity 0 on addition.

(f) $a \cdot b \in R$ (Closed under ·)
(g) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Associative under ·)
(h) $(a + b) \cdot c = a \cdot c + b \cdot c$ (Left distribution)
$c \cdot (a + b) = c \cdot a + c \cdot b$ (Right distribution)

Ring with unity—$1 \in R : a \cdot 1 = 1 \cdot a = a$ $\forall a \in R$.

Commutative ring—If $a \cdot b = b \cdot a$, $\forall a, b \in R$.

Zero divisor—R is commutative ring, $a \neq 0 \in R$, is zero divisor if there exist $b \in R$, $b \neq 0 : ab = 0$.

Integral domain : A commutative ring is an integral domain if it has no zero divisor.

Division ring (Skew field)—A ring is called a division ring if its non-zero elements form a group under multiplication.

Characteristic zero—An integral domain D is of characteristic zero if $ma = 0$, $a \neq 0 \in D$ $\Rightarrow$ $m = 0$.

Finite characteristic—An integral domain D is of finite characteristic if there exist a positive integer $m : ma = 0$, $\forall\ a \in D$.

Null (zero) ring—$(\{0\}, +, \cdot) : 0 + 0 = 0$ and $0 \cdot 0 = 0$.

Field—A field is a commutative division ring.

23. Homomorphism

Homomorphism—A mapping ϕ from ring R into ring R' is homomorphism if $\forall\ a, b \in R$.

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

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

Kernel—If ϕ is a homomorphism of R into R', then the kernel of ϕ, $I(\phi)$, is the set of all $a \in R : \phi(a) = 0$, the zero element of R'.

Zero homomorphism—$\phi(a) = 0$ for all $a \in R$ and $I(\phi) = R$.

Isomorphism—A homomorphism of R into R' if it is also one-to-one mapping.

Isomorphic—A and B are isomorphic, if there is a isomorphism from one onto another.

Some Important Theorems

1. If ϕ is homomorphism of R into R', then

   (i) $\phi(a) = 0$

   (ii) $\phi(-a) = -\phi(a)$, $\forall\ a \in R$.
2. If ϕ is homomorphism of R into R' with kernel $I(\phi)$, then

   (a) $I(\phi)$ is a subgroup of R under addition.

   (b) If $a \in I(\phi)$ and $r \in R$ then both $ar \in R$ and $ra \in R$.
3. The homomorphism ϕ of R into R' is an isomorphism iff $I(\phi) = 0$.
4. If integral domain is of finite characteristic then its characteristic is a prime number.

24. Ideals and Quotient Rings

Ideal—A non-empty subset U of R is Ideal if

(a) U is a subgroup under addition

(b) $\forall\ u \in U$ and $r \in R$, $ur, ru \in U$.

Quotient ring—If U is an ideal of ring R, then R/U is a quotient ring and is homomorphic image of R.

Maximal ideal—An ideal $M \neq R$ in a ring R is maximal ideal of R if whenever U is an ideal of $R : M \subset U \subset R$ then either $R = U$ or $M = U$.

Some Important Theorems

1. If R is a commutative ring with unit element and M is an ideal of R then M is maximum ideal of R iff R/M is a field.

2. If R is a commutative ring with unit element whose only ideals are (0) and R, itself. Then R is a field.

25. Euclidean Ring

Euclidean ring—An integral domain R is an Euclidean ring if for every $a \neq 0 \in R$ there is defined a non-negative integer $d(a)$:

(a) $\forall\, a, b \in R, a \neq 0, b \neq 0 \Rightarrow d(a) \leq d(ab)$

(b) for any $a, b \in R, a \neq 0, b \neq 0$, there exist $t, r \in R : a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.

Principal ideal—An integral domain R with unit element is a *principal ideal ring* if every ideal $A \in R$ is of the form $A = (a) = \{xa | x \in R\}$ for some $a \in R$.

Unit (elements)—$a \in R$ is unit element in R if there exist $b \in R : ab = 1$.

Unit—If R is a commutative ring with unit element.

Prime element—In Euclidean ring R a non unit π is said to be prime element of R if whenever $\pi = ab, a, b \in R$ then one of a or b is a unit in R.

Relatively prime—In the Euclidean ring R, $a, b \in R$ are relatively prime if their greatest common divisor is a unit of R.

