Elementry Topics in pure Mathemat

lecture # 01 MTH405

Introduction :- Set and Binary operation

1- Introduction to Group theory:-

* outlines
  - Introduction
  - Set
  - Binary operation.
  - Associative law
  - Group
  - Examples

* The term group was used by Galois in 1830 in order to describe set of one-to-one functions on finite sets under composition.

* Group theory is a Study of Symmetry.

Applications of Group theory:-

* Groups theory has its applications in Physics, Chemistry, Material Science etc.
* Crystals and molecules of hydrogen can be modeled with the help of Group Theory.
* Group theory is also used in Cryptography.

Scanned with CamScanner

Set:-

What is Set?

A Set is a collection of objects under certain rule.

In mathematics, we apply the Condition that the objects should be:-

- well defined
- Distinct

Example:-

- Set of the days of week
- Set of the newspaper of Pakistan

- Set is usually denoted by capital letters A, B, C, — X, Y, Z.
- The elements of a Set are denoted by small letter, a, b, c — x, y, z.

N = Set of the Natural number

= {1, 2, 3 — }

- R = Set of Real Number

$R = Q \cup Q'$

Scanned with CamScanner

* Binary Operation :-

* Let S be a non-empty set, The binary operation * is a function

$$* : S \times S \to S$$

which assigns each ordered pair (a, b) of $S \times S$, a unique element of S

* addition is a binary operation on Set 'S'.

* In other words, if * is the binary operation on a Set S, then for every $a, b \in S$

$$a * b \in S$$

Then S is called closed under the binary operation *.

Example 01 :-

Show that Multiplication is a binary operation on the Set of Natural numbers N.

Sol :- $N = \{1, 2, 3, \dots\}$

$7, 5 \in N$

$7 \times 5 = 35 \in N$

so, Multiplication is a binary operation on the set of N.

N is a Closed set on the multiplication binary operation.

Scanned with CamScanner

Example #02:-

Show that division is not binary operation on the set of Natural Numbers N.

$N = \{1, 2, 3, 4 \cdots\}$

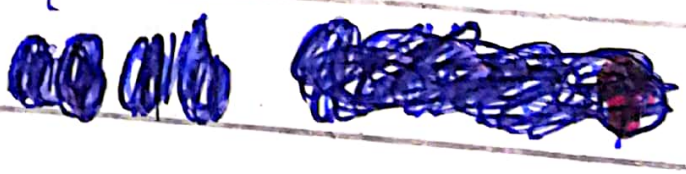
$4, 2 \in N$, $\therefore 4 \div 2 = 2 \in N$

, $2 \div 4 = 0.5 \notin N$

for all $x, y \in N$, $x \div y \notin N$

So $\div$ is not a binary operation on the set of natural numbers

x'



Scanned with CamScanner

Example #03:-

Show that Subtraction is not a binary operation on N.

$\because N = \{1, 2, 3, -\}$

$2, 3 \in N$

$3 - 2 = 1 \in N$

$2 - 3 = -1 \notin N$

So the Subtraction is not a binary operation

for all $x, y \in N$, $x - y \notin N$

Example #04:-

Show that division is a binary operation on R. => Rational Numbers

$\because R = Q \cup Q'$

$\frac{2}{3}, \frac{5}{7} \in R$

$\frac{2}{3} \div \frac{5}{7} = \frac{2}{3} \times \frac{7}{5} = \frac{14}{15} \in R$

$\sqrt{2} \div \sqrt{3} = \frac{\sqrt{2}}{\sqrt{3}} \in R$

for all $x, y \in R$, $x \div y \in R$

Hence $(\div)$ is a binary operation on 'R'.

Scanned with CamScanner

Example # 05:-

Show that the operation ○ (Cricle) defined by $x \circ y = 0$ for all $x, y \in z$ is a binary operation on z.

$$z = \{\dots, -3, -2, -1, 0, 1, 2, 3 \dots\}$$

$2, 3 \in z, \quad 2 \circ 3 = 0 \in z$

$x, y \in z, \quad x \circ y = 0 \in z$

Hence the operation '○' is a binary operation on set of integers.

Example # 06:-

Show that the operation ○ defined by:-

$x \circ y = x + y - xy$, for all, $x, y \in z$ is a binary operation on z.

$$z = \{\dots -3, -2, -1, 0, 1, 2, 3 \dots\}$$

$3, 5 \in z$

$$3 \circ 5 = 3 + 5 - (3)(5)$$
$$= 8 - 15$$
$$= -7 \in z$$

for $x, y \in z$

$x + y \in z$

$xy \in z$

$x + y - xy \in z$

$x \circ y \in z$

Scanned with CamScanner

lecture # 02

Groupied, Semi, Manoid & Group

Topic :- 01

Groupied definition

"A non-empty set with a binary operation is called Groupied."

for example :-

$$S \neq \phi$$

assume that binary operation is

$$(S, *)$$

for $x, y \in S$,

$$x * y \in S$$

for example :-

Suppose $N = \{1, 2, 3 \dots\}$

$$(N, +)$$

$3, 5 \in N$, $3+5 \in 8 \in N$

$x, y \in N$, $x+y \in N$

~~addv~~ set of Natural number is Closed under the addition operation on N

Scanned with CamScanner

Groupied Example #01:-

Show that, $(\mathbb{Z}, -)$ is a groupied under the operation of usual Subtraction.

Sol : $\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, \dots \}$

$3, 5 \in \mathbb{Z}, \quad 3 - 5 = -2 \in \mathbb{Z}$

Set of integer $\mathbb{Z}$ closed under the binary operation Subtraction

for $x, y \in \mathbb{Z}, \quad x - y \in \mathbb{Z}$

Groupied Example #02:-

Show that $(\mathbb{Z}, \div)$ is not a groupied under the operation of usual division.

$\mathbb{Z} = \{ \dots -3, -2, -1, 0, 1, 2, 3 \dots \}$

$1, 2 \in \mathbb{Z}, \quad 1 \div 2 \in \mathbb{Z}$

$1 \div 2 = 0.5$

$0.5 \notin \mathbb{Z}$

But Some integer are hold closer property.

for all $x, y \in \mathbb{Z}, \quad x \div y \notin \mathbb{Z}$ Hence $(\mathbb{Z}, \div)$ is not a groupied under the operation of division.

Scanned with CamScanner

Topic :- #02 :-

Semi Group

A non-empty set with an associative binary operation is called Semi-Group.

~~for example :-~~

$(S, *)$

Properties :-

(1) for all $x, y \in S$, $x * y \in S$

S is closed under $*$

(2) Associative law must hold.

for $x, y, z \in S$

$(x * y) * z = (y * z) * x$

Example #01 :-

Show that $N = \{1, 2, 3 \cdots\}$ is a Semigroup under the operation of addition

(1) $(N, +)$

$N = \{1, 2, 3 \cdots\}$

$11, 13 \in N$, $11 + 3 = 24 \in N$

Similarly, for $x, y \in N$, $x + y \in N$.

So, N is closed under the operation of addition.

(2) $7, 8, 9 \in N$

$(7+8) + 9 = 15 + 9 = 24 \in N$

$(8+9) + 7 = 7 + 17 = 24 \in N$

So the Associative law hold.

$(7+8) + 9 = 7 + (8+9)$

Scanned with CamScanner

for any $x, y, z \in N$,

$$(x+y)+z = x+(y+z)$$

So the set of N is Semigroup

Semigroup Example :- 02

Show that the set (Z, o) is a Semigroup, where o is the binary operation defined by :-

$$xoy = x+y-xy$$

$$Z = \{\cdots -3, -2, -1, 0, 1, 2, 3 \cdots\}$$

$$2, 3 \in Z$$

$$2o3 = 2+3-(2)(3)$$

$$= 5-6$$

$$= -1 \in Z$$

for $x, y \in Z$, $x+y \in Z$, $xy \in Z$

$$x+y-xy \in Z$$

$$xoy \in Z.$$

So the Closure property holds.

(2) Associative law

$$(xoy)oz = xo(yoz)$$

$$L.H.S = (xoy)oz$$

$$= [x+y-xy]oz$$

$$= (x+y-xy)+z-(x+y-xy)z$$

Scanned with CamScanner

$= x+y-xy+z-xz-yz+xyz$

$= x+y+z-xy-yz-xz+xyz \longrightarrow I$

R.H.S $= x \circ (y \circ z)$

$= x \circ (y+z-yz)$

$= x+(y+z-yz) - x(y+z-yz)$

$= x+y+z-yz-xy-xz+xyz$

$= x+y+z-xy-yx-xz+xyx \longrightarrow (ii)$

By I and II, Associative law holds.

$(x \circ y) \circ z = x \circ (y \circ z)$

Hence

$(Z, \circ)$ is a Semigroup, ~~whe~~ under the binary operation.

Topic # 03:- Monoid

"A non-empty set with an associative binary operation and an identity element is called Monoid."

Let S be a non-empty set

(1) Let $*$ be the binary operation on S.

for every $x, y \in S$, $x * y \in S$

So closure property holds.

(2) Associative law holds:-

for $x, y, z \in S$

$(x*y)*z = x*(y*z)$

Scanned with CamScanner

(3) Identity element exits in S;
for all $x \in S$, $e * x = x * e = x$
(e ↓ Identity)

Monoid example #01:-
Show that the Set $W = \{0, 1, 2, 3, \ldots\}$ is monoid under the binary operation of addition.

$W = \{0, 1, 2, \ldots\}$, $(W, +)$

(1) Closure property:-
$13, 15 \in W$
$13 + 15 = 28 \in W$
Hence the Closure property holds and addition is a binary operation.

(2) Associative law:-
we take any 3 whole numbers
$4, 5, 6, \in W$
$(4+5)+6 = 4+(5+6)$
$9+6 = 4+11$
$15 = 15$
So, associative law holds.
for any $x, y, z \in W$, $(x+y)+z = x+(y+$
Binary operation is fully ill.

Scanned with CamScanner

(3) Identity element :- $e = 0$

$2 + 0 = 2, \quad 0 + 2 = 2$

for any $x \in W$, $x + 0 = x = 0 + x$

So whole number set.

Since W satisfies all the three Conditions, so W is Monoied.

