439 State and prove Cayley's theorem on finite groups.

or

Prove that Every finite group is isomorphic to a permutation group

Statement → Every finite group is isomorphic to a permutation group.

Proof → Let G be a finite group.
If $a \in G$ then for every x in G the product $ax \in G$.
Now Let f_a be a function from G into G such that $f_a(x) = ax \quad \forall x \in G$ ..... (1)
The function f_a is one-one because
if $x, y \in G$ then
$f_a(x) = f_a(y)$
$\Rightarrow ax = ay$
$\Rightarrow x = y$ [By Left Cancellation law]
The function f_a is also onto because
if $x \in G$ then there exists an element $a^{-1}x$ in G such that
$f_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = ex = x$
So f_a is a one-one function from G on to G.
Thus f_a is a permutation on G

440 Let G be set of all such one-one onto functions defined on G with respect to every element of G be G' such that $G' = \{f_a : a \in G\}$ ... (2)

Now we shall prove that G' is a group isomorphic to G.

At first we will show that G' is a group with respect to the operation known as Composite or product of two functions.

Closure Property → Let $f_a, f_b \in G'$, where $a, b \in G$

then $(f_a \circ f_b)(x) = f_a\{f_b(x)\}$ [from equn (1)]

$= f_a(bx)$ [$f_a(x) = ax$]

$= a(bx)$ [from equn (1)]

$= (ab)x$

$= f_{ab}(x)$ [from equn (1)]

$\therefore f_a \circ f_b = f_{ab}$ ... (3)

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

$\Rightarrow f_{a \circ b} \in G'$ [from equn (2)]

$\Rightarrow f_{ab} \in G'$

$\Rightarrow f_a \circ f_b \in G'$ [from equn (3)]

Hence G is closed with respect to the product of functions.

441

Associative axiom

Let $f_a, f_b, f_c \in G'$ where $a, b, c \in G$

then $f_a(f_b f_c) = f_a(f_{bc})$ [from equⁿ ③]

$= f_{abc}$ [from equⁿ ③]

Again, $(f_a f_b) f_c = (f_{ab}) f_c$ [from equⁿ ③]

$= f_{abc}$ [from equⁿ ③]

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

So the associative axiom is satisfied and G' is associative.

Identity axiom

Let e be the identity element of G

then f_e is the identity of G'

Now, $(f_e f_a)(x) = f_e\{f_a(x)\}$

$= f_e^{(ax)}$ [By equⁿ ①]

$= e(ax)$ [By equⁿ ①]

$= (ea)x$

$= ax$ [By equⁿ ①]

$= f_a(x)$

$\therefore f_e f_a = f_a$

Similarly $f_a f_e = f_a$

$\therefore f_e f_a = f_a f_e = f_a$

Hence f_e is the identity element of G'.

Inverse axiom →

$f_a f_a^{-1} = f_{aa^{-1}}$ [By equⁿ ③]

$= f_e$, as $aa^{-1} = e$ in grp G.

Again $f_{a^{-1}} f_a = f_{a^{-1}a}$ [By equⁿ ③]

$= f_e$, as $a^{-1}a = e$ in grp G.

Hence f_a^{-1} is the inverse of f_a.

Hence G' is a grp.

Now we will prove that G is isomorphic to G'.

Let the function ϕ frm G into G' defined by

$\phi_a = f_a$ ..... ④ $\forall a \in G$

Now to prove ϕ is one-one.

Let $a, b \in G$ then

$\phi(a) = \phi(b) \Rightarrow f_a = f_b$ [frm equⁿ ④]

$\Rightarrow f_a(x) = f_b(x)$

$\Rightarrow ax = bx$ [frm equⁿ ②]

$\Rightarrow a = b$

Hence the mapping ϕ is one-one.

To prove ϕ is onto.

G is a finite set so ϕ is onto.

Also $\phi(ab) = f_{ab}$ [frm equⁿ ④]

$= f_a f_b$ [frm equⁿ ③]

$= \phi(a)\phi(b)$ [frm equⁿ ④]

$\therefore \phi$ is an isomorphism.

Hence $G \cong G'$

Thus Every finite grp G is isomorphic to a permutation grp.

