LINEAR ALGEBRA

BINARY OPERATION – It can be defined as an operation which is performed on set G. The func^n is given by $A*A$ where $*$ is the operation $(+, -, \times, \div, \ldots)$

GROUPOID (closed)
↓ + Associative
SEMI GROUP
↓ + Identity element
MONOID
↓ + Inverse
GROUP
↓ + commutative
ABELIAN GROUP

CLOSED / CLOSURE PROPERTY
$\forall a, b \in G \quad a*b \in G$ (Means oper^n lagake jo bhi answer aayega wo G m hona chahiye)

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

IDENTITY ELEMENT
$a*e = e*a = a$ (Here $e \rightarrow$ identity element) (Mostly multiplic^n m $e=1$, add^n m $e=0$)

INVERSE
$a*a^{-1} = a^{-1}*a = e$ (In add^n $-a = a^{-1}$ In multiplic^n $a^{-1} = 1/a$)

COMMUTATIVE
$a*b = b*a$

PROPERTIES OF A GROUP

Theorem 1 The identity element of a group is unique → Let G have two identity element e and e'
e' is identity $ae' = a$ ($e \rightarrow$ Normal element)
e is identity $ae = a$ ($e' \rightarrow$)
since ee' is unique $ae' = ae$ $e' = e$

Theorem 2 The inverse of an element in a grp. is unique → Let a be any element of G which has 2 inverses b and c where $a, b, c \in A$

$a^{-1} = b \Rightarrow ba = e = ab$
$a^{-1} = c \Rightarrow ca = e = ac$
$ab = e$
$ab*c = e*c$
$b*(a*c) = c$
$b*e = c$
$b = c$

Since a^{-1} is inverse of a
$aa^{-1} = e$
$a^{-1}a = e$
Inverse of a^{-1} is a
$(a^{-1})^{-1} = a$

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

Agar y product ... then ab ki inverse $b^{-1}a^{-1}$ h

Theorem 3 If G is a group then $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$ (Reversal Law)

Theorem 4 If a, b are elements of a group g 'G' then eq^n $ax = b$ and ~~by=~~ ay... have unique soln

$a \in G$ then $a^{-1} \in G$
$a^{-1} \in G \quad b \in G \Rightarrow a^{-1}b \in G$
$a(a^{-1}b) = (aa^{-1})b \qquad a^{-1}b = x$
$= eb$
$= b$

Now let the eq^n have 2 soln
$ax_1 = b$ and $ax_2 = b$
$ax_1 = ax_2$
$x_1 = x_2$

HOW TO PROVE A SEMIGROUP IS A GROUP??

If all the elements a, b, of a semigroup G, eq^n $ax = b$ and $ya = b$ have unique s... in G, then G is a grp.

G being a semigroup is a non empty set. Let $a \in G$
$ax = a$ and $ya = a$
Now, let these soln be denoted by e_1 and e_2
$ae_1 = a$ and $ae_2 = a$ —①
If $b \in G$ then by the given property
$ax = b \qquad ya = b$

$(ya)e_1 = be_1$
$y(ae_1) = be_1$
$ya = be_1$
$b = be_1$
e_1 is the right identity

$ax = b$
$(e_2 a)x = e_2 b$
$ax = e_2 b$
$b = e_2 b$

SUBGROUP - A group G is called a cyclic group if

A non empty subset H of G is called a subgroup if i.e $a \in H, b \in H \rightarrow ab \in H$
H is stable (closed) for the composition defined in G
H itself is a group for the composition induced by that of G

Every group has two subgroups - the group itself and the identity element. These are IMPROPER or TRIVIAL ~~groups~~ (SUBGROUP)
A subgroup other than these two is a PROPER SUBGROUP

PROPERTIES OF A SUB-GROUP

Theorem 1 If H is a subgroup of G then
a) The identity of H is the same as identity of G.
b) The inverse of any element a of H is the same as the inverse of the same regarded as an element of G
c) The order of any element a of H is the same as the order of a in G

Let e and e' be identity elements of G and H
If $a \in H$ $ae' = e'a = a$
If $a \in H \rightarrow a \in G$ $ae = ea = a$
$ae' = ae$
$e' = e$