Topic :-04

Group :-

"A non-empty set with an associative binary operation, an identity elements and the inverses of its all elements is called Group."

let $S \neq \{\}$, $(S, *)$

A set of real numb

(1) Closure property :- is an abelian

for $x, y \in S$, $x * y \in S$ so group

Closure property holds. and the set S is closed under the binary operation $*$.

(2) Associative law :-

for $x, y, z \in S$

$(x * y) * z = x * (y * z)$

Scanned with CamScanner

(3) Identity element exists.

$e \in S$, for all $x \in S$

$$e * x = x * e = x$$

(4) Inverses of all elements of S exists in S.

for all $x \in S$, $\exists\, x^{-1} \in S$

Such that $x * x^{-1} = e = x^{-1} * x$

Therefore $(S, *)$ is a group

Scanned with CamScanner

Lecture # 03:-

Examples of Group.

Example # 01:-

Show that the set $\{1, -1\}$ is a group under multiplication:-

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

$\cdot$	1	-1
1	1	-1
-1	-1	1

(1) Closure property:-

for $x, y \in G$, $xy \in G$

Closure property hold.

(2) Associative law:-

$(1 \cdot (-1)) \cdot (-1) = 1((-1) \cdot (-1))$

$\Rightarrow (-1)(-1) = 1 \cdot (1)$

$\Rightarrow 1 = 1$

for all $(xy)z = x(yz)$

for all $x, y, z \in G$

(3) Identity element:-

$e \cdot x = x = x \cdot e$ for all $x \in G$

$e = 1$

$1 \cdot x = x \cdot 1 = x \quad \forall x \in G$

(4) Inverse element:-

for every $x \in G$, $\exists\, x^{-1} \in G$ s.t

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

$(1)(1) = 1$, $x = 1$, $x^{-1} = 1$

$(-1)(-1) = 1$, $x = -1$, $x^{-1} = -1$

Scanned with CamScanner

Hence Inverse of each element of G exists in G. So the set G satisfy all the four Condition of a Group.

So $G = \{1, -1\}$ is a Group under Mutliplication.

Example #02:-

Show that $(Z, +)$ is a group under the binary operation of addition.

(1) $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$

for example we take two integers:-

$10, 15 \in Z$, $10 + 15 = 25 \in Z$

for every $x, y \in Z$, $x + y \in Z$

So closure property holds.

(2) Associative law:-

$(x+y)+z = x+(y+z)$

$(3+4)+7 = 3+(4+7)$

$\Rightarrow 7+7 = 3+11$

$\Rightarrow 14 = 14$

Associative law holds for $x, y, z \in Z$ with respect to addition.

Scanned with CamScanner

③ Identity element :- $e = 0$

for any $x \in z$, $0 + x = x + 0 = x$

④ Inverse element of each $x \in z$.

$2 + (-2) = 0$

$-10 + 10 = 0$

for every $x \in z$ $\exists -x \in z$

Such that $x + (-x) = -x + x = 0$

Set 'z' hold all four properly hold

So, $('z', +)$ is ~~satisfies~~ a group

Example #03:-

Show that $(z - \{0\}, .)$ is not a group under the binary operation of Multiplication:- (except zero)

$z - \{0\} = \{ \dots -2, -1, 1, 2, \dots \}$

① Closure property:-

$3, 4 \in z$, $3 \times 14 = 12 \in z$

Closure property hold.

for any $x, y \in z$, , $xy \in z$

② Associative law:-

$2, 5, 4 \in z$

$(2 \times 5) \times 4 = 2 \times (5 \times 4)$

$10 \times 4 = 2 \times 20 \Rightarrow 40 = 40$

Scanned with CamScanner

for any $x, y, z \in \mathbb{Z}$

$(xy)z = x(yz)$

So Associative law hold.

(3) Identity element: $e = 1 \in \mathbb{Z} - \{0\}$

$1 \cdot x = x \cdot 1 = x \quad \forall x \in \mathbb{Z} - \{0\}$

Identity property hold.

(4) Inverse Element of each $x \in \mathbb{Z} - \{0\}$

$2 \times \left(\frac{1}{2}\right) = 1$

But $\frac{1}{2} \notin \mathbb{Z} - \{0\}$

for any $x \in \mathbb{Z} - \{0\}$ there is no-inverse

i.e, $\frac{1}{x} \notin \mathbb{Z} - \{0\}$

So, $\mathbb{Z} - \{0\}$ is not a group.

Example #04:-

Show that $G = \{1, w, w^2\}$ is a group under Multiplication, where w is a cube root of unity.

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

$\cdot$	1	w	w^2
1	1	w	w^2
w	w	w^2	$w^3 = 1$
w^2	w^2	$w^3 = 1$	w

$x = \sqrt[3]{1}$

$x = (1)^{1/3}$

$x^3 = 1$

$1, w, w^2$

$w^3 = 1$

$w^2 w^2 w^4 = w^3 \cdot w$

$= 1 \cdot w$

Scanned with CamScanner

(1) So it is clear from the table that Closure propety holds.

(2) Associative law:-

$1, \omega, \omega^2 \in G$

$(1 \circ \omega) \circ \omega^2 = 1 \circ (\omega \circ \omega^2)$

$\omega \circ \omega^2 = 1 \cdot \omega^3$

$\omega^3 = \omega^3$

$1 = 1$

for any x, y, z ~~from~~ $\in X$.

$(xy)z = x(yz)$

(3) Identity element:- $e = 1$

$\omega \circ 1 = 1 \circ \omega = \omega$

$\omega^2 \circ 1 = 1 \circ \omega^2 = \omega^2$

$1 \cdot 1 = 1 \cdot 1 = 1$

(4) Inverse element of each element $x \in G$

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

$\omega \cdot (\omega^2) = 1 \Rightarrow \omega^{-1} = \omega^2$

$\omega^2 \cdot (\omega) = 1 \Rightarrow (\omega^2)^{-1} = \omega$

Hence G satisfies all the conditions of group.

Hence G is a group under Multiplication.

Scanned with CamScanner

~~For~~ Example # 05:-

Show that $G = \{1, -1, i, -i\}$ is a group under Multiplication.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

① Closure property:-

It is clear from that table that the Closure property holds.

② Associative property:-

$(i(-i))(-1) = i((-i)(-1))$

$(-i^2)(-1) = i(i)$

$-(-1)(-1) = i^2$

$-1 = -1$

for any $x, y, z \in G$, $(xy)z = x(yz)$

③ Identity element:- $e = 1$

~~(+)~~ e for any element $x \in G$

$1 \cdot x = x \cdot 1 = x$

Identity element exists in G.

④ inverse element of each $x \in G$.

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

$(1)(1) = 1 \Rightarrow (1)^{-1} = 1$

$(-1)(-1) = 1 \Rightarrow (-1)^{-1} = -1$

$(i)(-i) = 1 \Rightarrow i^{-1} = -i$

$(-i)(i) = 1 \Rightarrow -i^{-1} = i$

Scanned with CamScanner

So, G_7 satisfies all four property of Group. So G_7 is a Group under Multiplication.

lecture # 04

Theorems on Group.

* **Theorem #01:-**

In a group G, the Identity element is unique.

Contrarily Suppose that Identity element is not unique.

Let e & e' be two Identity elemen

for $x \in G$,

$$xe = x = ex$$

$$e'e = e' = ee' \longrightarrow (1)$$

Now $ee' = e = e'e \rightarrow (2)$

By (1) and (2) $e = e'$

Hence our Supposition is wrong and So, Identity element is unique.

Scanned with CamScanner

Definition :-

An element a of a group G is called "Idempotent" if $a^2 = a$

$a \in G$, $a^2 = a$

$1^2 = 1$, $0^2 = 0$

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $I^2 = I$

Theorem #02 :-

The only Idempotent element in a group G is the Identity ?

Proof :-

Let $a \in G$ be an Idempotent element.

$$a^2 = a$$

$$aa = a$$

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

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

$$ea = e$$ ∵ Identity element ko ksi be element sy Multiply krne sy wo element khud aa jata hai.

$$a = e$$

Hence proved.

Scanned with CamScanner

Theorem #03:-

In a group G, the Inverse of each element is unique.

Suppose Contrarly that the Inverse of each element is not unique:-

So, let

a^{-1} & a'^{-1} be the inverses of $a \in G$.

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

and $$a'^{-1}a = e = aa'^{-1} \longrightarrow (2)$$

Consider $aa^{-1} = e$

Mutiplying both Sides by a'^{-1}.

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

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

$$ea^{-1} = a'^{-1} \quad \text{by eq (2)}$$

$$a^{-1} = a'^{-1}$$

So our Supposition is flase. Hence the inverse of each element is unique.

Scanned with CamScanner

Theorem # 04:-

If G is a Group, then $(a^{-1})^{-1} = a$

(for all) $\Leftarrow \forall a \in G$

Proof:-

Since G is a group, and

$a \in G$, $a^{-1} \in G$

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

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

$(a^{-1})^{-1}a^{-1} = e = a^{-1}(a^{-1})^{-1} \rightarrow (2)$

from eq (2)

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

Xing 'a' on both sides

$(a^{-1})^{-1}a^{-1})\,a = ea$

$a^{-1})^{-1}(a^{-1}a) = a$ $\Rightarrow$ By Associative law

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

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

Hence proved.

Scanned with CamScanner

Theorem #05:-

Let G be a group, then $(ab)^{-1} = b^{-1}a^{-1}$ $\forall\ a, b \in G$.

proof:-

Since G is a group and a and $b \in G$

then $ab \in G$ $\Rightarrow$ closure property

So $(ab)^{-1} \in G$

$a^{-1} \in G$, $b^{-1} \in G$

Therefore, $(ab)^{-1} = ab = e$ $\rightarrow$ (1)

xing both sides by b^{-1}

$((ab)^{-1}ab)\,b^{-1} = eb^{-1}$

By Accostive law

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

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

$((ab)^{-1}a) = b^{-1}$ $\rightarrow$ (2)

xing both sides by a^{-1}

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

By Associative law:-

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

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

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

Hence proved.

Scanned with CamScanner

Theorem #06:-

for any ~~theorem~~ - three elements, a, b, c of a group G,

(i) $ab = ac \Rightarrow b = c$ (Left Cancellation law)

(ii) $ba = ca \Rightarrow b = c$ (Right Cancellation law).

