UNIT-4

MATHS SEM 3

LONGS

Statement :- Every finite group G is Isomorphic to its permutation group.

Proof :-

Operm < w.d, 1-1, onto

① group < C, A, I, I

③ Iso < w.d, Homo, 1-1, onto

Let $(G, \cdot)$ be finite group.

Let $a \in G$ for any $x \in G$ show that $ax \in G$ [∵ By closure law]

Define: $f : G \to G$ such that $f_a(x) = ax \; \forall a \in G$.

To prove that f_a is well-defined :

For $a, b \in G$

$x = y$

Multiply with 'a' on both sides

$ax = ay$

$f_a(x) = f_a(y)$

∴ 'f_a' is well-defined.

To prove f_a is one-one :

For $a, b \in G$

$f_a(x) = f_a(y)$

$ax = ay$

By using left cancellation law.

$x = y$

$\therefore$ f_a is one-one.

To prove f_a is onto :-

Let $x \in G$

$a \in G \Rightarrow a^{-1} \in G$ [$\because$ Inverse law]

$\exists a^{-1}x \in G$ such that $f_a(a^{-1}x) = a(a^{-1}x)$

$= (aa^{-1}x)$.

$= ex$

$= x$.

$\therefore$ f_a is onto.

$\therefore$ f_a is permutation.

Now we have to show that $G' = \{f_a \forall a \in G\}$ is a group.

* Closure law :

For $a, b \in G$.

$f_a, f_b \in G'$

$[f_a \cdot f_b](x) = f_a[f_b(x)]$

$= f_a(bx)$

$= a(bx)$

$= (ab)x$.

$(f_a \cdot f_b)(x) = f_{ab}x$

$f_a \cdot f_b = f_{ab}$

For $a, b \in G \Rightarrow ab \in G$ [$\because$ By using closure law]

$f_{ab} \in G'$

$f_a \cdot f_b \in G'$.

$\therefore$ G' satisfies closure law in G'.

* Associative law :-

$f_a, f_b, f_c \in G'$

$(f_a \cdot f_b) f_c = f_a \cdot (f_b \cdot f_c) \in G'$.

$L.H.S = (f_a \cdot f_b) f_c (x)$.

$= (f_a \cdot f_b)(cx)$

$= f_{ab}(cx)$

$= (ab)(cx)$

$= a(bc)x$

$= f_a (bc) x$

$= f_a (f_b f_c) x$

$= R.H.S$.

$\therefore$ " . " Satisfies Associative law in G'.

* Existence of Identity law :

Let $f_a \in G'$.

$\exists f_e \in G'$ Such that $f_a \cdot f_e = f_e \cdot f_a = f_a$

$L.H.S = f_a f_e$

$= f_{ae}$ [$\because$ f is ~~Holds~~]

$= f_a$

$= R.H.S$

Similarly we can prove that $f_e \cdot f_a = f_a$.

$\therefore$ 'f_e' is the multiplicative Identity of $\{f_a\}$ in G'.

is satisfies existence of Identity law in G'.

* Existence of Inverse law :-

For $f_a \in G'$

for $a \in G \Rightarrow a^{-1} \in G$

$\exists$ $f_{a^{-1}} \in G'$ such that $f_a \cdot f_{a^{-1}} = f_{a^{-1}} \cdot f_a = f_e$.

$L.H.S = f_a \cdot f_{a^{-1}}$

$= f_{aa^{-1}}$

$= f_e$

$= R.H.S$

Simillally we can prove that $f_{a^{-1}} \cdot f_a = f_e$

$\therefore f_{a^{-1}}$ is the multiplicative Inverse of f_a in G'

$\therefore$ '.' is satisfies Existence of Inverse in G'.

$\therefore (G', \cdot)$ is a permutation group.

Now we have to prove that $G \cong G'$.

Define : $\phi : G \rightarrow G'$ such that $\phi(a) = f_a \; \forall a \in G$

To prove ϕ is well-defined :

Let $a, b \in G$

$a = b$

Multiply with 'x' on both sides

$ax = bx$.

$f_a(x) = f_b(x)$

$f_a = f_b$

$\phi(a) = \phi(b)$

$\therefore \phi$ is well-defined.

To prove ϕ is one-one :

$\phi(a) = \phi(b)$

$f_a = f_b$

$f_a(x) = f_b(x)$

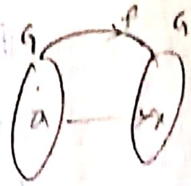
$ax = bx$

By using right cancellation law,

$a = b$

$\therefore \phi$ is one one.

To prove ϕ is onto :-



Let $x \in G'$

$\exists a \in G$ such that $f(a) = x$.

$\therefore \phi$ is onto.

To prove ϕ is structure Preserving :-

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

$\phi(ab) = f_{ab}$

$= f_a \cdot f_b$ [$\because f$ is Homo]

$= \phi(a) \cdot \phi(b)$

$\therefore \phi$ is structure preserving.

$\therefore \phi$ is Isomorphic.

Every finite group is Isomorphic to its Permutation group.

Theorem : 2

Prove that a group of prime order is Cyclic (or) If p is a prime number then Every group of order 'p' is cyclic.

Proof :

Let $p \geq 2$ be a prime number

Let $(G, \cdot)$ be a group of prime order

$$O(G) \geq p$$

Since, the number of elements is atleast 2, One of the element is other than 'e', let the element be 'a'.

Let $\langle a \rangle$ be a cyclic subgroup generated by a.

$\therefore a \in \langle a \rangle ; \langle a \rangle \neq \{e\}$

Let 'h' be the order of $\langle a \rangle$,

By Lagrange's theorem, $\frac{o(\langle a \rangle)}{O(G)} = \frac{h}{p}$.

But 'p' is a prime number

$h = 1$ (or) $h = p$.

Since $\langle a \rangle \neq \{e\} \Rightarrow h \neq 1$

$h = p$.

$\therefore o[\langle a \rangle] = O(G)$

$\therefore (G, \cdot)$ is also a cyclic group.

3 Prove that every Subgroup of cyclic group is cyclic.

Proof :-

Let $(G, \cdot)$ be a group

Let $(H, \cdot)$ be a Subgroup of G.

Scanned with CamScanner

Since H is a subgroup of G, Every element of H is an element of G.

Let 'd' be the least positive integer in H Such that $a^n \in H \ \forall n \in \mathbb{Z}$

Now we have to p.T $H = \langle a^d \rangle$

Let $a^m \in H \ \forall m \in \mathbb{Z}$

By using Division Algorithm we have to find the values of d and q.

Such that $m = dq + r \ \forall 0 \leq r \leq d$.

$$a^m = a^{dq+r}$$

$$= a^{dq} \cdot a^r$$

$$a^m = (a^d)^q \cdot a^r \quad \text{——} \ ①.$$

$$a^d \in H \Rightarrow (a^d)^q \in H \ \forall q \in \mathbb{Z}$$

$$a^{dq} \in H$$

$$a^{-dq} \in H$$

$$a^m \in H, a^{-dq} \in H.$$

$$a^m \cdot a^{-dq} \in H \quad [\because \text{Closure law}]$$

$$a^{m-dq} \in H$$

$$a^r \in H.$$

This is contradiction to our assumption

i.e., d is the least positive Integer

$$r = 0$$

$$\text{From } ① \Rightarrow a^m = (a^d)^q \cdot a^0$$

$$= (a^d)^q \in H$$

$$H = \langle a^d \rangle$$

$\therefore$ Every Subgroup of cyclic group is cyclic.

Scanned with CamScanner