

NORMAL SUBGROUPS! -

→ A subgroup H of a group G is said to be normal subgroup of G if for every $x \in G$, and for every $h \in H$,

$$xh x^{-1} \in H$$

→ A subgroup H of G is called normal if all the left cosets are equal to right cosets.

→ every subgroup of Abelian grp is a normal subgroup.

→ if $aH = Ha \quad \forall a \in G$

Theorem A subgroup H of a group G is normal iff $aHa^{-1} = H \quad \forall a \in G$.

PROOF

Let $aHa^{-1} = H \quad \forall a \in G$.

$\Rightarrow aHa^{-1} \subseteq H \quad \forall a \in G$.

$\Rightarrow H$ is normal subgroup of G .

QUOTIENT GROUP / FACTOR GROUP! -

Let H be a normal subgroup of G . The set of all cosets of H in G is known as quotient or factor group

$$G/H = \{Ha : a \in G\}$$

Theorem

The product of two right (left) cosets in G is also right (left) coset in G .

solⁿ Proof

Let G is group and H is normal subgrp. of G .

then,

$G/H = \{Ha : a \in G\}$ be quotient group.

let

$$Ha, Hb \in G/H. \Rightarrow$$

$$(Ha)(Hb) = H(aH)b$$

$$= H(Ha)b$$

$$(\because Ha = aH)$$

$$\Rightarrow (Hb)(aH)$$

$$\Rightarrow H(ab) \quad \forall a \in G, b \in G.$$

\Rightarrow right coset of H in G generated by ab .

Theorem There is one to one correspondence b/w the elements of subgroup H and those of any coset of H in G .

solⁿ

we define mapping $f: H \rightarrow aH$ by
 $f(h) = ah. \quad \forall h \in H.$

let $h_1, h_2 \in H$ such that

$$f(h_1) = f(h_2)$$

$$ah_1 = ah_2$$

$$\Rightarrow h_1 = h_2. \quad (\text{left cancellation})$$

$\therefore f$ is one-one.

Every element of aH of form ah for some $h \in H. \therefore f$ is onto.

Theorem If G is finite group, H is normal subgroup of G then $O(G/H) = \frac{O(G)}{O(H)}$

Proof we have;
 $O(G/H) = \text{no. of distinct right cosets of } H \text{ in } G.$
 $= \frac{\text{no. of elements in } G}{\text{no. of elements in } H}$
 $= \frac{O(G)}{O(H)}.$

PERMUTATION GROUP: - (SYMMETRIC GROUP)

Let S be finite set consisting of n elements then the set of all one-one mapping of S onto itself is called permutation if -

$$(f: S \rightarrow S)$$

- ① f is one to one.
- ② f is onto.

No. of distinct elements in finite set S is called degree of permutation. It is denoted by:-

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

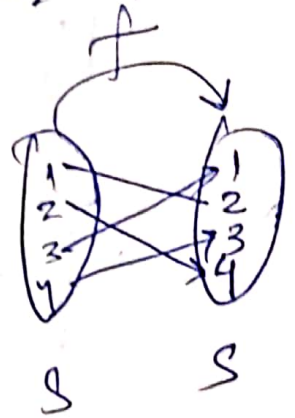
$$S = \{a_1, a_2, a_3, \dots, a_m\}$$

eg: $S = \{1, 2, 3, 4\}$ and mapping $f: S \rightarrow S$.

is given as.

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

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



EQUALITY OF PERMUTATIONS:-

If f and g are 2 permutations on set S ,
then $f = g$ iff

$$\boxed{f(x) = g(x)} \quad \forall x \in S.$$

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

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

$$\therefore (f = g)$$

$$\begin{aligned} f(1) &= 2 \\ f(2) &= 3 \\ f(3) &= 1 \\ f(4) &= 4 \end{aligned}$$

$$\begin{aligned} g(1) &= 2 \\ g(2) &= 3 \\ g(3) &= 1 \\ g(4) &= 4 \end{aligned}$$

Identity Permutation:-
 If each element of permutation is mapped by itself then it is called identity per. (I)

eg. $I = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$ is an identity permutation

$S = \{a, b, c, \dots\}$

$I(a) = a \quad \forall a \in S$

Total no of Permutations:-
 If there are n elements in set S then total no of permutations is $n!$