Proof:-

(i) $ab = ac$ $\quad \because a \in G, a^{-1} \in G$

Xing 'a^{-1}' on both sides:-

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

By Associative law:-

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

$$eb = ec$$

$$b = c$$ Hence proved.

(ii) $ba = ca$

'xing' a^{-1} on both side:-

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

By Associative law

$$b(aa^{-1}) = c(aa^{-1})$$

$$be = ce$$

$$b = c$$

Hence proved.

Scanned with CamScanner

~~Lecture #05:~~

ORDER of A Group

"The number of elements in a group G is called order of the group. It is denoted by $O(G)$ or $|G|$."

* **Finite Group:-**

"If a group has a finite number of elements, then it is called a finite group."

* **Infinite Groups:-**

"If a group has an infinite number of elements, then it is called an infinite group."

Example :- What is the order of the group $G = \{1, -1, i, -i\}$?

Since there are 4 elements in the group G.

$$O(G) = 4$$
$$|G| = 4$$

Example :- What is the order of the group, $G = \{1, -1, i, -i, j, -j, k, -k\}$?

Since there are 8 elements in the group G.

Scanned with CamScanner

So the order of G_7 is 8,

$$O(G_7) = 8$$

$$|G_7| = 8$$

Example:- What is the order of the group $(\mathbb{Z}, +)$?

$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2 \cdots\}$

Since there are infinite many elements in $\mathbb{Z}$;

$$O(\mathbb{Z}) = \infty$$

$$|\mathbb{Z}| = \infty$$

Example:- What is the order of the group $\{2^k; k = 0, \pm 1, \pm 2 \cdots\}$?

$G_7 = \{2^k; k = 0, \pm 1 \pm 2, \cdots\}$

Since the values of k are infinite So there are infinite many elements of the group in form 2^k.

So order of the group is infinity :-

$$|G_7| = \infty$$

Scanned with CamScanner

ORDER of an elements of a Group:-

Let G be a group and $a \in G$, then the order of 'a' is the least +ve integer n such that;

$a^n = e$ where 'e' is Identity

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

$e = 1$

$(1)^1 = 1$, order of 1 is 1 -

$(-1)^2 = 1$ order of $-1 = 2$

Example:-

Find the order of each element of the group:-

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

$(G, \cdot)$ Here $e = 1$

$(1)^1 = 1$ $\quad a^n = 1 \Rightarrow n = 1$

$\boxed{O(1) = 1}$

$(-1)^2, (-1)(-1) = 1 \Rightarrow \boxed{O(-1) = 2}$

$(i^2) = -1$ $\quad \because i = \sqrt{-1}$

$(i)^3 = i^2 \cdot i = -1 \cdot i = -i$

$(i)^4 = i^2 \cdot i^2 = (-1)(-1) = 1$

$\boxed{O(i) = 4}$

Scanned with CamScanner

$(-i)^2 = i^2 = -1$

$(-i)^3 = (-i^2)(-i) = (-1)(-i) = i$

$(-i)^4 = (-i^2)(-i^2) = (-1)(-1) = 1$

$\boxed{O(-i) = 4}$

Example:-

find the order of each element of the group

$G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

of residue class modulo 5, under addition.

Here, $e = \bar{0}$

$\bar{0} = \bar{0}$ $\quad \boxed{O(\bar{0}) = 1}$

$\bar{1} + \bar{1} = \bar{2}$

$\bar{1} + \bar{1} + \bar{1} = \bar{3}$

$\bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{4}$

$\bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0}$

$\boxed{O(\bar{1}) = 5}$

$5 \overline{)5}\ 1$, 5, 0

$\bar{2} + \bar{2} = \bar{4}$

$\bar{2} + \bar{2} + \bar{2} = \bar{1}$

$\bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{3}$

$\bar{2} + \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{0}$

$\boxed{O(\bar{2}) = 5}$

$5 \overline{)6}\ 1$, 5, 1

$5 \overline{)8}\ 1$, 5, 3

$\boxed{a^n = e}$ $\quad \boxed{na = e}$

Scanned with CamScanner

$\bar{3}+\bar{3} = \bar{1}$

$\bar{3}+\bar{3}+\bar{3} = \bar{4}$

$\bar{3}+\bar{3}+\bar{3}+\bar{3} = \bar{2}$

$\bar{3}+\bar{3}+\bar{3}+\bar{3}+\bar{3} = \bar{0}$

$\boxed{o(\bar{3}) = 5}$

Similarly, $\boxed{o(\bar{1}) = 5}$

$$5\overline{)9}\ (1,\ 5,\ 4)$$

$$5\overline{)12}\ (2,\ 10,\ 2)$$

Theorem:- If n is the order of an element 'a' of a group G, then for any integer m, $a^m = e$ if and only if $m = qn$, where q is an integer.

$a^m = e$ if and only if n divides m.

Given :- $a \in G$

$a^n = e \rightarrow$ (i) n is least +ve inte

Suppose $a^m = e \rightarrow$ (ii)

By division algorithm, there exist $q, r \in x$, such that

$m = qn + r \quad 0 \le r < n$

$$n\overline{)m}\ (q,\ r)$$

By eq (ii)

$a^m = e$

$a^{qn+r} = e$

$a^{qn} \cdot a^r = e$

$(a^n)^q \cdot a^r = e$

Scanned with CamScanner

$e^q \cdot a^r = e$ $\because a^n = e$

$e^q \cdot a^r = e$ ~~$e^r = e$~~

$e \cdot a^r = e$ $e^q \cdot a^r = a^r$

$a^r = e$

It is possible only when

$r = 0$

$m = qn + r$

$= qn + 0$

$m = qn$

n divides m.

Conversely, suppose that

$m = qn$

Consider:-

$a^m = a^{qn}$

$= (a^n)^q$

$= e^q$

$a^m = e$

Hence it is proved.

Scanned with CamScanner

Theorem:-

Show that in a group, the order of an element is same as that of its inverse?

Let G be a group, $a \in G$

Suppose $a^n = e$ ——— (1)

$(a^{-1})^m = e$ ——— (2)

Now we have to prove that $n = m$

By eqn (1)

$$a^n = e$$

$$a^{-n} a^n = a^{-n} e$$

$$a^{-n+n} = a^{-n}$$

$$e = a^0 = a^{-n}$$

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

But the order of a^{-1} is m, so n must divide n ——— I

By eqn (2)

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

$$a^{-m} = e$$

$$a^m a^{-m} = a^m e$$

$$a^{m-m} = a^m$$

$$a^0 = a^m$$

$$e = a^m$$

But the order of a is n, so n must devide m ——— II

Scanned with CamScanner

It is possible only when

$m = n$

Hence it is proved.

Theorem:-

Let G be a group and $a, b \in G$ show that the order of ab and ba are of equal.

Let $(ab)^n = e$ → (1)

$(ba)^m = e$ → (2)

from eq (1) $(ab)^n = e$

$(ab)(ab) \cdots (ab) = e$ n-factors.

$a^{-1}a(bab \cdots bab) = a^{-1}e$

$e(baba \cdots bab) = a^{-1}$

$ba \cdot ba \cdots ba \cdot b = a^{-1}$

$ba \cdot ba \cdots ba \cdot ba = a^{-1}a$

$(ba)^n = e$

By equation 2 the order of ba is m,

Therefore m must divide n → (A)

from (2)

$(ba)^m = e$

$ba \cdot ba \cdots ba = e$ n-factors.

$b^{-1}(ba \cdot ba \cdots ba) = b^{-1}e$

$b^{-1}b(a \cdot ba \cdots ba) = b^{-1}$

Scanned with CamScanner

$e(ab.ab \cdots ba) = b^{-1}$

$ab.ab \cdots ab.a = b^{-1}$

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

$ab.ab \cdots ab.ab = e$

$(ab)^m = e$

But from eq ①, the order of ab is n. So m must divide n. —→ Ⓑ

By Ⓐ & Ⓑ, $m = n$

$O(ba) = O(ab)$

Hence proved.

Scanned with CamScanner

lecture #06.-

Abelian group:-

Let $(G, *)$ be a group, then G is called an Abelian group or Commutative group if the commutative law holds in G with respect to $*$ i.e.

$$x * y = y * x \quad \text{for all } x, y \text{ in } G$$

Non-Abelian group:-

Let $(G, *)$ be a group, the G is called a Non-Abelian group or Non-Commutative group if the Commutative law does not hold in G with respect to $*$, i.e.

$$x * y \neq y * x \quad \text{for all } x, y \text{ in } G.$$

Example:-

Show that the group $(\mathbb{Z}, +)$ is an Abelian group.

$\mathbb{Z} = \{ \dots, -1, 0, 1 \dots \}$

$10 + 21 = 31$

$21 + 10 = 31$

for all $x, y \in \mathbb{Z}$

$x + y = y + x$

$\mathbb{Z}$ is an abelian group

① Closure property.
② Associative law
③ Identity
④ Inverse
⑤ Commutative law.

Scanned with CamScanner

Example:-

Show that the group $(R, +)$ is an Abelian Group

$2 \cdot 5 + 3 \cdot 5 = 6 \cdot 0$

$3 \cdot 5 + 2 \cdot 5 = 6$

for all $x, y \in R$,

$x + y = y + x$

So Commutative law holds.

So $(R, +)$ is an Abelian group.

Example:-

Show that the group $G = \{1, \omega, \omega^2\}$ where ω is the cube root of unity. is an Abelian group

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

$\omega \cdot \omega^2 = \omega^3 = 1$

$\omega^2 \cdot \omega = \omega^3 = 1$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

for all $x, y \in G$,

$xy = yx$ So Commutative law holds.

So G is an abelian group.

Example:-

Show that the group $(1, -1, i, -i$ is an Abelian group.

Scanned with CamScanner

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

$i(-i) = 1$

$(-i)(1) = 1$

$-1 \cdot i = -i$

$i \cdot (-1) = -i$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

for any $x, y \in G$

$xy = yx$

So G is an abelian group.

Example:-

Show that the group $(1, -1, i, -i$ $j, -j, k, -k)$ is a Non-Abelian Group.

