Dr. O. P. Raman
Dept of Mathematics

For T.D.C. Part II
Paper - 3
Abstract (Modern) Algebra



**Q. Define homomorphism of groups with examples.**

*Definition* Let $(G, o)$ and $(G', o')$ be two groups. A mapping $f: G \to G'$ satisfying $f(a \circ b) = f(a) o' f(b) \forall \quad a, b \in G$ is called a homomorphism of the group $G$ with the group $G'$, where $f(a)$ and $f(b)$ are the images of $a$ and $b$ under $f$.

[Note If $f$ is an onto mapping then $G'$ is said to be a homomorphic image of $G$, that is, $G' = f(G)$.]

*Examples*

1. We know that $(Z_0, \cdot)$ and $(Q, \cdot)$ are two arbitrary multiplicative groups of nonzero integers and rational numbers respectively. Then the mapping $f: Z_0 \to Q$ defined by $f(x) = \frac{1}{x}, \forall \quad x \in Z_0$ is a homomorphism of $Z_0$ into $Q$.
2. We know that $(Z, +)$ is a group where $Z$ is the set of integers and $+$ is the usual addition in $Z$ and $(Z', \cdot)$ is another group where $Z' = \{1, -1\}$ and $\cdot$ is the usual multiplication in $Z'$. Then the mapping $f: Z \to Z'$, defined by $f(x) = 1$ and $-1$ accordingly when $x$ is even and odd, is a homomorphism of $Z$ onto $Z'$.

## *Important Theorems on Homomorphism of Groups.*

*59. ***Theorem 1:*** *If $f$ be a homomorphism from the group $G$ into the group $G'$ and if $e$ and $e'$ be the identities in $G$ and $G'$ respectively then prove that $f$ maps $e$ of $G$ onto $e'$ of $G'$. That is $f(e) = e'$.*

*Proof* Let $a \in G$. Then, by the identity axiom of group $G'$, we have

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

But, from the identity axiom of group G, we have

$$ae = a.$$

Using this result in (1), we get

$$f(a)\, e' = f(ae) \qquad \ldots(2)$$

But, from the definition of homomorphism of groups, we have

$$f(ae) = f(a)\, f(e).$$

Using this result in (2), we get

$$f(a)\, e' = f(a)\, f(e) \qquad \ldots(3)$$

Since $G'$ is a group, therefore the cancellation laws hold in $G'$. Hence, using left cancellation law in (3), we get

$$e' = f(e) \ ; \text{i.e. } f(e) = e'.$$

Further since $G'$ is a group, therefore there exists an unique identity element in $G'$. Hence $f(e)$ is the identity element of $G'$.

*60. *Theorem 2: If $f$ is a homomorphism from the group $G$ into the group $G'$ then prove that $f$ maps the inverse of any element $a$ of $G$ onto the inverse of $f(a)$. That is $f(a^{-1}) = [f(a)]^{-1}$, where $a \in G$.*

*Proof* Let $a \in G$ and $a^{-1}$ be the inverse of $a$ in $G$.

Then, by the inverse axiom of the group $G$, we have

$$a\, a^{-1} = e \text{ and } a^{-1}\, a = e, \text{ where } e \text{ is the identity element of } G$$

$$\Rightarrow f(aa^{-1}) = f(e) \text{ and } f(a^{-1}a) = f(e) \qquad \ldots(1)$$

But from the definition of homomorphism of groups, we have

$$f(aa^{-1}) = f(a)\, f(a^{-1}) \text{ and } f(a^{-1}a) = f(a^{-1})\, f(a).$$

Also we know that $f(e) = e'$, where $e'$ is the identity element of $G'$.

Putting these results in (1), we get

$$f(a)\, f(a^{-1}) = e' \text{ and } f(a^{-1})\, f(a) = e'.$$

Hence $f(a^{-1})$ is an inverse of $f(a)$. Since $G'$ is a group, therefore inverse must be unique.