Some Important Theorems

1. If R is an Euclidean ring and A an ideal of R. Then there exist an element $a_0 \in R$: A consists exactly of all $a_0 x$ as range over R.
2. A Euclidean ring possesses a unit element,
3. If R is an euclidean ring. Then any two elements $a, b \in R$ have a greatest common divisor d. Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.
4. If R is an integral domain with unit element and suppose for $a, b \in R$, $a|b$ and $b|a$ are true. Then $a = ub$, where u is a unit in R.
5. If R is an Euclidean ring and $a, b \in R$. If $b \neq 0$ is not a unit in R, then $d(a) < d(ab)$.
6. If R is an Euclidean ring. Then every element in R is either a unit in R or can be written as the product of a finite number of prime elements of R.
7. If R is an Euclidean ring. Suppose for $a, b, c \in R$, $a|bc$ but $(a, b) = 1$. Then $a|c$.
8. If π is a prime element in the Euclidean ring R and $\pi | ab$, where $a, b \in R$ then π divides atleast one of a or b.
9. If π is a prime element in the Euclidean ring R and $\pi | a_1 a_2 \ldots\ldots a_n$, then π divides atleast one $a_1, a_2, \ldots\ldots, a_n$.
10. **Unique factorization theorem**—If R is an Euclidean ring and $a \neq 0$ a non-unit in R. Suppose $a = \pi_1 \pi_2 \ldots\ldots \pi_n = \pi_1' \pi_2' \ldots\ldots \pi_m'$ where π_i and π_i' are prime elements in R. Then $n = m$ and each π_i, $i = 1, \ldots, n$ is an associate of same π_j', $j = 1 \ldots n$ and conversely each π_j' is associated with same π_j.
11. Every non-zero element in an Euclidean ring R can be uniquely written as a product of prime elements or is a unit in R.
12. The ideal $A = (a_0)$ is a maximal ideal of the Euclidean ring R iff a_0 is a prime element of R.

26. Polynomial Ring

If F is a field. The ring of polynomials in the indeterminate, x, $F[x]$ is set of polynomials $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_n x^n$, where n is non-negative integer and $a_0, \ldots\ldots a_n \in F$.

Equal polynomial—If $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_m x^m$ and

$q(x) = b_0 + b_1 x + b_2 x^2 + \ldots\ldots + b_n x^n$ are in $F[x]$ then $p(x) = q(x)$ iff $\forall\, i \geq 0, a_i = b_i$.

Addition of polynomial—If $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_m x^m$ and

$q(x) = b_0 + b_1 x + b_2 x^2 + \ldots\ldots + b_n x^n$ are in $F[x]$

then $p(x) + q(x) = c_0 + c_1 x + \ldots\ldots + c_i x^i$

where $c_i = a_i + b_i$.

Multiplication of polynomial—If $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_m x^m$ and

$q(x) = b_0 + b_1 x + b_2 x^2 + \ldots\ldots + b_n x^n$ are in $F[x]$

then $p(x)\, q(x) = c_0 + c_1 x + \ldots\ldots + c_k x^k$

where $c_i = a_i b_0 + a_{i-1} b_1 + a_{i-2} b_2 + \ldots + a_0 b_i$

Degree of $p(x)$—If $p(x) = a_0 + a_1 x + \ldots\ldots + a_m x^m \neq 0$ and $a_m \neq 0$ the degree of $p(x)$ is $\deg p(x) = m$.

Irreducible polynomial—A polynomial $p(x) \in F[x]$ is irreducible if whenever $p(x) = a(x)\, b(x)$, with $a(x), b(x) \in F[x]$, then one of $a(x)$ or $b(x)$ has degree 0 (*i.e.* constant).

Some Important Theorems

1. If $f(x)$ and $g(x)$ are non-zero elements of $F[x]$, then
   (a) $\deg (f(x)\, g(x)) = \deg f(x) + \deg g(x)$
   (b) $\deg f(x) \leq \deg (f(x)\, g(x))$
2. $F[x]$ is a Euclidean ring.
3. $F[x]$ is a principal ideal ring.
4. Given two polynomials, $p(x), g(x) \in F[x]$, we have a greatest common divisor $d(x)$ which can be realized as $d(x) = \lambda(x) f(x) + \mu(x)\, g(x)$
5. Any polynomial in $F[x]$ can be written as unique product of irreducible polynomials in $F[x]$.
6. The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal iff $p(x)$ is irreducible over F.