$ij = -ji$ $\quad ij \neq ji$

$jk = -kj$ $\quad jk \neq kj$

$ki = -ik$ $\quad ki \neq ik$

So the given is not Abelian.

① Closure Property

② Associative law

③ Identity

④ Inverse exi

⑤ Commutative law.

Example:-

Show that the set of non-singular matrices of order 2 is a Non-Abelian Group.

Scanned with CamScanner

G_7 : Set of non-singular matrices of order 2.

(1) Closure property :-

Let $A, B \in G_7$, $AB = C \in G_7$

(2) Associative law :-

$(AB)C = A(BC)$

(3) Identity Element exists :-

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ such that

$AI = A = IA$ $\forall A \in G_7$

(4) Inverse of each element in G_7 :-

Since G_7 has non-singular matrices

So for all $A \in G_7$.

$\exists A^{-1} \in G_7$, $A^{-1}A = I = AA^{-1}$

(5) Commutative law :-

In general

$AB \neq BA$

So Commutative law does not hold,

So G_7 is a non-abelian group.

Scanned with CamScanner

Theorem:-

Show that a group G is abel if and only if $(ab)^2 = a^2b^2$ for all a, b in G.

Let G be an abelian.

$ab = ba \rightarrow (1) \quad \forall a, b \in G$

Consider $(ab)^2 = (ab)(ab)$

$= a(ba)b$

$= a(ab)b \rightarrow$ by (1)

$= (aa)(bb)$

$= a^2 b^2$ Hence proved.

Now Conversely Suppose that:-

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

$(ab)(ab) = (aa)(bb)$

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

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

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

$e(ba)b = e(ab)b$

$(ba)b = (ab)b$

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

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

$(ba)e = (ab)e$

$ba = ab$

So the Commutative law holds, so G is an abelian group.

Hence proofs.

Scanned with CamScanner

Theorem:-

If a group G is such that $a \cdot a = e$ for all a in G. where e is identity, then G is an Abelian group.

Let $a, b \in G$

$a \cdot a = e \rightarrow (1)$

$b \cdot b = e \rightarrow (2)$

By (1) $a^{-1}(a \cdot a) = a^{-1}e$

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

$ea = a^{-1}$

$a = a^{-1} \rightarrow (3)$

By (2)

$b \cdot b = e$

$b^{-1}(b \cdot b) = b^{-1}e$

$(b^{-1}b)b = b^{-1}e$

$eb = b^{-1}$

$b = b^{-1} \rightarrow (4)$

Since $a, b, \in G$, $ab \in G$.

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

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

$ab = ba$

Since the Commutative law hold.

So G is an Abelian group.

Scanned with CamScanner

Theorem:-

If each element of a group G is its own inverse, then show that G is an Abelian group.

Let $a, b, \in G$,

$a = a^{-1} \rightarrow (1)$

$b = b^{-1} \rightarrow (2)$

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

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

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

$ab = ba$

So G is an Abelian group.

Theorem:-

If a group G has three elements then show that G is an Abelian Group:- $(a \neq b \neq e)$

Let $G = \{a, B, b\}$

from the table, it is clear that $a^2 \in G$.

There are three possibilities.

(i) $a^2 = e$ $\quad a \neq b \neq e$

(ii) $a^2 = a$

(iii) $a^2 = b$

$\cdot$	e	a	b
e	e	a	b
a	a	a^2	ab
b	b	ba	b^2

Scanned with CamScanner

Case (i): Suppose $a^2 = e$ X

Since $ab \in G$ then

1) $ab = e \Rightarrow a(ab) = ae \Rightarrow a^2 b = a$

2) $ab = a \Rightarrow b = e$ Not possible

3) $ab = b$

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

$ae = e$

$a = e$ Not possible.

$ab = a$
$b = a$
It is not possi

Case (ii) Suppose $a^2 = a$

$aa = a$

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

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

$ea = a^{-1}e$

$a = e$ Not possible.

Case (iii)

$G = \{e, a, a^2\}$

Clearly the elements of the group G satisfy Commutative law.

So G is an abelian group.

$a^2 = e$ X

$a^2 = a$ X

$a^2 = b$

(1) 2 1

Scanned with CamScanner

Lecture #07

Subgroups:-

Let $(G, *)$ be a group and H be a subset of G. If H is itself a group under the same binary operation $*$.

Then H is called a subgroup of G.

Example:-

(i) $H = \{1, -1\}$ is a subgroup of $\{1, -1, i, -i\}$ under the binary operation of '.'.

(2) $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$

(3) $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$

(4) $(\mathbb{R}, +)$ is a subgroup of $(\mathbb{C}, +)$

Remarks:-

If H is a subset of a group G and H is a group under different binary operation than that of group G, then 'H' is not called a subgroup of G.

$H = \{1, -1\}$ $(H, \cdot)$

$\mathbb{Z} = \{\cdots, -1, 0, 1 \cdots\}$, $(\mathbb{Z}, +)$

$H \subset \mathbb{Z}$

H is not a subgroup of $\mathbb{Z}$.

Scanned with CamScanner

Trivial Subgroups:-

Every group G has at least two subgroups $\{e\}$ and G itself. These two subgroups $\{e\}$ and G are called trivial subgroups of G.

Example: $G = \{1, -1, i, -i\}$

$\{1\}$, $\{1, -1, i, -i\}$

Non-Trivial Subgroup:-

Any subgroups of a group G, other than $\{e\}$ and G are called non-trivial subgroups of G.

Example:-

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

Trivial Subgroups: $\{1\}$, $\{1, -1, i, -i\}$

Non-Trivial Subgroups: $\{1, -1\}$

Theorem:-

Let $(G, *)$ be a group. A non-empty subset H of G is a subgroup of G if and only if:-

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

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

where a^{-1} is the inverse of a.

Scanned with CamScanner

Suppose H is subgroup of G.
Since H is a group.
So closure property holds, for any $a, b \in H$, $a * b \in H$
and inverse of each element of H exists.
for all $a \in H$, $a^{-1} \in H$ Hence proved.
Conversely, suppose that.
for $a, b \in H$, $a * b \in H$ —(1)
for $a \in H$, $a^{-1} \in H$ —(2)

C_1 : Closure property holds by (1)
C_2 : Associative law:
Since $H \subseteq G$ and associative law holds in G, so the associative law holds in H, too.

C_3 : By (2) for $a \in H$, $a^{-1} \in H$,
So inverse of every element of H exists,
C_4 : By (1) $a, a^{-1} \in H$, $a * a^{-1} \in H$
So identity exists in H.
So H is the subgroup of G.

Scanned with CamScanner

Theorem:-

The intersection of any collection of subgroups of a group $(G, *)$ is a subgroup of G.

Let $(G, *)$ be a group.

$\{H_d, d \in I\}$ be a collection of subgroups, of G.

$\bigcap_{d \in I} H_d$ is the intersection of all H_d, $d \in I$.

Suppose $a, b \in \bigcap_{d \in I} H_d$

$\Rightarrow a, b \in H_d$, for all $\alpha \in I$

$a * b^{-1} \in H_d$, for all $\alpha \in I$

H_d are groups.

$\Rightarrow a * b^{-1} \in \bigcap_{d \in I} H_d$

Let $a, b \in H$

$a * b^{-1} \in H$

So H is a subgro

Hence $\bigcap_{d \in I} H_d$ is a subgroup of G. Hence the proof.

Theorem:-

The union of two subgroups H and K of a group G is a subgroup of G if and only if either $H \subseteq K$ and $K \subseteq H$.

Scanned with CamScanner

HUK is a subgroup of G if and only if either $H \subset K$ or $K \subset H$

Suppose either $H \subset K$ or $K \subset H$.

When $H \subset K \Rightarrow HUK = K$

Since K is a subgroup of G so HUK is also a subgroup of G.

When $K \subset H \Rightarrow HUK = H$

Since H is a subgroup of G, So HUK is also a subgroup of G.

Hence the proof.

Now Suppose that HUK is a subgroup of G, then we have to show that either $H \subset K$ or $K \subset H$.

Suppose contrarily, $H \not\subset K$ or $K \not\subset H$

if $a \in H$, then $a \notin H \rightarrow (A)$

if $b \in H$, then $b \notin H \rightarrow (B)$

Scanned with CamScanner

then $a, b \in H \cup K$

$a * b \in H \cup K$ $\because H \cup K$ is a subgroup of G.

$a * b \in H$ or $a * b \in K$

When $a * b \in H$, then $a^{-1} * (a * b) \in$

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

$e * b \in H$

$b \in H$

Which contradicts to (B)

When $a * b \in K$, then

$(a * b) * b^{-1} \in K$

$a * (b * b^{-1}) \in K$

$a * e \in K$

$a \in K$

which contradicts (A)

So our Supposition that $H \not\subset K$ or $K \not\subset H$ is wrong

Therefore either $H \subset K$ or $K \subset H$

Hence proved.

Scanned with CamScanner

Theorem:-

The union of two subgroups H and K of a group G is a subgroup of G if and only if either $H \subset K$ or $K \subset H$.

HUK is a subgroup of G, if and only if :-

either $H \subset K$ or $K \subset H$

Suppose either $H \subset K$ or $K \subset H \rightarrow (1)$

When $H \subset K \Rightarrow HUK = K$

Since K is a subgroup of G.

So HUK is also a subgroup of G. When $K \subset H \Rightarrow HUK = H$

Since H is a subgroup of G.

Hence the proof.

Now suppose that HUK is a subgroup of G, then we have to show that either $H \subset K$ or $K \subset H$.

Suppose contrarily, $H \not\subset H$ or $K \not\subset H$

Scanned with CamScanner

if $a \in H$, then $a \notin K \rightarrow (A)$
if $b \in K$, then $b \in H \rightarrow (B)$
the $a, b \in H \cup K$
$a * b \in H \cup K$
$a * b \in H$ or $a * b \in K$
When $a * \in H$, then $a^{-1} * (a * b) \in$
$(a^{-1} * a) * b \in H$
$e * b \in H$
$b \in H$
When contradicts to (B)
when $a * b \in K$ then
$(a * b) * b^{-1} \in K$
$a * (b * b^{-1}) \in K$
$a * e \in K$
$a \in K$
which contradicts (A)
So our supporition that is
$H \not\subset K$. or $K \not\subset H$ is wrong
Therefore either $H \subset K$ or $K \subset H$
Hence proof.