Hence we conclude that

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

***Define isomorphism of groups with examples.***

*Definition* Let $(G, o)$ and $(G', o')$ be two groups. A one-one onto mapping $f : G \to G'$ satisfying

But, from the identity axiom of group G, we have

$$ae = a.$$

Using this result in (1), we get

$$f(a)\, e' = f(ae) \qquad \ldots(2)$$

But, from the definition of homomorphism of groups, we have

$$f(ae) = f(a)\, f(e).$$

Using this result in (2), we get

$$f(a)\, e' = f(a)\, f(e) \qquad \ldots(3)$$

Since $G'$ is a group, therefore the cancellation laws hold in $G'$. Hence, using left cancellation law in (3), we get

$$e' = f(e) \ ; \text{i.e. } f(e) = e'.$$

Further since $G'$ is a group, therefore there exists an unique identity element in $G'$. Hence $f(e)$ is the identity element of $G'$.

*60. *Theorem 2: If $f$ is a homomorphism from the group $G$ into the group $G'$ then prove that $f$ maps the inverse of any element $a$ of $G$ onto the inverse of $f(a)$. That is $f(a^{-1}) = [f(a)]^{-1}$, where $a \in G$.*

*Proof* Let $a \in G$ and $a^{-1}$ be the inverse of $a$ in $G$.

Then, by the inverse axiom of the group $G$, we have

$$a\, a^{-1} = e \text{ and } a^{-1}\, a = e, \text{ where } e \text{ is the identity element of } G$$

$$\Rightarrow f(aa^{-1}) = f(e) \text{ and } f(a^{-1}a) = f(e) \qquad \ldots(1)$$

But from the definition of homomorphism of groups, we have

$$f(aa^{-1}) = f(a)\, f(a^{-1}) \text{ and } f(a^{-1}a) = f(a^{-1})\, f(a).$$

Also we know that $f(e) = e'$, where $e'$ is the identity element of $G'$.

Putting these results in (1), we get

$$f(a)\, f(a^{-1}) = e' \text{ and } f(a^{-1})\, f(a) = e'.$$

Hence $f(a^{-1})$ is an inverse of $f(a)$. Since $G'$ is a group, therefore inverse must be unique.

Hence we conclude that

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

***Define isomorphism of groups with examples.***

*Definition* Let $(G, o)$ and $(G', o')$ be two groups. A one-one onto mapping $f : G \to G'$ satisfying

$$f(a \circ b) = f(a) \circ' f(b), \forall \quad a, b \in G$$

is called an isomorphism of $G$ to $G'$ where $f(a)$ and $f(b)$ are the images of $a$ and $b$ under $f$.

The group $G$ is said to be isomorphic to $G'$. Symbolically we write

$$(G, \circ) \cong (G', \circ')$$

or

$$G \cong G'.$$

*Examples*

1. Let $G$ be the set of all integers and $G' = \{..., 2^{-3}, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, 2^3, .... \}$ and we know that $(G, +)$ and $(G', \cdot)$ are two groups where + and $\cdot$ stand for the usual addition and multiplication in $G$ and $G'$ respectively.

Then the mapping $f : G \to G'$, defined by $f(x) = 2^x \forall \quad x \in G$, is an isomorphism.

**Q.** **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., $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$**

**In other words, if $f : G \to G'$ be a homomorphism, then their identities correspond and their inverses correspond.**

**(iii) If the order of $a \in G$ is finite, then the order of $f(a)$ is a divisor of the order of $a$.**

**Proof :** (i) Let $f(e) = e'$ where $e$ is the identity of $G$ and $e' \in G'$.

If $f$ is a homomorphism, we have to prove that $e'$ is the identity of $G'$.

Take $x \in G$ and let $f(x) = x' (x' \in G')$

Now $x = ex$.

$\therefore$ $f(x) = f(ex) = f(e) \cdot f(x)$; since $f$ is a homomorphism

$\Rightarrow$ $x' = e'x'$

which means that $e'$ (i.e., $f(e)$) is the identity in $G'$.

(ii) Given $f(a) = a'$.

Now $aa^{-1} = e$ (the identity in $G$)

$\therefore$ $f(aa^{-1}) = f(e) = e'$; from (i)

That is, $f(a) \cdot f(a^{-1}) = e'$ since $f$ is a homomorphsim

i.e., $a' f(a^{-1}) = e'$ which means that the inverse of $a'$ is $f(a^{-1})$.

That is, $f(a^{-1}) = (a')^{-1} = [f(a)]^{-1}$.

(iii) Let $a \in G$ and $o(a) = m$.

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

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

$\Rightarrow$ $f(aaa \ldots \text{to } m \text{ factors}) = e'$

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

Hence 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 $o(a)$.