27. Polynomials over the Rational Fields

Primitive—The polynomial $f(x) = a_0 + a_1 x + \ldots\ldots + a_n x^n$, where $a_0, a_1, a_2, \ldots\ldots, a_n$ are integers is primitive if the greatest common divisor of $a_0\, a_1\, a_2 \ldots\ldots a_n$ is 1.

Content—The content of polynomial $p(x) = a_0 + a_1 x + \ldots\ldots + a_n x^n$, where a's are integer, is the greatest common divisor of integers $a_0, a_1, \ldots\ldots, a_n$.

Integer monic—A polynomial is integer monic if all the coefficients are integers and the highest coefficient is 1.

Some Important Theorems

1. If $f(x)$ and $g(x)$ are primitive polynomials, then $f(x)\, g(x)$ is a primitive polynomials.
2. **Gauss' Lemma**—If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.
3. If an integer monic polynomial factors as the product of two non-constant polynomials having rational coefficients then it factors as the product of two integer monic polynomials.
4. **Einstein criterion**—If $g(x) = a_0 + a_1 x + \ldots\ldots + a_n x^n$ is a polynomial with integer coefficients. Suppose that for some prime number p, $p \nmid a_n$, $p | a_1$, $p | a_2, \ldots\ldots, p \nmid a_0$, $p^2 \nmid a_0$. Then $g(x)$ is irreducible over the rationals.

28. Polynomial Rings over Commutative Rings

$F[x_1, \ldots\ldots x_n]$: The field of rational functions in $x_1, \ldots\ldots, x_n$ over F.

Unique factorization domain—An integral domain, R_1 with unit element is a unique factorization domain if—

(a) Any non-zero element in R is either a unit or can be written as the product of a finite number of irreducible elements of R.

(b) The decomposition in part (a) is unique upto the order and associates of the irreducible elements.

Some Important Theorems

1. If R is an integral domain, then so is $R[x]$.
2. If R is an integral domain, then so is $R[x_1, \ldots\ldots x_n]$.
3. If R is a unique factorization domain and if $a, b \in R$, then a and b have the greatest common divisor $(a, b) \in R$. Moreover, if a, b are relatively prime $(a, b) = 1$, whenever $a|bc$ then $a|c$.
4. If $a \in R$ is an irreducible element and $a|bc$, then $a|b$ or $a|c$.
5. If R is a unique factorization domain, then the product of two primitive polynomials in $R[x]$ is again a primitive polynomial in $R[x]$.
6. If R is a unique factorization domain and if $f(x), g(x) \in R[x]$ then $c(fg) = c(f)\, c(g)$.
7. If $f(x) \in R[x]$ is both primitive and irreducible as an element of $R[x]$, then it is irreducible as an element of $F[x]$. Conversely, if the primitive element $f(x) \in R[x]$ is irreducible as an element of $F[x]$, it is also irreducible as an element of $R[x]$.
8. If R is a unique factorization domain and if $p(x)$ is a primitive polynomial in $R[x]$, then it can be factored in a unique way as the product of irreducible elements in $R[x]$.
9. If R is a unique factorization domain, then so is $R[x]$.

10. If R is a unique factorization domain then so is $R[x_1, \ldots\ldots, x_n]$.
11. If F is a field then $F[x_1, \ldots\ldots, x_n]$ is a unique factorization domain.

29. Fields

Field (F) is a non-empty set, F is a field.

(a) (F, +) is an Abelian group.

(b) (F,·) is semi-Abelian, *i.e.*, (F–{0},·) is Abelian group.

(c) Multiplication is distributive over addition

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

$$(b + c)a = ba + ca.$$

Extension—K, F are fields, K is an extension of F if $F \subset K \Leftrightarrow$ F is a subfield of K.

Degree of extension—The degree of extension K over F, [K; F] is the dimension of K as a vector space of F.

Algebraic over F—K is an extension of F, $a \in$ K is algebraic over F, if there exist elements $\alpha_0, \alpha_1, \ldots\ldots, \alpha_n \in F$, not all zero, such that $\alpha_0 a^n + \alpha_1 \alpha^{n-1} + \ldots\ldots + \alpha_n = 0$.

Sub-field obtained by adjoining *a* to F—If K is an extension of F, $a \in$ K, then F(*a*), is the smallest subfield containing both F and *a*.