Scanned with CamScanner

MTH 405
Lecture # 08

Definition :-

Let G be a group under multiplication, then G is called cyclic group. if each element of G can be written as a power of an element $a \in G$.

Let $a \in G$.

for all $x \in G$.

$x = a^n$ for $n \in \mathbb{N}$

$G = \langle a ; a^n = e \rangle$

Example :-

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

$(-1)^1 = -1$

$(-1)^2 = 1$

So G is a cyclic group generated by -1.

Scanned with CamScanner

Examples:-

Let $G = \{1, -1, i, -i\}$, Show that G is a cyclic group.

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

$(1)^1 = 1$ $\quad (i)^1 = i$ $\quad i = \sqrt{-1}$

$(1)^2 = 1$ $\quad (i)^2 = -1$ $\quad i^2 = (\sqrt{-1})^2$

$(-1)^1 = -1$ $\quad i^3 = i^2 \cdot i$ $\quad i^2 = -1$

$(-1)^2 = 1$ $\quad = -i$

$(-1)^3 = -1$ $\quad (i)^4 = i^2 \cdot i^2$

$(-1)^4 = 1$ $\quad = (-1)(-1)$

$= 1$

$G = \langle i : i^4 = 1 \rangle$

$(-i)^1 = -i$

$(-i)^2 = i^2 = -1$

$(-i^3) = -i^3 = -i^2 \cdot i$

$= -(-1)i$

$= i$

$(-i)^4 \; i^4 = i^2 \cdot i^2 = (-1)(-1)$

$= 1$

$G = \langle -i : (-i)^4 = 1 \rangle$

Scanned with CamScanner

Theorem:-

Every cyclic group is an abelian group.

Let G be a cyclic group with the generators a.

Let $x, y \in G$ such that

$x = a^m$, $y = a^n$. $m, n \in Z$

Consider

$$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$$

$xy = yx$ for $x, y \in G$

Hence G is an abelian group

Remark 1:

A cyclic group may have two generators.

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

$(i)^1 = i$ $\quad (-i)^1 = -i$ $\quad |G| = 4$

$(i)^2 = -1$ $\quad (-i)^2 = -1$ $\quad i^4 = (-i)^4 = 1$

$i^3 = -i$ $\quad (-i)^3 = i$ $\quad |i| = |-i| = 4$

$i^4 = 1$ $\quad (-i)^4 = 1$

$G = \langle i \rangle$, $G = \langle -i \rangle$

Scanned with CamScanner

Remark 2: $a \in G$

$a^n = e$

$aaa \cdots a = a^n$ n-times

$aa = a^2$

$aaa = a^3$ $\because G = \{1, -1, i, -i\}$

$(G', +)$ $a \in G'$, $e' \in G'$

$\boxed{na} = a + a + \cdots + a = e'$

$a + a = 2a$, $a + a + a = 3a$

Theorem :-

✓ Every Subgroup of a cyclic group is cyclic?

Let G be a cyclic group generated by $a \in G$.

Let H be a Subgroup of G.

$a^k \in H$ k is least +ve Integer.

Let $b \in H$ be an arbitrary element of H,

So $b = a^m \in H$ for some integer m.

$k < m \rightarrow (1)$

Scanned with CamScanner

By division algorithm, $\exists q, r$ such that

$m = qk + r, \quad 0 \leq r \leq k$

$$k \overline{)\, m \,(\, q \,}$$
$$\underline{\quad}$$
$$r$$

Consider

$a^m = a^{qk+r} \longrightarrow (2)$

$a^m = a^{qk} \cdot a^r$

$a^m \cdot a^{-qr} = a^{qk} a^r a^{-qk}$

$= a^{qk - qk} a^r$

$= a^0 a^r$

$a^m \cdot (a^k)^{-q} = a^r$

Since $a^k \in H$, $(a^k)^{-q} \in H$ $\therefore H$ is Subgroup.

Also $a^m \in H$, $a^m \cdot (a^k)^{-q} \in H$

$a^r \in H$

It is possible when $r = 0$

So $a^m = a^{qk+0}$

$b = a^m = (a^k)^q$

Hence a^k is the generator of H. Therefore H is a cyclic group.

Hence Prove.

Scanned with CamScanner

Theorem:-

The order of a cyclic group is equal to the order of its generator?

Let G be a cyclic group generated by a.

and $|G| = n$

So its elements are $a, a^2, a^3, \dots a^n$.

We have to Show that $|a| = n$

$$a^n = e$$

Suppose that the order of a is m,

$$m < n$$

$$a^m = e$$

$$a^m a = ea$$

$$a^{m+1} = a$$

$$a^{m+1} a = aa$$

$$a^{m+2} = a^2$$

$$\vdots$$

$a, a^2, a^3, \dots a^m, a^{m+1}, a^{m+2}, \dots a^n$

$a, a^2, a^3 \dots e, a, a^2 \dots, \dots a^n$

Which is Contradiction that there n elements in G.

Scanned with CamScanner

$a^m = e$, $m < n$

is Wrong.

$a^n = e$

$a, a^2, a^3, \ldots, a^n$

$a^r = a^s \quad 0 < s < r < n$

$a^r a^{-s} = a^s a^{-s}$

$a^{r-s} = a^{s-s}$

$a^{r-s} = a^0$

$a^{r-s} = e$, $r - s < n$

Which is the Contradiction :-

So, $a^r \neq a^s$

$a^n = e$

Hence $|a| = n$

$|G| = |a| = n$

Theorem :- Show the group ~~of the Student~~ $(Q, +)$ is abelian but not cyclic?

$Q = \left\{ \frac{p}{q} \mid p, q \in Z, q \neq 0 \right\}$

Since Commutative law holds :-

w.r.t. $+$,

$a + b = b + a \quad \forall a, b \in Q$

So $(Q, +)$ is an abelian group.

Suppose Contrarily that Q is

Scanned with CamScanner

cyclic. and can be generated by $a \in Q$.

$a = \frac{p}{q}$, $p, q \in Z$.

for $x \in Q$, $x = na$

$\frac{1}{2q} \in q$, so $\frac{1}{2q} = na$

$$\frac{1}{2q} = n\frac{p}{q}$$

$$\frac{1}{2} = np$$

But the product of two integers is integers. so (1) is wrong.

Hence every rational number cannot be written in form generator.

so $(Q, +)$ is not a cyclic.

Theorem :-

Let G be a cyclic group of order n generated by a, then for each positive divisor of d of n, there is a unique subgroups (of G) of order d

$G = \langle a : a^n = e \rangle$

Suppose d divides n, $n = qd$

Scanned with CamScanner

let $b \in G$, $b = a^q$

$$(b)^d = (a^q)^d$$

$$b^d = a^{qd} = a^n = e$$

$H = \langle b : b^d = e \rangle$

which is the required subgroup of G. Suppose contrarily that subgroup of order d is not unique, there exists another subgroup K of order d. K is generated by an element $c = a^k$.

Since order of K is d, so

$$a^k = c$$

$$(a^k)^d = c^d$$

$$a^n = c^d$$

$$e = c^d$$

$kd = n$, $qd = n$

$$kd = qd$$

$$k = q$$

$$b = a^q = a^k$$

$$K = H$$

Hence H is a unique subgroup of order d.

Scanned with CamScanner

Theorem :-

If G is a cyclic group of even order, then prove that there is only one subgroup of order 2 in G?

Let G be a cyclic group with even order.

$|G| = 2n$ n is +ve integer

By pervious theorem, if a +ve integer d divides order of a group G, then there will be a subgroup of order d.

Since 2 divides $2n$, so there must exist a subgroup of order 2.

Hence proved.

Scanned with CamScanner

Lecture #09

* **Left Coset:-**

Let H be a subgroup of a group G and $a \in G$. Then the set :

$$aH = \{ah, h \in H\}$$

is called a left coset of H in G determine by a.

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

$H = \{1, -1\}$

$i \in G$, $iH = \{i \cdot 1, i(-1)\} = \{i, -i\}$

* **Right Coset:-**

Let H be a subgroup of a group G and $a \in G$, then the set :-

$$Ha = \{ha, : h \in H\}$$

is called a Right coset of H in G determined by a.

Example:- $G = \{1, -1, i, -i\}$

$H = \{1, -1\}$

$Hi = \{1 \cdot i, -1, i\}$

$= \{i, -i\}$

Scanned with CamScanner

Remark 1:-

The left cosets of H in G determine by the Identity element e is H itself.

$$eH = \{eh, : h \in H\} = \{h : h \in H\} = H$$
$$He = \{he : h \in H\} = \{h : h \in H\} = H$$

Remark 2:-

If the binary operation of the group G is $+$, then the left cosets of H in G determined by a is given by:-

$$a + H = \{a + h : h \in H\}$$
$$H + a = \{h + a : h \in H\}.$$

Example #01:-

Find all the left Costs of $H = \{1, -1\}$ in $G = \{1, -1, i, -i\}$.

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

$H = \{1, -1\}$ $\quad a \in G, aH$

$1 \in G, \ 1H = \{1 \cdot 1, 1 \cdot (-1)\} = \{1, -1\}$

$-1 \in G \Rightarrow -1H = \{-1 \cdot 1, -1 \cdot (-1)\} = \{-1, 1\}$

$i \in G \Rightarrow iH = \{i \cdot 1, i(-1)\} = \{i, -i\}$

$-i \in G \Rightarrow -iH = \{-i \cdot 1, (-i)(-1)\} = \{-i, i\}$

Scanned with CamScanner

Example #02:-

Find all the right cosets of $H = \{1, -1\}$ in $G = \{1, -1, i, -i\}$

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

$H = \{1, -1\}$ $\quad a \in G$, aH

$1 \in G \Rightarrow H1 = \{1 \cdot 1, -1 \cdot 1\} = \{1, -1\}$

$-1 \in G \Rightarrow H(-1) = \{1 \cdot (-1), (-1)(-1)\} = \{-1, 1\}$

$i \in G \Rightarrow H(i) = \{1 \cdot (i), (-1)(i)\} = \{i, -i\}$

$-i \in G \Rightarrow H(-i) = \{1(-i), (-1)(-i)\} = \{-i, i\}$

Example #03:-

Let $G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ be the group of residue classes modulo 6 under addition, and $H = \{\bar{0}, \bar{2}, \bar{4}\}$ is the subgroup of G, then find left and right cosets of H in G.