443

(*) If $f: G \to G'$ be a homomorphism then prove that their identities correspond and their inverse also correspond

(or)

Let $f: G \to G'$ be a homomorphism of groups

(i) If e and e' be the identities in G and G' respectively then

$$f(e) = e'$$

(ii) If $f(a) = a'$ then $f(a^{-1}) = (a')^{-1}$

i.e. $f(a^{-1}) = [f(a)]^{-1}$ $\forall a \in G$.

Proof → (i) Let $a \in G$ then by the identity axiom of Group G' we have

$$f(a)e' = f(a) \quad [e' \text{ is identity of } G']$$
$$= f(ae) \quad [\because e \text{ is identity of } G]$$
$$= f(a)f(e) \quad [\text{Because } f \text{ is a homomorphism}]$$

Now G' is a group.

So, $f(a)e' = f(a)f(e)$

$\Rightarrow e' = f(e)$ ....(1) [By the left cancellation law in G']

Since G' is a group, so there exists an unique identity element in G'.

So $f(e)$ is the identity element of G'.

444 (ii) Since $f(a) = a'$ ... (2)

Now $a a^{-1} = e$ (e is the identity element in G)

$\therefore f(a a^{-1}) = f(e)$ [we have proved $f(e) = e'$ (by equn (1))]

$= e'$

$\Rightarrow f(a) f(a^{-1}) = e'$

$\Rightarrow a' f(a^{-1}) = e'$ [from equn (2)]

which shows that $f(a^{-1})$ is inverse of a'.

i.e. $f(a^{-1}) = (a')^{-1} = [f(a)]^{-1}$ Proved

(iv) If $f : G \to G'$ be a homomorphism prove that if the order of a is finite, then the order of $f(a)$ is a divisor of the order of a.

Proof: Let $a \in G$ and $o(a) = m$

we have $o(a) = m \Rightarrow a^m = e$

$\therefore f(a^m) = f(e)$

$\Rightarrow f(a.a.a \ldots \text{m times}) = e'$

$\Rightarrow f(a).f(a).f(a) \ldots \text{m times} = e'$

$\Rightarrow [f(a)]^m = e'$

So if n is the order of $f(a)$ in G' then n must be a divisor of m

i.e. $o\{f(a)\}$ is a divisor of $o(a)$.

Define Kernel of a homomorphism.

445

If f be a homomorphism of the group G into the group H, then prove that

(i) Kernel f is a subgroup of G

(ii) the image f is a subgroup of H.

Definition ⇒ **kernel of a homomorphism**

Let f be a homomorphism of a group G into a group H. Then the set K is called the Kernel of K.

$$K = \{x \in G : f(x) = e'\} \text{ where } e' \in H$$

Proof ⇒ (2) Let e and e' be the identity elements of groups G and H respectively

Let $a, b \in \ker f$

By the definition of kernel

$$f(a) = e' \quad \ldots (1)$$

$$f(b) = e' \quad \ldots (2)$$

$\because$ $\ker f$ is a subset of G

So, $a, b \in \ker f$

$\Rightarrow a, b \in G$

Since G is a group, so $b^{-1} \in G$ (inverse axiom)

Now $a \in G$, $b^{-1} \in G$, so $ab^{-1} \in G$ (closure axiom)

$\because$ Homomorphism f maps the inverse of any element b of G onto the inverse of $f(b)$.

$$\therefore f(b^{-1}) = [f(b)]^{-1} = (e')^{-1} \quad [\text{from eqn (2)}]$$

By the definition of homomorphism

$$f(ab^{-1}) = f(a) f(b^{-1}) = f(a)[f(b)]^{-1}$$

$$= e'[e']^{-1} = e'$$

446

$\therefore f(ab^{-1}) = e'$

$\therefore ab^{-1} \in \ker f$, $\forall a, b \in \ker f$

Hence we conclude that $\ker f$ is a subgroup of G.

(ii) Let $a', b' \in$ image f

then $\exists$ (there exists) $a, b \in G$

such that $f(a) = a'$

and $f(b) = b'$

$\therefore G$ is a group

$\therefore ab^{-1} \in G$

Since H is a group and image $f \subseteq H$

and $a', b' \in H$

So $b'^{-1} \in H$ and $a' b'^{-1} \in H$

Again $b^{-1} = [f(b)]^{-1} = f(b^{-1})$

Now $a' b'^{-1} = f(a) f(b^{-1})$

$= f(ab^{-1}) \in$ image f

for every $a', b' \in$ image f.

Hence image f is a subgroup of H.