Let a be an element having two inverses b and c in H and G respectively
In H $ab = e$
In G $ac = e$
$\cancel{a}b = \cancel{a}c$
$b = c$

HOW TO PROVE A SUBGROUP
- $ab \in H$ $\forall a, b \in H$
- $e \in H$
- $a \in H$ $a^{-1} \in H$

$(a-b) \in H$ for addn

Theorem 2 A non void subset H of a group G is a subgroup iff $a \in H, b \in H \Rightarrow ab^{-1} \in H$

Considering H is the subgroup
if $a \in H$ $b \in H$ then $b^{-1} \in H$
$ab^{-1} \in H$ (by closure)

Considering the condn to be true then prove H is a subgroup $[a \in H$ $b \in H$ $ab^{-1} \in H]$
H is a non empty set
Identity element exists $e \in H$ $a^{-1} \in H$
$ea^{-1} = a^{-1} \in H$
Inverse exists
$a \in H$ $b \in H$ then $b^{-1} \in H$
$a(b^{-1})^{-1} = ab \in H$

Theorem 3 A non void finite subset H of a ~~subgroup~~ group G is a subgroup iff $a \in H, b \in H \Rightarrow ab \in H$

Considering H is a subgroup
If $a \in H$ $b \in H$
$ab \in H$ (closure)

$a \in H$ $b \in H \Rightarrow ab \in H$ is true
Then $a \in H \Rightarrow aa \in H = a^2 \in H$
$a, a^2, a^3, \ldots, a^n \in H$ $\forall n \in N$
But H is a finite subset, so all the powers of a cannot be distinct
$a^i = a^j$
$a^i a^{-j} = a^j a^{-j}$
$a^{i-j} = a^0$
$a^{i-j} = e$ (identity exists)

Theorem 4 Intersecn of any 2 subgroups of G is again a subgroup

Let H_1 and H_2 be two subgroups of G
$e \in G \Rightarrow e \in H_1, e \in H_2 \Rightarrow e \in H_1 \cap H_2$
Now let $a, b \in H_1 \cap H_2$
then $a, b \in H_1$ $a, b \in H_2$
$\Rightarrow ab^{-1} \in H_1$ $ab^{-1} \in H_2$
$ab^{-1} \in H_1 \cap H_2$
$H_1 \cap H_2$ is a subgroup

Theorem 5 If H and K are two subgroups of a group G then HK is a subgroup iff $HK = KH$

Let $HK = KH$
$(HK)(HK)^{-1}$
$= HKK^{-1}H^{-1}$
$= HKH^{-1}$
$= KHH^{-1}$
$= K(HH^{-1})$
$= KH$

HK is a subgroup of G
$(HK)^{-1} = HK$
$K^{-1}H^{-1} = HK$
$KH = HK$
($\because$ H, K are subgroups)

$b \quad f(a) \circ f(b)$ EPIMORPHISM

ORDER OF A GROUP → For a finite group G, the number of elements in a grp. is
s.t.b order of G

ORDER OF AN ELEMENT → element ko baar baar operⁿ lagane pe kitne set k elements generate hote hain

CYCLIC GROUP – A group G is called a cyclic group if there exists an element $a \in G$ such that $G=[a]$
i.e every element of G can be expressed as some integral power of a
Here a is called GENERATOR.

$G=\{\dots a^{-3}, a^{-2}, a^{-1}, a^{0}, a^{1}, a^{2}, a^{3}, \dots\}$ for $\times$

$G=\{\dots -3a, -2a, -a, 0, a, 2a, 3a, \dots\}$ for $+$

PROPERTIES OF A CYCLIC GROUP

Theorem 1 Every cyclic group is abelian. → $G=[a]$ be a cyclic group
$x, y \in G$ where
$x=a^m \quad y=a^n \quad m,n \in \mathbb{Z}$
$xy = a^m a^n = a^{m+n}$
$= a^{n+m} = yx$
$yx, xy \in G$

Theorem 2 If a is a generator of cyclic group G, then a^{-1} is also its generator.

let $G=[a]$ be a cyclic group
$x \in G \quad x=a^m$ where $m \in \mathbb{Z}$
$x = ((a^{-1})^{-m}) \quad -m \in \mathbb{Z}$
x can be expressed as an integral power of a^{-1}
a^{-1} is also a generator