$\bar{0} \in G$, $\bar{0} + H = \{\bar{0} + \bar{0}, \bar{0} + \bar{2}, \bar{0} + \bar{4}\} = \{\bar{0}, \bar{2}, \bar{4}\}$

$\bar{1} \in G$, $\bar{1} + H = \{\bar{1} + \bar{0}, \bar{1} + \bar{2}, \bar{1} + \bar{4}\} = \{\bar{1}, \bar{3}, \bar{5}\}$

$\bar{2} \in G$, $\bar{2} + H = \{\bar{2} + \bar{0}, \bar{2} + \bar{2}, \bar{2} + \bar{4}\} = \{\bar{2}, \bar{4}, \bar{0}\}$

$\bar{3} \in G$, $\bar{3} + H = \{\bar{3} + \bar{0}, \bar{3} + \bar{2}, \bar{3} + \bar{4}\} = \{\bar{3}, \bar{5}, \bar{1}\}$

$\bar{4} \in G$, $\bar{4} + H = \{\bar{4} + \bar{0}, \bar{4} + \bar{2}, \bar{4} + \bar{4}\} = \{\bar{4}, \bar{0}, \bar{2}\}$

$\bar{5} \in G$, $\bar{5} + H = \{\bar{5} + \bar{0}, \bar{5} + \bar{2}, \bar{5} + \bar{4}\} = \{\bar{5}, \bar{1}, \bar{3}\}$

Scanned with CamScanner

In same manner we find Right cosets of group.

Example # 04:-

Partition of a set A :- (subset)

The collection $\{A_\alpha : \alpha \in I\}$ of subsets of a set A is called the partition of A if

(i) $A = \bigcup_{\alpha \in I} A_\alpha$

(ii) $A_\alpha \cap A_B = \phi$ for $\alpha \neq B$

Scanned with CamScanner

Lecture # 10 MTH405

Lagrange's Theorem

1- Index of a subgroup:-

Index of H in G:-

"The number of distinct left cosets of a subgroup H of a group G is called the Index of H in G, and is denoted by $[G:H]$."

Example:-

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

$1 \in G$, $1H = \{1 \cdot 1, 1 \cdot -1\} = \{1, -1\}$

$-1 \in G$, $-1H = \{-1 \cdot 1, -1 \cdot -1\} = \{-1, 1\}$

$i \in G$, $iH = \{(i)(1), (i)(-1)\} = \{i, -i\}$

$-i \in G$, $-iH = \{(-i)(1), (-i)(-1)\} = \{-i, i\}$

Number of distict left cosets of H in G is $= 2$

$$[G:H] = 2$$

Scanned with CamScanner

Example #01:-

Find the distict left or (right) Cosets of $E=\{0, \pm 2, \pm 4, \cdots\}=\{2n : n \in z\}$ in the group $(z, +)$.

$z = \{\cdots -3, -2, -1, 0, 1, 2, 3 \cdots\}$

$E = \{\cdots -4, -2, 0, 2, 4, \cdots\}$

$0 \in z$, $0+E = \{\cdots, 0+(-4), 0+(-2), 0+0, 0+2, 0+4 \cdots\}$

$= \{\cdots -4, -2, 0, 2, 4 \cdots\}$

$1 \in z$, $1+E = \{\cdots 1+(-4), 1+(-2), 1+0, 1+2, 1+4 \cdots\}$

$= \{\cdots -3, -1, 1, 3, 5 \cdots\}$

Number of distinct left cosets = 2

$[z : E] = 2$

★ Lagrange's Theorem:-

"Both the order and index of a subgroup of a finite group divide the order of the group"

Let G be a group and H be its subgroup such that $|G| = n, |H| = m$

let $a_i \in G$, $a_1H, a_2H, \cdots a_kH$ be distinct left cosets of H in G.

$[G : H] = k$

Define a function from $\phi : H \longrightarrow a_iH$

$a_i \in G$

Scanned with CamScanner

by $a(h) = a_i h$ $\quad h \in H$

since each element $a_i h \in a_i H$ for each $h \in H$, so the ϕ is onto.

Consider $\phi(h_1) = \phi(h_2)$ $\quad h_1, h_2 \in$

$a_i h_1 = a_i h_2$ $\quad \because a_i \in G$

$h_1 = h_2$

Hence ϕ is a one-one function so ϕ is bijective function.

Therefore the number of elements in H is equal to the number of elements in $a_i H$.

$|H| = m = |a_1 H| = |a_2 H| \cdots = |a_k H|$

Since the Cosets define the partition of G.

So $a_1 H \cap a_2 H = \phi$

$a_i H \cap a_j H = \phi$ for any $i \neq j$

and

$G = a_1 H \cup a_2 H \cup \cdots \cup a_k H$

$|G| = |a_1 H| + |a_2 H| + \cdots + |a_k H|$

$n = m + m + \cdots + m$.

$n = mk$

m divides n & k divides n

$\Rightarrow |H|$ divides $|G|$ & $[G : H]$ divides $|G|$.

Scanned with CamScanner

Hence the proof.

Theorem #01 :-

The order of an element of a finite group divides the order of the group.

Let G be a group and x belongs to group G.

$|G| = n$

$|x| = m$

We show that m divides n.

$x \in G$, ~~$H \subseteq G$~~ $H = \langle x \rangle \subseteq G$.

But $|x| = m$, so, $|H| = m$

By 'Lagrange's Theorem the order of a subgroup 'H' divides order of the group G.

$|H|$ divides $|G|$.

'm' divides 'n'

Hence the proof.

Scanned with CamScanner

Theorem #02:-

A group G whose order is a prime number is necessarily cyclic.

Let G be a group:-

$|G| = p$. p is prime number.

let $x \in G$ be a non-identity element.

$H = \langle x \rangle \subset G$

By lagrange's theorem, $|H|$ divides $|G|$. But $|G| = p$, so $|H|$ can divide $|G|$ only when $|H| = p$ or $|H| = 1$

Therefore $|H| = p$, but $|G| = p$

it means $H = G$

So G must be a cyclic group

Hence the proof.

Example:- Let G be a group of order 89. Can G have a Subgroup

i) of order 12

ii) of order 16

iii) of order 24

$|G| = 89$

i) let H be a subgroup of order 12.

Scanned with CamScanner

$|H| = 12$

Since 89 is a prime numbers, and 12 does not divide it, so by Lagrange's theorem,

It is not a subgroup of G.

Lecture # 11:-

* Permutation

"Let X be a non-empty set. A bijective mapping $\alpha : X \to X$ is called the permutation on X.

* Identity Permutation:-

Let X be non-empty set. A bijective mapping $\alpha : X \to X$ is called the identity permutation on X, if $\alpha(x) = x$, for all $x \in X$

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

$\alpha(1) = 1$

$\alpha(2) = 2$

$\alpha(3) = 3$

$$\begin{pmatrix} 1 & 2 & 3 \\ \alpha_1 & \alpha(2) & \alpha_3 \end{pmatrix}$$

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

$X = \{x_1, x_2 \cdots x_n\}$

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \alpha(x_1) & \alpha(x_2) & \cdots & x_n \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}$$

Scanned with CamScanner

Remarks:-

If 'X' has n elements, then total number of permutation on X is n!

1. $X = \{1\}$, $n = 1$, Total permutation $= 1! = 1$

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

2. $X = \{1, 2\}$, $n = 2$ Total permutation $= 2!$

$$2 \times 1 = 2$$

$$\alpha_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \alpha_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

(3) $X = \{1, 2, 3\}$, $n = 3$, Total permutations $= 3! = 3 \times 2 \times 1 = 6$

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Inverse Permutation:-

Let X be a non-empty set and $\alpha : X \to X$ be a permutation on X such that

$$\alpha(x) = y, \quad \forall\, x, y \in X$$

Then the inverse permutation $\alpha^{-1} : X \to X$ of α is defined as

$$\alpha^{-1}(y) = x, \quad \forall\, x, y \in X$$

Scanned with CamScanner

*222*4#

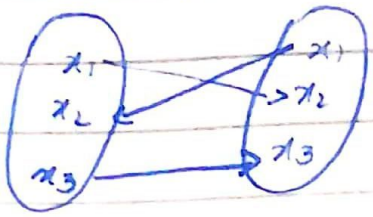
7421

19B

$\alpha(x_1) = x_2$

$\alpha(x_2) = x_1$

$\alpha(x_3) = x_3$



$\alpha(x_2) = x_1$

$\alpha^{-1}(\alpha(x_2)) = \alpha^{-1}(x)$

$x_2 = \alpha^{-1} x$

$\alpha(x_1) = x_2$

$x_1 = \alpha^{-1}(x_2)$

$\alpha^{-1}(x_3) = x_3$

Example :- 01

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Example :- 02

Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 5 & 4 & 1 \end{pmatrix}$ find

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 6 & 1 & 4 & 5 \end{pmatrix}$$

Example :- 03

Let $B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 6 & 2 & 4 \end{pmatrix}$

find $B^{-1} = ?$

Scanned with CamScanner

$$\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 3 & 4 \end{pmatrix}$$

Lecture #12:-
Examples of Permutations

Q#1:- Write the inverse permutation of

let $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Q#2:- Write the inverse permutation of

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Q#3:- Write the inverse permutation of

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

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Scanned with CamScanner

Q4:- Write the inverse permutation of

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

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

Q5:- Write the inverse permutation of

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 4 & 3 \end{pmatrix}$$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 5 & 4 & 1 \end{pmatrix}$$

Q6:- Write the inverse permutation of

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 3 & 4 \end{pmatrix}$$

$$\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 6 & 2 & 4 \end{pmatrix}$$

Is the Subtraction is binary operation on the set of Real numbers R.