Algebraic of degree *n*—The element $a \in$ F is algebraic of degree *n* over F if it satisfies a non-zero polynomial over F of degree *n* but no, non-zero polynomial of lower degree.

Algebraic extension—The extension K of F is called an algebraic extension of F if every element in K is algebraic over F.

Algebraic number—A complex number is algebraic number if it is algebraic over the field of rational number.

Some Important Theorems

1. If L is a finite extension of K and if K is a finite extension of F, then L is a finite extension of F and [L : F] = [L : K] [K : F].
2. If L is a finite extension of F and K is a sub-field of L which contains F, then [K:F]|[L:F].
3. The element $a \in$ K is algebraic over F iff F(*a*) is a finite extension of F.
4. If $a \in$ K is algebraic of degree *n* over F, then [F(*a*) : F] = *n*.
5. If $a, b \in$ K are algebraic over F then $a \pm b$, ab and a/b $(b \neq 0)$ are all algebraic over F, *i.e.*, the elements in K which are algebraic over F form a subfield of K.
6. If $a, b \in$ K are algebraic over F, of degrees *m* and *n*, respectively, then $a \pm b$, ab and a/b $(b \neq 0)$ are algebraic over F of degree atmost *mn*.
7. If L is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.

30. Roots of Polynomials

Root of $p(x)$—If $p(x) \in F[x]$, then an element *a* in some extension field of F is called a root of $p(x)$, if $p(a) = 0$.

Multiplicity—The element $a \in$ K is a root of $p(x) \in F[x]$ is of multiplicity *m* if $(x - a)^m | p(x)$, whereas $(x - a)^{m+1} \nmid p(x)$.

Splitting fields—If $f(x) \in F[x]$, a finite extension E of F is said to be a splitting field over F for $f(x)$ if over E (*i.e.* in E[*x*]), but not over any proper sub-field of E, $f(x)$ can be factored as a product of linear factors.

Some Important Theorems

1. **Remainder theorem**—If $p(x) \in F[x]$ and if K is an extension of F then for any element $b \in$ K, $p(x) = (x - b)\, q(x) + p(b)$, where $q(x) \in K[x]$ and $\deg q(x) = \deg p(x) - 1$.
2. If $a \in$ K is a root of $p(x) \in F[x]$, where $F \subset$ K, then in K[*x*] $(x - a) \mid p(x)$.
3. A polynomial of degree *n* over a field B can have atmost *n* roots in any extension.
4. If $p(x)$ is a polynomial in F[*x*] of degree $n \geq 1$ and is irreducible over F, then there is an extension E of F, such that [E : F] = *n*, in which $p(x)$ has a root.
5. If $f(x) \in F[x]$, then there is a finite extension E of F in which $f(x)$ has a root. Moreover $[E : F] \leq \deg f(x)$.
6. Let $f(x) \in F[x]$ be of degree $n \geq 1$. Then there is an extension E of F of degree at most *m* in which $f(x)$ has a root.

31. The Ring, Integral Domain and Field

	Ring (R, +, .)	Integral Domain (D, +, .)	Field (F, +, .)
(a) Abelian Group	(R, +) Abelian group	(D, +) Abelian group	(F, +) Abelian group
(b) (·) is associative	(·) is associative	(·) is associative	(·) is associative
(c) distributive law follows	distributive law follows	distributive law follows	distributive law follows
(d) Commutative (·)	—	(·) is commutative	(·) is commutative
(e) Unity	—	Unity belongs to D	Unity belongs to F
(f) Multiple inverse of non-zero element exists	—	—	Multiple inverse of non-zero element exists and belong to F
(g) Zero divisors	May or may not possess proper zero divisor	does not possess proper zero divisor	does not possess proper zero divisor.

The Different Groups

	Quasi group	Semi group	Monoid	Group	Abelian Group
Closure	√	√	√	√	√
Associative	—	√	√	√	√
Existence of identity	—	—	√	√	√
Existence of inverse	—	—	—	√	√
Commutative	—	—	—	—	√