Inverse of Permutation:-

If f is a permutation on 'S'
 $S = \{a_1, a_2, \dots, a_n\}$ such that

$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$

then there exist a permutation called inverse denoted as f^{-1} such that:

$f \circ f^{-1} = I$

$\begin{cases} f(a_1) = y \\ f^{-1}(y) = a_1 \end{cases}$

$f^{-1} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$

Identity Permutation:-
 If each element of permutation is mapped by itself then it is called identity per. (I)

eg. $I = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$ is an identity permutation

$S = \{a, b, c, \dots\}$

$\boxed{I(a) = a} \forall a \in S.$

Total no of Permutations:-
 If there are n elements in set S then total no of permutations is $n!$

Inverse of Permutation:-

If f is a permutation on 'S'
 $S = \{a_1, a_2, \dots, a_n\}$ such that

$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$

then there exist a permutation called inverse denoted as f^{-1} such that:

$\boxed{f \circ f^{-1} = I}$

$\begin{pmatrix} f(a_i) = y. \\ f^{-1}(y) = a_i \end{pmatrix}$

$f^{-1} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$

PRODUCT OF PERMUTATIONS (COMPOSITIONS OF PERMUTATIONS) :-

The product of two permutations f and g of same degree is denoted by fg or gf meaning perform f and then g :-

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_m \\ b_1 & b_2 & b_3 & \dots & b_n \end{pmatrix} \text{ and } g = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

$$\text{then } fg = gf = \begin{pmatrix} a_1 & a_2 & \dots & a_m \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

- Now fg is also permutation on $S = \{a_1, a_2, \dots, a_n\}$

TOTAL NO. OF PERMUTATIONS

Q) # $A = \{1, 2, 3\}$ then $S_3 = \{P_0, P_1, P_2, P_3, P_4, P_5\}$

$S_n \rightarrow$ set of all permutations of degree n , then set S_n be the set consisting of all permutations of degree n , then the S_n will have $n!$ distinct permutations of degree n . This set S_n is called symmetric set of permutations of degree n .

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

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

PERMUTATION GROUP: -

Let A be a set of degree n . Let P_n be the set of all permutations of degree n on A . Then $(P, *)$ is a group called as Permutation Group and the opⁿ $*$ is the composition of permutations.

CLOSURE PROP: -

Let f and g be any two permutations in P_n . where,

$$f = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \quad g = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

then

$$fg = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

(Hence P_n is closed for the composition as product of two permutations)

Since a_1, a_2, \dots, a_n are also arrangements of n element of $\text{set } S$. $\therefore fg$ is a permutation of degree n . $fg \in P_n$
 $\forall f, g \in P_n$.

2) ASSOCIATIVITY :-

$$h = \begin{pmatrix} a_1 & a_2 & \dots & a_m \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$$

$$(fgh) = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix} = fg(h).$$

3) EXISTENCE OF IDENTITY :-

$$fI = If = f$$

$$I = \begin{pmatrix} c_1 & c_2 & \dots & c_m \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

4) EXISTENCE OF INVERSE :-

Let f be the permutation of degree 'n'.
then the permutation f^{-1} is also of degree 'n'.

$$ff^{-1} = f^{-1}f = I$$

$\therefore (P_n, *)$ is a group of order $n!$ with respect to composition of permutations.

CYCLIC PERMUTATION :-

Let 'f' be a permutation of degree 'n' on set S having 'n' distinct elements. Suppose it is possible to arrange 'n' elements in a row in such a way that the f-image of each element of set S in a row is the element following it, the f-image of

last element is the first element and the remaining $(n-m)$ elements of the set 'S' are left unchanged by 'f'. Then 'f' is called a cyclic permutation.

eg. $f = (1, 3, 4, 5) = \begin{pmatrix} 1 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 \end{pmatrix}$

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

→ A circular permutation may be denoted by more than one rowed symbols.

⇒ length of cycle means the no. of elements permuted by the cycle.

⇒ DISJOINT CYCLES are those which have no common elements. Every permutation of a finite set can be expressed as a cycle or as a product of disjoint cycles.

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

this is written as

$(1 \ 2), (3 \ 4 \ 6), (5) \}$ 3 cycles.
 ↓ length ↓ ↓
 2 3 1