Scanned with CamScanner

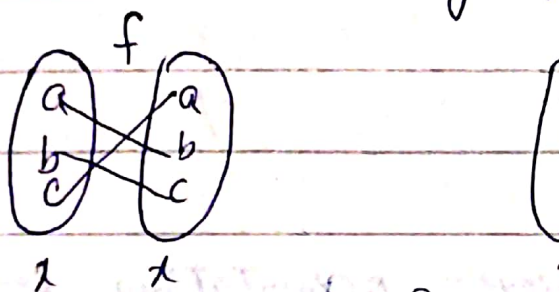
Lecture #13:-

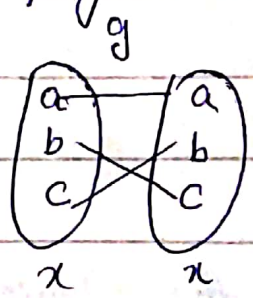
Product or Composition of Permutations:-

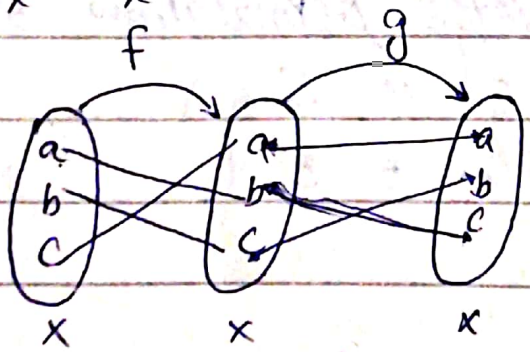
Let $f: X \to X$ and $g: X \to X$ be two Permutation on non-empty set X, then the permutation $fg: X \to X$ on X defined as:-

$$(x)fg = ((x)f)g \qquad \forall x \in X$$

is called the product or Composition of permutations f and g. It is also denoted by fog.







$$fOg(x) = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$ Ans

Scanned with CamScanner

Example #01:-

Find the product of the following permutation:-

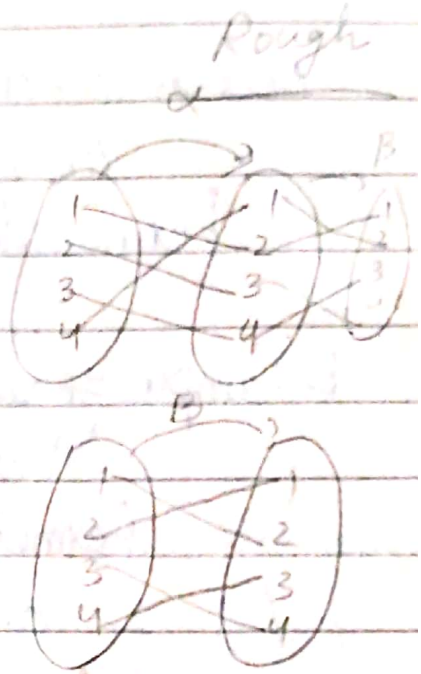
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

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

~~$\alpha \times \beta = \begin{pmatrix} 1 & 2 & \end{pmatrix}$~~

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$ Ans.



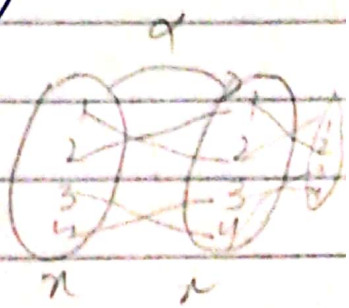
Example #02:-

Find the product or Composition $\alpha \cdot \alpha$ of the permutation:-

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

$$\alpha \cdot \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$ Ans.



Scanned with CamScanner

Example #03:-

Solve easily Same as Solve before.

Lecture # 141:-

Examples of Composition of Permutations:-

Example #01:-

Multiply the following Permutations

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}$$

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

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

Scanned with CamScanner

Example:-

Mutiply the following permutations.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 4 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 1 & 4 \end{pmatrix}$$

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

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

Example :-

Multipply the following permutations:-

$$\begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 9 & 2 & 3 \end{pmatrix} \begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 3 & 9 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 9 & 7 & 3 & 2 & 8 & 6 \end{pmatrix}$$ Ans.

Scanned with CamScanner

Example:

Let

$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

find fog, f^2og and f^3og.

(i) fog:

$f^2 = fof = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

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

$f^3 = ffof = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

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

(ii) $fog = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

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

(iii) $f^2og = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

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

Scanned with CamScanner

(iii) $f^3 \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ Ans.

Example:-

let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

Show that $f^4 = g^2$.

$f^2 = f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

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

$f^3 = f^2 \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

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

$L.H.S = f^4 = f^3 \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

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

$R.H.S = g^2 = g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

Hence proved $\Rightarrow$ L.H.S = R.H.S.

Scanned with CamScanner

Lecture # 15:-
Cyclic permutation

1 - Cyclic permutation:-

Let $X = \{x_1, x_2, x_3, \cdots x_n\}$ then a permutation α is called cyclic permutation or cycle of length n if

$$\alpha = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_2 & x_3 & x_4 & \cdots & x_1 \end{pmatrix}$$

$$\alpha = (x_1\ x_2\ x_3 \cdots x_n)$$

Example :-

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

$$= (1\ 2\ 3\ 4\ 5)$$

Example :-

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

$$= (1\ 2\ 3\ 4)$$

if element of X is

$$X = \{x_1, x_2, \cdots x_k, x_{k+1}, \cdots x_n\}$$

$k < n$.

$$\alpha = \begin{pmatrix} x_1 & x_2 & \cdots & x_k & x_{k+1} & \cdots & x_n \\ x_2 & x_3 & \cdots & x_1 & x_{k+2} & & x_n \end{pmatrix}$$

$= (x_1\ x_2 \cdots x_k)$ Cycle of length k.

Scanned with CamScanner

جو نمبر اپنے آپ پر map ہو رہے ہوں گے ignore کر رہے ہیں۔

Example:-

Find the length of cycle:-

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

$= (1\ 2\ 3\ 4\ 5\ 6)$ length = 6

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

$= (3\ 4\ 5) \Rightarrow$ length = 3

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

$= (1\ 2\ 5) \Rightarrow$ length = 3

Example:-

Find the following product and express it as a product of cyclic permutations on mutually disjoint sets.

$(14)(235)(35)(45)$

$= (14)(235)(35)(45)$

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

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

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

Scanned with CamScanner

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

disjoint cycle

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

$$= (1\ 5\ 2\ 4)$$ Ans

Example :- Find the following product and Express it as a product of cyclic permutation on mutually disjoint sets.

$(1\ 2\ 4)(1\ 3\ 6\ 5\ 4)$.

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

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

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

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

$= (1\ 2)(3\ 6\ 5\ 4)$ Ans.

Scanned with CamScanner

Example:-

Express the following permutation as a product of disjoint cycles.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 8 \\ 8 & 1 \end{pmatrix} \begin{pmatrix} 3 & 6 & 4 \\ 6 & 4 & 3 \end{pmatrix} \begin{pmatrix} 5 & 7 \\ 7 & 5 \end{pmatrix}$$

$$= (18)(364)(57)$$ Ans.

Example :-

Express the following permutation as a product of disjoint cycles.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix}$$

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

$$= (134)(26)(587)$$ Ans.

Scanned with CamScanner

Lecture #16 :- Examples of cyclic permutation

Example #01

The length of the cyclic permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$ is ----?

$= (1\,2\,3\,4\,5\,6\,7)$

length of cyclic permutation is 7.

Example #02:-

The length of the cyclic permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 5 & 6 \end{pmatrix}$ is ——.

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

$= (3\ 4)$

length of the cyclic permutation is 2.

Example #03:-

Express the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 2 & 1 & 3 \end{pmatrix}$ as a product of disjoint cycles.

$= \begin{pmatrix} 1 & 5 \\ 5 & 1 \end{pmatrix}\begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix}\begin{pmatrix} 3 & 6 \\ 6 & 3 \end{pmatrix} = (1\,5)(2\,4)(3\,6)$ Ans

Scanned with CamScanner

Example #04:-

Express the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix}$ as a product of disjoint cycles.

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

$$= (1\ 5\ 3)(2\ 4\ 6)$$ Answer.

Example #05:-

Express the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 2 & 1 & 4 & 3 & 8 \end{pmatrix}$ as a product of disjoint cycles.

$$= \begin{pmatrix} 1 & 5 \\ 5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 6 & 4 \\ 6 & 4 & 2 \end{pmatrix} \begin{pmatrix} 3 & 7 \\ 7 & 3 \end{pmatrix}$$

$$= (1\ 5)(2\ 6\ 4)(3\ 7)$$ Answer.

Scanned with CamScanner

Lecture # 17.

Symmetric Group.

"The group S_n of all permutations defined on a set X with n elements is called Symmetric group of degree n."

نوٹ:- "کسی بھی سمٹرک گروپ بنانے کیلئے S_4 کو کوئی بھی نمبر لیں گے let convert کریں گے permutation اسکو $S_4 = \{1, 2, 3, 4\}$ مثلاً permutation کرنا ہے۔ جتنے ایلمنٹس ہونگے اتنے factorial permutation میں جو factorial کا جواب آئے گا اتنے permutation بنائے گا۔ مثلاً $S_4 = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$"

Theorem # 01:-

The Set S_n of all permutations defined on a set X with n elements is a group under the operation of Composition of permutations.

Proof:-

i) **Closure property:-**

Let $f, g \in S_n$, then we have to Show $fog \in S_n$.

Scanned with CamScanner

نوٹ:- گروپ ثابت کرنے کے لیے جتنی کرنا ہے کہ گروپ کی جو properties ہوتی کرتا ہے کہ پتہ -

Since $f, g \in S_n$

So $f: X \to X$, $g: X \to X$ are bijective functions

therefore, the Composition of two bijective function is also bijective.

So $fog: x \to x$ is bijective.

$fog \in S_n$

So, the Colurse property holds.

2. Associative law:-

we have to show that (denote the Circle.)

$(fog) oh = fo(goh)$

L.H.S $= (x)[(fog)oh]$

$= ((x)(fog))h = ((x)f)g)h \to ①$

R.H.S $= (x)[fo(goh)] = ((x)f)(goh)$

$= (((x)f)g)h \to ②$

By ① and ②

$(fog)oh = fo(goh)$

3. Identity Permutation :- $I(x)$

$foI = Iof = f$

$(x)(foI) = ((x)f)I = f(x) = (x)f$ $\because I(x) = x$

$(x)(I of) = ((x)(I))f = (x)f$

$foI = Iof = f$

Identity permutation hold.