(5)

**Theorem**

8. State & prove Cayley's theorem

**Every finite group is isomorphic to a permutation group.**

**Proof :** Let $G$ be a finite group of order $n$.

We must find a group say $\overline{G}$ of permutations which should be isomorphic to $G$. Since $G$ is all we have to work with, we will have to use it to construct $\overline{G}$.

Let $G = \{a_1, a_2, a_3, \ldots, a_n\}$ be of order $n$.

Let $a$ be any one of the elements of $G$.

Since $G$ is a group, therefore $G$ is closed. This implies that for every $x \in G$, the product $ax$ is also an element of $G$.

Consider the function $f_a : G \to G$ defined by $f_a(x) = ax$ for all $x \in G$.

For example, $f_{ai}, (x) = a_i x$ for all $x \in G$. Thus under the mapping $f_{ai}$, $a_1 \to a_i a_1$, $a_2 \to a_i \cdot a_2, \ldots, a_n \to a_i a_n$; $i = 1, 2, 3, \ldots, n$.

The function $f_a$ is *one-one.*

Let $x, y \in G$, then $f_a(x) = f_a(y) \Rightarrow ax = ay$

$\Rightarrow x = y$; by left cancellation law.

Hence $f_a$ is one-one.

The function $f_a$ is also *onto,* because if $x$ is any element of $G$ (codomain) then there exists an element $a^{-1}x$ in $G$ (domain) such that $f_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = ex = x$.

Thus $f_a$ is a one-one function from $G$ onto $G$.

Therefore $f_a$ is a *permutation* on $G$.

Let $G'$ denote the set of all such one-one onto functions defined on $G$ corresponding to every element of $G$ i.e., $G' = \{f_a : a \in G\}$.

First we shall 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 $a, b \in G$.

We need to show that $f_a f_b \in G'$.

From our definition of product of two functions, we have

$$(f_a f_b)(x) = f_a[f_b(x)] = f_a(bx) = a(bx) = (ab)x$$

$$= f_{ab}(x) \text{ for all } x \in G.$$

Hence from the definition of equality of two functions, we have $f_a f_b = f_{ab}$

Since $ab \in G$, $\therefore f_{ab} \in G'$ and hence $f_a f_b \in G'$.

Thus $G'$ is closed with respect to the product of functions.

**Associativity :** 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 (1), we have $f_b f_c = f_{bc}$

$= f_{a(bc)}$; again from (1)

$= f_{(ab)c}$; $\because G$ is associative

$= f_{ab} f_c$; from (1)

$= (f_a f_b) f_c$.

Therefore $G'$ is associative with respect to the given operation.

**Existence of identity :** If $e$ is the identity of $G$, then $f_e$ is the identity of $G'$, because for every $f_a$ in $G'$, we have $f_e f_a = f_{ea} = f_a$ and $f_a f_e = f_{ae} = f_a$.

**Existence of Inverse :** If $a^{-1}$ is the inverse of $a$ in $G$, then $f_{a^{-1}}$ is the inverse of $f_a$ because $f_{a^{-1}} f_a = f_{a^{-1}a} = f_e$ and $f_a f_{a^{-1}} = f_{aa^{-1}} = f_e$.

Thus $G'$ is a group.

Now, we shall show that $G$ is isomorphic to $G'$ i.e, $G \cong G'$.

Consider the function $\phi$ from $G$ into $G'$ defined by $\phi(a) = f_a$ for all $a \in G$.

**$\phi$ is one-one :** Let $a, b \in G$.

Then $\phi(a) = \phi(b) \Rightarrow f_a = f_b$

$\Rightarrow f_a(x) = f_b(x)$ for all $x \in G$

$\Rightarrow ax = bx$ for all $x \in G$

$\Rightarrow a = b$

$\therefore \phi$ is one-one.

**$\phi$ is onto :** Let $f_a$ be any element of $G'$.

Then $a \in G$ and we have $\phi(a) = f_a$.

$\therefore$ $\phi$ is onto.

**$\phi$ preserves operations in $G$ and $G'$ :** Let $a, b \in G$.

Then $\phi(ab) = f_{ab}$; by definition of $\phi$

$= f_a f_b$; from (1)

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

$\therefore \phi$ preserves operations in $G$ and $G'$.

Hence $G$ is isomorphic to $G'$ i.e., $G \cong G'$.