B.Sc Part II (Honors)

Paper III Cayley's Theorem.

Theorem:- State and prove Cayley's theorem on finite groups.

Proof:- Let $G = \{a_1, a_2, a_3 \text{ ---- } a_r \text{ ---- } a_n\}$ be of order n with '0' as binary operations

let $a \in G$, for every $x \in G$ then $ax \in G$ by closure law

suppose a function $f_a : G \to G$ defined by

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

Now, $f_a(a_r) = aa_r$ and $f_a(a_s) = aa_s$

$f_a(a_r) = f_a(a_s)$

$\Rightarrow aa_r = aa_s$

$\Rightarrow a_r = a_s$ (By left Cancellation law)

$\therefore f_a$ is one-one.

The mapping f_a is also onto because if x is any element of G then $\exists\ a^{-1}x$ in G such that

$$f_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = ex = x$$

$\therefore f_a$ is onto.

Since f_a is one-one and onto so it is permutation on G.

Now we shall show that S is a group isomorphic to G, for this we first prove that S is a group w.r.t. Composite Composition.

(i) closure law: Let $f_a, f_b \in S$, $a, b \in G$

then $(f_a \circ f_b) = f_a\{f_b(x)\} = f_a(bx)$ — by (i)

$= a \cdot (bx)$ — by (i)

$= (ab)x = f_{ab}(x)$ ---- by (i)

$\therefore f_a \circ f_b = f_{ab}$

Also $a, b \in G \Rightarrow ab \in G$

$\Rightarrow f_{ab} \in S$

$\Rightarrow f_{ab} \in S \quad (\because a \circ b = ab)$

$\Rightarrow f_a \circ f_b \in S \quad$ By (2)

$\therefore S$ is closed.

(ii) Associative:

We have $f_a(f_b f_c) = f_a(f_{bc}) \quad$ — By (2)

$= f_{abc} \quad$ — By (2)

Again $(f_a f_b) f_c = (f_{ab}) f_c \quad$ — By (2)

$= f_{abc} \quad$ — By (2)

$\therefore f_a(f_b(f_c)) = (f_a f_b) f_c$

$\therefore S$ obey associative law.

(iii) Existence of identity :— Let e be the identity of G.

We have $(f_e f_a)(x) = f_e\{f_a(x)\} = f_e(ax)$ by (1)

$= e(ax) \quad$ — by (1)

$(f_e f_a)(x) = (ea)x = ex = f_a(x)$ — By (1) $\forall$ $x \in G$.

$\therefore f_e$ is the identity of S.

(iv) Existence of inverse :—

We have by (2), $f_a f_{a^{-1}} = f_{aa^{-1}} = f_e$

$(\because aa^{-1} \in G)$

Also $f_{a^{-1}} f_a = f_{a^{-1}a} \quad [\text{By (1)}] = f_e$

$\therefore f_{a^{-1}}$ is the inverse of f_a

$\therefore S$ is a group.

Now we shall show that G is isomorphic to S i.e. $G = S$

Let $\phi : G \to S$ defined by $\phi(a) = f_a \; \forall \; a \in a$

(i) ϕ is one-one : Let $a, b \in G$ then

$\phi(a) = \phi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x)$ $\forall x \in G$.

$\Rightarrow ax = bx \; \forall \; x \in G \Rightarrow a = b \quad \therefore \phi$ is one-one.

(iii) ϕ is onto: let $f_a \in S$. Then $a \in G$ and we have $\phi(a) = f_a$

$\therefore \phi$ is onto.

(iv) ϕ preserves operation in G and S

Let $a, b \in G$. Then

$\phi(ab) = f_{ab}$ (By definition of ϕ)

$\therefore f_a f_b$ (by (i))

$= \phi(a)\,\phi(b)$ (by definition of ϕ)

$\therefore \phi$ preserves operation in G and S

$\therefore G = S$ i.e. G is isomorphic to S.

Theorem:- Prove that every isomorphic image of a cyclic group is again cyclic.

Proof:- Let $G = \{a\}$ be cyclic group generated by a.

Let G' be an isomorphic image of G under the isomorphism f i.e. $f: G \to G'$

Let $f(a^n) \in G'$ be the image of $a^n \in G$.

We have

$f(a^n) = f(aaa \text{ ---- to } n \text{ factors})$

$= f(a)\,f(a)\,f(a)$ ---- to n factors

[$\because f$ is a isomorphism]

$= [f(a)]^n$

i.e. every element of G' can be expressed as an integral power of $f(a)$.

Thus G' is cyclic and $f(a)$ is a generater of G'.

Hence proved.

Harjani Kumar Singh