Scanned with CamScanner

(4) Inverse Permutation :-

Let $f \in S_n$, then $f: X \to X$ is a bijective mapping. then $f^{-1}: X \to X$ is also a bijective mapping.

$$f^{-1} \in S_n$$

$$f \circ f^{-1} = f^{-1} \circ f = I$$

$$(x)(f \circ f^{-1}) = ((x)f)f^{-1}$$
$$= (y)f^{-1}$$
$$= x$$
$$= I(x) \to I$$

$\because y = f(x)$

$f^{-1}(y) = x$

$I(x) = x$

$$(y)(f^{-1} \circ f) = ((y)f^{-1})f$$
$$= xf = y$$
$$= I(y) \to (II)$$

By I & II

$$f^{-1} \circ f = f \circ f^{-1} = I$$

Scanned with CamScanner

Theorem #02:-

Show that (S_3, o) is a non-abelian group.

We know that S_3 is a group of permutations on a set X with three elements.

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

All possible permutations on X are

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

~~$\alpha_1 \alpha_2 =$~~

We have to show that

$$\alpha_1 \alpha_2 \neq \alpha_2 \alpha_1$$

$$\alpha_1 \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\alpha_2 \alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Hence prove that (S_3, o) is a non-abelian group.

Scanned with CamScanner

Theorem #03:-

Find all the Subgroups of S_3.

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

All possible permutation on X are the following:-

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$S_3 = (I, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta)$

where $\alpha^3 = I = \beta^2 = (\alpha\beta)^2 = (\alpha^2\beta) = I$

Trivial Subgroups of S_3 : I, S_3

Non-Trivial Subgroups of S_3 : $\{I, \alpha, \alpha^2\} = h_1$

$\{\beta, I\} = h_2$

$H_3 = \{\alpha^2\beta, I\}$, $H_4 = \{\alpha\beta, I\}$

Scanned with CamScanner

Lecture # 18:-

Transposition

"A cycle of length '2' is called transposition."

e.g $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\ 2)$

Example 01:-

Theorem:-

Every cyclic permutation can be expressed as the product of transpositions.

Suppose we have cyclic permutation $(a_1, a_2, a_3 \cdots a_n)$ of length n.

we have to show that

$$(a_1\ a_2\ a_3 \cdots a_n) = (a_1 a_2)(a_1 a_3) \cdots (a_1 a_n) \rightarrow (1)$$

we prove it by using Mathematical Induction.

Step 1:- $n = 2$

L.H.S $= (a_1 a_2)$, R.H.S $= (a_1 a_2)$

So it is true for $n = 2$.

Scanned with CamScanner

$n = 3$

L.H.S $= (a_1\ a_2\ a_3)$

R.H.S $= (a_1\ a_2)(a_1\ a_3)$

$$= \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}$$

$$= (a_1\ a_2\ a_3)$$

L.H.S = R.H.S

Theorem #02:-

Every permutation of degree n can be expressed as the product of transpositions.

Since we have a result that every permutation of degree 'n' can be expressed as the product of disjoint cycles.

We also know that every cyclic permutation can be written as the product of transpositions.

Therefore, every permutation of degree n, can be expressed as the product of transposition.

Hence proved.

Scanned with CamScanner

Example #01

Express the following permutation as the product of transposition.

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

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

$$= (1\,2)(3\,4) \quad \text{Ans}$$

Example #02:-

Express the following permutation as the product of transposition.

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

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

$$= (1\,5)(2\,3)$$

Example #03:-

Express the following permutation as the product of tranposition.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 1 & 6 & 4 \end{pmatrix}$$

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

$$= (1\,3)(1\,2)(1\,5)(1\,6)(1\,4)$$

Scanned with CamScanner

Example #04:-

Express the following permutation as the product of transpositions.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 6 & 1 & 3 & 5 & 8 & 9 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 3 & 6 & 5 \\ 6 & 5 & 3 \end{pmatrix} \begin{pmatrix} 7 & 8 & 9 \\ 8 & 9 & 7 \end{pmatrix}$$

$$= (1\ 2\ 4)(3\ 6\ 5)(7\ 8\ 9)$$

$$= (1\ 2)(1\ 4)(3\ 6)(3\ 5)(7\ 8)(7\ 9)$$ Ans

Example #05:-

Express the following permutation as the product of transposition

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 6 & 2 & 9 & 8 & 3 & 1 & 4 & 5 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 10 & 7 \\ 10 & 7 & 1 \end{pmatrix} \begin{pmatrix} 2 & 6 & 3 \\ 6 & 3 & 2 \end{pmatrix} \begin{pmatrix} 4 & 9 & 5 & 8 \\ 9 & 5 & 8 & 4 \end{pmatrix}$$

$$= (1\ 10\ 7)(2\ 6\ 3)(4\ 9\ 5\ 8)$$

$$= (1\ 10)(1\ 7)(2\ 6)(2\ 3)(4\ 9)(4\ 5)(4$$

Scanned with CamScanner

Lecture # 19

Even and Odd Permutation

1. Even Permutation :-

"A Permutation α in S_n is called an even Permutation if it can be written as a product of even number of transpositions."

Example:-

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 6 & 1 & 3 & 5 & 8 & 9 & 7 \end{pmatrix}$$

$$= (1\ 2)(1\ 4)(3\ 6)(3\ 5)(7\ 8)(7\ 9)$$

2. Odd Permutation :-

"A Permutation α in S_n is called an odd permutation if it can be written as a product of odd number of transposition."

Example:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 6 & 2 & 9 & 8 & 3 & 1 & 4 & 5 & 7 \end{pmatrix}$$

$$= (1\ 10)(1\ 7)(2\ 6)(2\ 3)(4\ 9)(4\ 5)(4\ 8)$$

Scanned with CamScanner

Example #01:-

Is the permutation (1 2 3)(2 5 6)(4 3 5 1) odd or even?

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

$$= (1\,2)(1\,3)(2\,5)(2\,6)(4\,3)(4\,5)(4\,1)$$

Since, these are 7 transpositions so, the given permutation is an odd permutation.

Example #02:-

Is the Permutation (147)(345)(87)(8345) odd or even?

نوٹ:-

even اور odd کو Permutation ثابت کرنے کے لیے ہر ایک نمبر کو اس کے cycle کے ہر ایلیمنٹس کو الگ الگ کرنا ہے۔

$$= (1\,4)(1\,7)(3\,4)(3\,5)(8\,7)(8\,3)(8\,4)(8\,5)$$

Since these are 8 transposition so, the given permutation is even permutation.

Scanned with CamScanner

Theorem:-

The Product of two even or two odd permutations is an even even permutation..

Let α and β be two even permutations of length n. Suppose α and β can be expressed as m and p transpositions respectively, then $\alpha\beta$ will Contain $m+p-2k$ transpositio where 'k' is a positive Integer.

Since m, p and 2k are even Integers so $m+p-2k$ will also be even p. Integers.

Scanned with CamScanner

Lecture # 20

Examples of Even and odd Permutation.

MCQs

Example:

The Permutation $(1\,2)(1\,3)$ is an even permutation

- True ✓
- False

Example:-

The Permutation $(a\,b)(a\,c)(c\,d)$ is an even permutation

- True
- false ✓

Example:-

Show that the following Permutation is even.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 6 & 1 & 3 & 5 & 8 & 9 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 3 & 6 & 5 \\ 6 & 5 & 3 \end{pmatrix} \begin{pmatrix} 7 & 8 & 9 \\ 8 & 9 & 7 \end{pmatrix}$$

Scanned with CamScanner

$= (1\ 2\ 4)(3\ 6\ 5)(7\ 8\ 9)$

$= (1\ 2)(1\ 4)(3\ 6)(3\ 5)(7\ 8)(7\ 9)$

prove that it is an even permutation.

نوٹ:

★ اگر given سائیکلز کی تعداد Even ہو گی اور ہر سائیکل میں دو ایلیمنٹس ہونگے تو وہ permutation even ہو گی۔

★ اگر given سائیکلز کی تعداد odd ہو گی اور ہر سائیکل میں دو ایلیمنٹس ہونگے تو وہ odd permutation ہو گی۔

★ اگر give سائیکلز میں دو سے زیادہ ایلیمنٹس ہوں تو پہلے سب سائیکلز میں دو ایلیمنٹس بنائیں گے

Scanned with CamScanner

Lecture #21.

ORDER of Permutation.

Let α be a permutation. Then the least positive Integer m is called order of α if $\alpha^m = I$, where I is an Identity permutation.

Example $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$$\alpha^2 = \alpha \cdot \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

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

$$\alpha^3 = \alpha^2 \cdot \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \boxed{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}} \Rightarrow \text{Identity per....}$$

$\alpha^3 = I$

So the order of α is 3

Scanned with CamScanner

For Higher order permutation

Find کرنا ہو Higher کی Permutation کو
cyclic کی given permutation کو - کرنا ہو تو
کرنا ہو کی لکھتے ہیں -

اس کے بعد جتنی cyclic permutation بنتی ان کی
L.C.M کی length کے L.C.M سے لیتے ہیں اور جو
order آئے گا وہی اس کا order ہوگا - Answer

Remark:-

The order of a transposition is '2.'

Theorem:-

The order of a cyclic permutation of length n is n.

Proof:-

Let $\alpha = (a_1\ a_2\ a_3 \cdots a_n)$ be a cyclic permutation.

$\alpha: a_1 \to a_2,\ a_2 \to a_3 \cdots a_n\ a_1$

$\alpha = \alpha^2: a_1 \to a_3\ a_2 \to a_4 \cdots a_n\ a_2$

and upto so on ——.

$\alpha^n: a_1 \to a_1,\ a_2 \to a_2 \cdots a_{n-1}\ a_n$

$\alpha^n = I$, where I is Identity permutatio

Scanned with CamScanner

Example :-

Find the order of permutation.

Let

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

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

$$= \underset{\alpha_1}{(12)}\ \underset{\alpha_2}{(34)}$$

length of $\alpha_1 = 2$

length of $\alpha_2 = 2$

ORDER of permutation = LCM(2, 2)

= 2. Ans.