

Lectured By Dr. H.K. Yadav.
 Deptt. of Mathematics, Mandoori College, Jabalpur
 B.Sc - part - I (H), paper - I, Date - 01-05-2020
 01-06-2020

Q.1. State and prove Cayley's Theorem:

Soln. Statement: $\rightarrow$ Every finite group G is isomorphic to its permutation group.

Proof: Let G be a finite group of order n such that
 $G = \{a_1, a_2, a_3, \dots, a_n\}$.

Let $a \in G$. Define a map $f_a: G \rightarrow G$ given by

$$f_a(x) = ax, \quad \forall x \in G \quad \text{--- (I)}$$

f_a is one-one.

$$\text{Let } f_a(x_1) = f_a(x_2), \quad \forall x_1, x_2 \in G$$

$$\Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$$

f_a is onto.

$f_a: G \rightarrow G$ is one-one and G is finite

$\Rightarrow f_a$ is onto. Thus, f_a is one-one map of a finite set G onto itself. It means that f_a is a permutation of degree n . Here

$$f_a = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ aa_1 & aa_2 & \dots & aa_n \end{pmatrix}$$

The elements $aa_1, aa_2, \dots, aa_n$ are all distinct elements of G .

We write, $G' = \{f_a : a \in G\}$, then G' is a set of permutations of degree n .

Now, we claim that $(G', *)$ is a group, where $*$ denotes permutations multiplication.

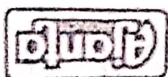
Let $a, b, c \in G$ be arbitrary and e be the identity in G .

Let a^{-1} denote inverse of a in G .

$$\text{So, that } a^{-1}a = aa^{-1} = e.$$

(I) Closure property: $f_a f_b \in G' \Rightarrow f_a f_b \in G'$

$$\text{Let us consider } (f_a f_b)(x) = f_a[f_b(x)] = f_a(bx)$$



$$= a(bx) = (ab)x \quad [\text{by associativity in } G]$$

$$= f_{ab}(x)$$

$$\Rightarrow f_a f_b = f_{ab} \quad \text{--- II}$$

$$a, b \in G \Rightarrow ab \in G \Rightarrow f_{ab} \in G' \Rightarrow f_a f_b \in G'$$

III Associativity: Let $a, b, c \in G$

$$\Rightarrow (ab)c = a(bc) \Rightarrow f_{(ab)}c = f_{a(bc)}$$

$$\Rightarrow f_{(ab)}f_c = f_a f_{bc} \Rightarrow (f_a f_b)f_c = f_a(f_b f_c)$$

IV Existence of identity:

$$a, e \in G \Rightarrow f_e \in G' \text{ and } ae = ea = a$$

$$\Rightarrow f_{ae} = f_{ea} = f_a \Rightarrow f_a f_e = f_e f_a = f_a$$

$\Rightarrow f_e \in G'$ is identity element of G' .

V Existence of inverse: $a \in G \Rightarrow a \cdot a^{-1} \in G \Rightarrow f_a f_{a^{-1}} \in G'$

$$\text{Also, } aa^{-1} = a^{-1}a = e$$

$$f_{aa^{-1}} = f_{a^{-1}a} = f_e \text{ or, } f_a f_{a^{-1}} = f_{a^{-1}} f_a = f_e$$

$\Rightarrow f_{a^{-1}} \in G'$ is the inverse of $f_a \in G'$.

VI Order of G' :

$$\text{For } o(G) = n, G' = \{f_a : a \in G\} \Rightarrow o(G') = n$$

Therefore, we have $(G', *)$ is a finite group of order n .

Now, we claim that $(G, *) \cong (G', *)$

Now, we define a map $f: G \rightarrow G'$ such that $f(x) = f_x, \forall x \in G$.

i) f is one-one:

$$\text{For } f(x_1) = f(x_2), \forall x_1, x_2 \in G$$

$$\Rightarrow f_{x_1} = f_{x_2} \Rightarrow f_{x_1}(x) = f_{x_2}(x), \forall x \in G$$

$$\Rightarrow x_1 x = x_2 x \Rightarrow x_1 = x_2 \quad [\text{by I}]$$

ii) f is onto:

$$\text{For any } f_a \in G' \Rightarrow a \in G \text{ such that } f(a) = f_a$$

iii) f preserves composition in G and G' :

$$\text{For } f(x_1 x_2) = f_{x_1 x_2} \quad [\text{where } x, x_2 \in G \Rightarrow x_1 x_2 \in G]$$

$$= f_{x_1} f_{x_2} = f(x_1) \cdot f(x_2)$$

Hence, f is an isomorphism of G onto G' and hence

$$G \cong G'$$

Proved.