PART–B

1. The set S of square matrices of same order with respect to matrix addition, is a—
   (A) Quasi-group (B) Semi-group
   (C) Group (D) Abelian group
2. The set of square matrices order 2, with respect to matrix multiplication is a—
   (A) Quasi-group (B) Semi-group
   (C) Monoid (D) Group
3. The set of all non-singular square matrices of same order with respect to matrix multiplication is—
   (A) Quasi-group (B) Monoid
   (C) Group (D) Abelian group
4. If order of group G is p^2, where p is prime then—
   (A) G is Abelian
   (B) G is not Abelian
   (C) G is ring
   (D) None of these
5. If G is a group, for $a \in$ G, N(a) is the normalizer of a, then $\forall\, x \in N(a)$—
   (A) $xa = ax$ (B) $xa = e$
   (C) $ax = e$ (D) $xa \neq ax$
6. If G is a group, then for all $a, b \in$ G—
   (A) $(ab)^{-1} = a^{-1}\, b^{-1}$ (B) $(ab)^{-1} = b^{-1}\, a^{-1}$
   (C) $(ab)^{-1} = ab$ (D) $(ab)^{-1} = ba$
7. If G is a set of integers and $a \cdot b \equiv a - b$, then G is—
   (A) Quasi-group (B) Semi-group
   (C) Monoid (D) Group
8. In a group G, for each element $a \in$ G, there is—
   (A) No inverse
   (B) A unique inverse $a^{-1} \in$ G
   (C) More than one inverse
   (D) None of these
9. If $a, b \in$ G, a group then b is conjugate to a if exist $c \in$ G ....
   (A) $b = c^{-1}\, a\, c$ (B) $a = cb$
   (C) $b = ac^{-1}$ (D) $b = cc^{-1}\, a$
10. If p is prime number and $p \mid o(G)$, then $a \in$ G—
    (A) $a^p \in$ G (B) $a^p \notin$ G
    (C) $a^p \subset$ G (D) $a^p \supset$ G
11. If G is a group of order n then, order of identity element is—
    (A) One (B) Greater than one
    (C) n (D) None of these
12. If $a \in$ G is of order n and p is prime to n, then the order of a^p is—
    (A) n (B) One
    (C) Less than n (D) Greater than n
13. If the orders of elements $a, a^{-1} \in$ G are m and n respectively then—
    (A) $m = n$ (B) $m \neq n$
    (C) $m = n = 0$ (D) None of these
14. If in a group G, $a \in$ G, the order of a is n and order of a^p is m then—
    (A) $m \leq n$ (B) $m \geq n$
    (C) $m = 0$ (D) None of these
15. The identity permutation is—
    (A) Even permutation
    (B) Odd permutation
    (C) Neither even nor odd
    (D) None of these
16. The product of even permutation is—
    (A) Even permutation
    (B) Odd permutation
    (C) Neither even nor odd
    (D) None of these
17. The inverse of an even permutation is—
    (A) Odd permutation
    (B) Even permutation

(C) Even or odd permutation
(D) None of these

18. The product of (1 2 4 5) (3 2 1 5 4) is—
(A) (2 3) (B) (1 5)
(C) (3 4 1) (D) (1 5 3 1)

19. The inverse of an odd permutation is—
(A) Odd permutation
(B) Even permutation
(C) Even or odd
(D) None of these

20. If b and c are the inverse of some element $a \in G$, then—
(A) $b = c$
(B) $b \neq c$
(C) $b = \alpha c$, for same α
(D) None of these

21. Let Z be a set of integers, then under ordinary multiplication $(Z, \cdot)$ is—
(A) Monoid (B) Semi-group
(C) Quasi-group (D) Group

22. If N is a set of natural numbers then under binary operation $a \cdot b = a - b$, $(N, \cdot)$ is—
(A) Quasi-group (B) Semi-group
(C) Monoid (D) Group

23. If G is a finite group and order of group is m then $\forall a \in G$—
(A) $a^m = e$, an identity
(B) $a^m \neq e$
(C) $a^m = a$
(D) $a^m = a^{-1}$

24. HK is a sub-group of G iff—
(A) HK = KH (B) $HK \subset KH$
(C) $HK \supset KH$ (D) $HK \neq KH$

25. If G is a group and $a \in G$ such that $a^2 = a$, then a is equal to—
(A) Identity element
(B) Inverse
(C) Zero element
(D) None of these

26. The generators of a group $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$ are—
(A) a and a^5 (B) a^2 and a^4
(C) a^3 and a^5 (D) a^2 and a^3

27. If $G = \{1, -1, i, -i\}$ is a multiplicative group, then order of $-i$ is—
(A) One (B) Two
(C) Three (D) Four

28. If $G = \{(0, 1, 2, 3, 4), +_5\}$ the order of 2 is—
(A) One (B) Two
(C) Four (D) Five

29. If G is a group of even order, $\forall a \neq e$ if $a^2 = e$ then G is—
(A) Abelian group (B) Sub-group
(C) Normal group (D) None of these