Theorem 3 The order of finite cyclic group is equal to the order of its generator
o(finite cyclic group) = o(generator of group)

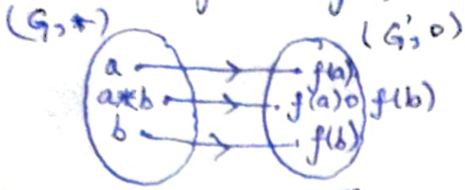
let $G=[a]$ be a finite cyclic group $o(a)=n$
let $H=\{a, a^2, a^3, \dots a^n\}$
H is a subgroup of G
when $m \leq n$ $a^m \in G$ then $a^m \in H$ $H \subset G$ — ①
$m > n$ $m = qn + r$
$(a^q)^n \cdot a^r$
$= a^r$
$G \subset H$ — ②
$G = H$
$o(H) = n = o(G) = n$

Theorem 4 Every finite cyclic group has two and only two generators

Theorem 5 Every subgroup of a cyclic group is also cyclic

HOMOMORPHISM - A mapping from Group $(G,*)$ to (G', o) is called Homomorphism if

$f(a*b) = f(a) \circ f(b)$



MONOMORPHISM → Homomorphism + one one (injection)

EPIMORPHISM → Homomorphism + onto (surjection)

ISOMORPHISM → Epimorphism + Monomorphism (one-one + onto + homomorphism)

ENDOMORPHISM → Homomorphism from G to itself

AUTOMORPHISM → Endomorphism + Isomorphism
f is a homomorphism from G to itself and it is one-one & onto

PROPERTIES OF HOMOMORPHISM

Theorem 1 If f is a homomorphism from G to G' and e and e' be their respective identity elements : then

$f(e) = e'$

Let $a \in G$, then $ae = a = ea$

$f(ae) = f(a) = f(ea)$

Homomorphism

$f(a).f(e) = f(a) = f(e).f(a)$

$f(e)$ is the identity element

$f(a^{-1}) = [f(a)]^{-1}$

a^{-1} be the inverse of $a \in G$

then $aa^{-1} = e = a^{-1}a$

$f(aa^{-1}) = f(e) = f(a^{-1}a)$

$f(a).f(a^{-1}) = e' = f(a^{-1}).f(a)$

$f(a^{-1}) = [f(a)]^{-1}$

Theorem 2 If f is a homomorphism of a group G to a group G'
H is a subgroup ⇒ f(H) is a subgroup

If H is a subgroup of G $f(H) \subset G'$

then $e \in H$

$f(e) = e'$

Let a', b' be elements of $f(H)$

$f(a) = a'$ $f(b) = b'$

$a'(b')^{-1} = f(a)[f(b)]^{-1}$

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

$= f(ab^{-1})$

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

$f(ab^{-1}) \in f(H)$

KERNEL OF HOMOMORPHISM → f be a homomorphism of a group G to G' then set K of all those elements of G which are mapped to the identity element of G' is called kernel of homomorphism

$Ker f = \{x \in G \mid f(x) = e'\}$

ISOMORPHISM - A homomorphism f of a group $(G,*)$ to a group (G', o) is an isomorphism if f is one-one, onto

f is one-one i.e $f(a) = f(b) \Rightarrow a = b$

f is onto $f(G) = G'$

f is a morphism $f(a*b) = f(a) \circ f(b)$ $\forall a, b \in G$

symbolically $G \cong G'$

Theorem 2 ... called idempoden ... for eg 8_n

PERMUTATION – A permutation of finite set S is the bijection from S to itself
$f: S \xrightarrow[\text{onto}]{1\text{-}1} S$ if $a \in S$ then $f(a) \in S$

$$f = \begin{bmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ f(a_1) & f(a_2) & f(a_3) & \dots & f(a_n) \end{bmatrix}$$

EQUALITY OF TWO PERMUTATION – Let f and g be two permutations then they are called equal iff $f(a) = g(a)$ $\forall a \in S$

Image of ~~both~~ every element under f and g are equal

IDENTITY PERMUTATION – Let S be a finite set of elements then a permutation is called identity permutation if $a = f(a)$ $\forall a \in S$ $\begin{bmatrix} a & b & c & \dots & n \\ a & b & c & \dots & n \end{bmatrix}$

