Lectured By Dr. H.K. Yadav.
Deptt. of Mathematics, Marwari College, DBG.
B.Sc. part - II(H), paper - I. Date 25-05-2020.

Q.1. State and prove Cayley's theorem.

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

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

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

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

f_a is one-one.

Let $f_a(x_1) = f_a(x_2)$, $x_1, x_2 \in G$

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

f_a is onto.

$f_a : G \to G$ 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,

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

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

Write $G' = \{f_a : a \in G\}$, then G' is a set of ~~permutat~~ 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.

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

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

Let us consider $(f_a f_b)(x) = f_a[f_b(x)] = f_a(bx)$

$= a(bx) = (ab)x$, by associativity in G.

$= f_{ab}(x)$

$\Rightarrow f_a f_b = f_{ab}$ —— (ii)

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

(II) Associativity : Let $a, b, c \in G$

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

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

III Existence of identity: $a, e \in G \Rightarrow f_e \in G'$ 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'.

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

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

$f_{aa^{-1}} = f_{(a^{-1}a)} = f_e$ or $f_a f_{a^{-1}} = f_{a^{-1}} f_a = f_e$

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

(V) Order of G':

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, define a map $\phi : G \to G'$ such that $\phi(x) = f_x, \forall x \in G$

(I) ϕ is one-one:

For $\phi(x_1) = \phi(x_2)$: $x_1, x_2 \in G$

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

$\Rightarrow x_1 x = x_2 x$ [by I]

$\Rightarrow x_1 = x_2$.

(II) ϕ is onto:

For any $f_a \in G' \Rightarrow a \in G$ such that $\phi(a) = f_a$

(III) ϕ preserves composition in G and G'

For $\phi(x_1 x_2) = f_{x_1 x_2}$ [where $x_1, x_2 \in G \Rightarrow x_1 x_2 \in G$]

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

Hence, ϕ is an isomorphism of G onto G' and

$G \cong G'$

Proved.