30. Every group of prime order is—
(A) Cyclic (B) Abelian
(C) Sub-group (D) Normal group

31. If H_1 and H_2 are two right coset sets of sub-group H then—
(A) $H_1 \cap H_2 = \phi$ or $H_1 = H_2$
(B) $H_1 \cap H_2 \neq \phi$
(C) $H_1 \cup H_2 = \phi$
(D) $H_1 \neq H_2$ and $H_1 \cap H_2 \neq \phi$

32. The number of elements in a group is—
(A) Identity of group
(B) Order of group
(C) Inverse of group
(D) None of these

33. A one-one mapping of a finite group onto itself is—
(A) Isomorphism (B) Homomorphism
(C) Automorphism (D) None of these

34. If in a group G, $\forall a \in G$—
(A) $(a^{-1})^{-1} = a$ (B) $(a^{-1})^{-1} = a^{-1}$
(C) $(a^{-1})^{-1} = a^2$ (D) None of these

35. If $f = (2\ 3)$ and $g = (4\ 5)$ be two permutation on five symbols 1, 2, 3, 4, 5 then gf is—
(A) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$ (B) $\begin{pmatrix} 1 & 2 & 3 & 5 & 6 \\ 1 & 4 & 6 & 5 & 4 \end{pmatrix}$
(C) $\begin{pmatrix} 1 & 2 & 3 & 5 & 7 \\ 1 & 4 & 6 & 4 & 1 \end{pmatrix}$ (D) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$

36. Given permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 4 & 3 \end{pmatrix}$ is equivalent to—
(A) (1 6 3 2) (2 1) (B) (1 6 3 2) (1 1)
(C) (1 6 3 2) (4 5) (D) (1 6 3 2) (5 4)

37. If given permutations are $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$,

$B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$ find BA—

(A) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$ (B) $\begin{pmatrix} 2 & 1 & 5 & 3 & 5 \\ 1 & 6 & 4 & 2 & 1 \end{pmatrix}$

(C) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 1 \end{pmatrix}$ (D) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

38. If number of left cosets of H in G are n and the number of right cosets of H in G are m then—

(A) $m = n$ (B) $m \geq n$

(C) $m \leq n$ (D) None of these

39. If H is a subgroup of finite group G and order of H and G are respectively m and n then—

(A) $m \mid n$ (B) $n \mid m$

(C) $m \nmid n$ (D) None of these

40. If G is a finite group of order n, then for every $a \in$ G, we have—

(A) $a^n = e$, an identity element

(B) $a^n = a^{-1}$

(C) $a^n = a$

(D) None of these

41. If H_1 and H_2 are two subgroups of G then following is also a subgroup of G—

(A) $H_1 \cap H_2$ (B) $H_1 \cup H_2$

(C) $H_1 H_2$ (D) None of these

42. The set M of square matrices (of same order), with respect to matrix multiplication is—

(A) Group (B) Semi-group

(C) Monoid (D) Quasi-group

43. If (G, $*$) is a group and $\forall\ a, b \in$ G

$b^{-1} * a^{-1} * b * a = e$, then G is—

(A) Abelian group (B) Non-Abelian

(C) Ring (D) Field

44. If G is a group such that $a^2 = e$, $\forall\ a \in$ G, then G is—

(A) Abelian group

(B) Non-Abelian group

(C) Ring

(D) Field

45. If $f = (2\ 3)$ and $g = (4\ 5)$ are two permutations on 1 2, 3, 4, 5 then fg is—

(A) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$ (B) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 2 & 5 & 6 \end{pmatrix}$

(C) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 6 \end{pmatrix}$ (D) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

46. If n is the order of element a of group G then $a^m = e$, an identity element iff—

(A) $m \mid n$ (B) $n \mid m$

(C) $m \chi n$ (D) $n \nmid m$

47. The order of identity element in a group G is—

(A) One

(B) Zero

(C) Order of group

(D) Less than order of group

48. If $a, a^{-1} \in$ G, a group and order of a and a^{-1} are m and n respectively then—

(A) $m > n$ (B) $m < n$

(C) $m = n$ (D) None of these

49. If $a, b \in$ G, a group of order m then order of ab and ba are—

(A) Same (B) Equal to m

(C) Unequal (D) None of these

50. If G = {1 , – 1} is a group, then order of 1 is—

(A) One (B) Two

(C) Zero (D) None of these

51. The product of permutations $(1\ 2\ 3) \cdot (2\ 4\ 3) \cdot (1\ 3\ 4)$ is equal to—

(A) I (B) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 2 & 1 \end{pmatrix}$