PRODUCT OF COMPOSITION OF PERMUTATION – Let f and g be a permutation of A then the product of two permutation is also a combination of permutation

$$(f \cdot g)(x) = f \circ g(x) = f[g(x)]$$

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \quad g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$$

$$g \cdot f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix} \quad \cancel{gf} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix} = f \cdot g$$

$$f = (1\ 2\ 3\ 4) \qquad g = (1\ 3\ 2\ 4)$$

CYCLIC PERMUTATION OR CYCLES – A permutation σ of a set S is a cycle permutation or a cycle if $\exists$ a finite subset $(a_1, a_2, \dots, a_n)$ of S such that

$$\sigma(a_1) = a_2 \quad \sigma(a_2) = a_3 \quad \sigma(a_n) = a$$

If $\sigma(x) = x$ and $x \in S$
Then $x \notin (a_1, a_2, \dots a_n)$

ORDER OF CYCLE / LENGTH OF CYCLE – Number of elements in a cycle

ORDER OF CYCLE – Length of cycle (Kitni baar wo element ki image lene pe woi same element ayega)

INVERSE OF A CYCLE – $(a\ b\ c\ d) \to (d\ c\ b\ a)$

DISJOINT CYCLE – Two cycles are disjoint if they have nothing in common

Product of disjoint cycle commutes

ORDER OF PERMUTATION – LCM of disjoint cycle
Eg $(1\ 2)(3\ 4\ 5\ 6)$ Order $= \text{LCM}(2,4) = 4$

TRANSPOSITION – Any cycle of length 2
Every transposition is self inverse

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 2 & 5 & 1 & 3 & 8 & 7 \end{bmatrix}$$

$$(1\ 4\ 5)(2\ 6\ 3)(7\ 8)$$

Order $= \text{LCM}(3,3,2) = 6$

Transposition $\to (1,4)(1,5), (2,6), (2,3), (7,8)$

INTEGRAL DOMAIN.

INVERSION – If σ be a permutaⁿ then the pair (i, j) $0 < i < j \le n$ is an inversion for σ if $\sigma(i) > \sigma(j)$

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{bmatrix}$$

$1 < 3$ but $f(1) > f(3)$
$5 < 6$ but $f(5) > f(6)$
$2 < 3$ but $f(2) > f(3)$
$2 < 4$ but $f(2) > f(4)$
$(1,3), (2,3), (2,4), (5,6)$ are called inversion

SIGNATURE → Total number of inversions

EVEN AND ODD PERMUTATION – A permutation is called odd or even if its total no. of transposition are odd or even

Eg $\sigma = \{1\ 2\ 3\ 4\ 5\}$
$\sigma = (1\ 2)(3\ 3)(1\ 4)(1\ 5)$
Even transposition ⇒ Even permutaⁿ

Identity permutation is an even permutaⁿ
Every transposition is an odd permutaⁿ
Product of 2 even transposⁿ is an even transposⁿ
Product of 2 odd transposⁿ is an ~~odd~~ even transposⁿ
Product of even and odd is odd permutaⁿ

Transposition ↓ permutaⁿ

PERMUTATION GROUP – The set S_A of all permutⁿ of a non void set A is a group for product of permutⁿ and is denoted by $(S_A, o) = G$

Closure property → $f \in S_A$ and $g \in S_A$
$f o g \in S_A$

Associativity → $f, g, h \in S_A$ $fog(h) = f(og\ h) = f(gh)$
Identity → $I_A \in S_A$ (identity permutaⁿ) $f o I = f$
Inverse → $f o f^{-1} = I_A$

SYMMETRIC GROUP – The group of permutaⁿ of set $\{1, 2, \ldots, n\}$ is called symmetric group of degree n.
Order of this group → $n!$

symmetric group of ~~order 3~~ set $\{1,2,3\}$ contains 6 elements

$$P_0 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad P_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

$$\mu_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad \mu_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \quad \mu_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

ALTERNATING GROUP – Group of even permutaⁿ – The set A_n of all even permutⁿ of degree n is a group of order $\frac{n!}{2}$ for the product of permutⁿ