(C) $\begin{pmatrix} 1 & 2 & 5 & 1 \\ 1 & 6 & 5 & 1 \end{pmatrix}$ (D) $\begin{pmatrix} 1 & 2 & 5 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

52. The permutation $\begin{pmatrix} 1 & 2 & 5 & 3 & 4 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ is equal to—

(A) (1 5) (1 3) (2 4) (B) (1) (2) (3)

(C) (1 3 5) (5 6) (D) (1 4 2) (5 3)

53. Given the permutation $c = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ then c^3 is—

(A) (1 3 5 7 2 4) (B) (1 4 7 3 6 2 5)

(C) (1 7 6 5 4 3 2) (D) I

54. If $c = (1\ 2\ 3\ 4)$ then c^2 is—
(A) $(1\ 3)(2\ 4)$ (B) $(1\ 3)$
(C) $(2\ 4)$ (D) $(2\ 3)(3\ 1)$

55. Statement A : All cyclic groups are abelian
Statement B : The order of cyclic group is same as the order of its generator.
(A) A and B are false
(B) A is true, B is false
(C) B is true, A is false
(D) A and B are true

56. Statement A : Every isomorphic image of a cyclic group is cyclic
Statement B : Every homomorphic image of a cyclic group is cyclic.
(A) Both A and B are true
(B) Both A and B are false
(C) A is true only
(D) B is true only

57. A element a^p of a finite cyclic group G of order n is a generator of G iff $0 < p < n$ and also—
(A) p is prime to n
(B) p is the multiple of n
(C) n is the multiple of n
(D) None of these

58. If G is a finite group of order n, $a \in$ G and order of a is m, if G is cyclic then—
(A) $m = n$ (B) $m > n$
(C) $m < n$ (D) None of these

59. If $a \in$ G is a generator of a cyclic group and order of a is $n < \infty$ then order of a cyclic group m is—
(A) Infinity (B) $m = n$
(C) $m > n$ (D) $m < n$

60. If e_1 and e_2 are two identity elements of a group G then—
(A) $e_1 = e_2$
(B) $e_1 \neq e_2$
(C) $e_1 = ce_2$, for some c
(D) None of these

61. The idempotent element in a group are—
(A) Inverse elements of a group
(B) Identity element of a group
(C) Any element of a group
(D) None of these

62. Let G = {1, –1} then under ordinary multiplication (G, ·) is—
(A) Monoid (B) Semi-group
(C) Quasi-group (D) Group

63. Let Q be a set of rational numbers then under ordinary addition (Q, +) is—
(A) Monoid (B) Semi-group
(C) Quasi-group (D) Group

64. Let G be a group of square matrices of same order with respect to matrix multiplication then it is not a—
(A) Quasi group (B) Abelian group
(C) Semi-group (D) None of these

65. If G is a finite group, then for every $a \in$ G, the order of a is—
(A) Finite (B) Infinite
(C) Zero (D) None of these

66. In the additive group of integers, the order of every element $a \neq 0$ is—
(A) Infinity (B) One
(C) Zero (D) None of these

67. In the additive group of integers, the order of identity element is—
(A) Zero (B) One
(C) Infinity (D) None of these

68. In the additive group G of integers, the order of inverse element a^{-1}, $\forall\, a \in$ G is—
(A) Zero (B) One
(C) Infinity (D) None of these

69. The singleton {0} with binary operations addition and multiplication is ring and it is called—
(A) Zero ring (B) Division ring
(C) Singleton ring (D) None of these

70. The element $a \neq 0 \in$ R, the commutative ring is an integral domain if—
(A) $ab = 0$, $b \in$ R and $b = 0$
(B) $ab = 0$, $b \in$ R and $b \neq 0$
(C) $ab \neq 0$, $b \in$ R and $b = 0$
(D) $ab = 0$, $b \in$ R and $b = 0$

71. A ring R is an integral domain if—
(A) R is commutative ring
(B) R is commutative ring with zero divisor