5.3 HOMOMORPHISM AND ISOMORPHISM

5.3.1 Homomorphism

Definition of homomorphism. Let $(G,\circ)$ and $(G',*)$ be two groups. Then a mapping $f:G\to G'$ is said to be a homomorphism if

$$f(a\circ b)=f(a)*f(b)\ \forall a,b\in G.$$

Epimorphism & Monomorphism

A homomorphism is said to be **epimorphism** if it is onto mapping and is said to be **monomorphism** if it is one - one.

Endomorphism

A homomorphism of a group into itself is called an endomorphism.

Illustration

(i) Let $G=(Z,+)$, $G'=(3Z,+)$,

Consider a mapping $f:G\to G'$ defined by $f(x)=3x,\ x\in G$

Then $f(x_1)=3x_1,\ f(x_2)=3x_2,\ \forall x_1,x_2\in G.$

$\therefore$ Now $x_1,x_2\in G\Rightarrow x_1+x_2\in G\Rightarrow f(x_1+x_2)=3(x_1+x_2)$

Hence $f(x_1+x_2)=f(x_1)+f(x_2).$

So f is a homomorphism.

(ii) Let $(G,\circ)$ be a group and $f:G\to G$ be a mapping defined by $f(a)=e$, the identity element, $\forall a\in G$. Then $f(a)=e,\ f(b)=e\ \forall\ a,b\in G$. Now $a,b\in G\Rightarrow a\circ b\in G\Rightarrow f(a\circ b)=e$

$$\Rightarrow f(a\circ b)=e\circ e=f(a)\circ f(b).$$

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

Thus f is a homomorphism of G into G. Hence f is an endomorphism.

Theorem 1. Let $f:G\to G'$ be a homomorphism. Then

(i) $f(e)=e'$ where e and e' are identities of G and G' respectively.

Scanned by CamScanner

(ii) $f(a^{-1}) = [f(a)]^{-1}\ \forall a \in G$. [W.B.U.Tech 2006]

(iii) $o(f(a))$ is a divisor of $o(a)$ when $o(a)$ is finite $\forall\ a \in G$.

(iv) the homomorphic image $f(G)$ of G is a subgroup of G.

Proof : (i) Let $a \in G$. Then $f(a) \in G$

$\therefore f(a) * e' = f(a)$, as e' is the identity of G'

$= f(a \circ e)$, as e is the identity of G

$= f(a) * f(e)$ ($\because f$ is a homomorphism)

$\therefore f(a) * e' = f(a) * f(e)$, in G'

$\Rightarrow e' = f(e)$, by left cancellation law in group.

$\therefore f(e) = e'$

(ii) Let $a \in G$. Then $a^{-1} \in G$.

Now $e' = f(e) = f(a \circ a^{-1}) = f(a) * f(a^{-1})$

Also $e' = f(e) = f(a^{-1} \circ a) = f(a^{-1}) * f(a)$.

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

Hence $f(a^{-1})$ is the inverse of $f(a)$ in G'. Thus $f(a^{-1}) = [f(a)]^{-1}$

(iii) Let $a \in G$ and $o(a) = m$, a finite number

$\therefore a^m = e . \Rightarrow f(a^m) = f(e) \Rightarrow f(a \circ a \circ a ....m\ times) = e'$

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

Therefore, if n is the order of $f(a)$ in G', then n must be a divisor of m, by an earlier theorem. Hence $o(f(a))$ is a divisor of $o(a)$.

Kernel of a Homomorphism

Let $(G, \circ)$ and $(G', *)$ be two groups and $f : G \to G'$ be a homomorphism. Then the kernel of f is a subset of those element of G which are mapped to the identity element e' in G' and is denoted by Ker f. Thus Ker $f = \{x \in G : f(x) = e'\}$.

Theorem 2 : Let $f : G \to G'$ be a homomorphism. Then **Ker f** is a normal subgroup of G.

Proof : Let e, e' be the identities of G and G' respectively. Then $f(e) = e'$. So Ker f is a non-empty subset of G.

Let $a, b \in$ Ker$f$. Then $f(a) = e'$, $f(b) = e'$.

Now $f(a \circ b^{-1}) = f(a) * f(b^{-1}) = f(a) * \{f(b)\}^{-1} = e' * e'^{-1} = e'$

$\therefore a \circ b^{-1} \in$ Ker f

Therefore Ker f is a subgroup of G.

Next let $g \in G, h \in$ Ker f. Then $f(h) = e'$.

Now $f(g \circ h \circ g^{-1}) = f(g) * f(h) * f(g^{-1})$

$= f(g) * e' * \{f(g)\}^{-1} = f(g) * \{f(g)\}^{-1} = e'$

$\therefore g \circ h \circ g^{-1} \in$ Ker f

Therefore Ker f is a normal subgroup of G.

Theorem 3 : Let $f : G \to G'$ be a homomorphism. Then f is one-to-one if and only if Ker $f = \{e\}$.

Proof : Let f be one-to-one.

Also let $a \in$ Ker f be arbitrary. Then $f(a) = e'$, the identity element of G'.

$\therefore f(a) = f(e)$ [$\because f(e) = e'$] or, $a = e$ [$\because f$ is one-to-one]

Thus $a \in$ Ker $f \Rightarrow a = e$

$\therefore$ Ker $f = \{e\}$

Conversely, let Ker $f = \{e\}$.

Let $a, b \in G$. Then $f(a) = f(b)$

$\Rightarrow f(a) * \{f(b)\}^{-1} = f(b) * \{f(b)\}^{-1}$

$\Rightarrow f(a) * f(b^{-1}) = e'$ [$\because f$ is a homomorphism]

$\Rightarrow f(a \circ b^{-1}) = e' \Rightarrow a \circ b^{-1} \in$ Ker $f \Rightarrow a \circ b^{-1} = e \Rightarrow a = b$

$\therefore f$ is one-to-one.

5.3.2 Isomorphism.

Definition of Isomorphism

Let $(G,\circ)$, $(G',*)$ be two groups and $f: G \to G'$ be a homomorphism. Then f is said to be an isomorphism if f is one-to-one and onto (i.e if f is a monomorphism as well as an epimorphism.)

Isomorphic Groups.

Two groups $(G,\circ)$ and $(G',*)$ are said to be isomorphic if there exists an isomorphism f, $f: G \to G'$. Two isomorphic groups are writen as $G \approx G'$.

Automorphism: An isomorphism of a group G onto itself is called an *automorphism.*

Illustration. Let $G = (Z,+)$, $G' = (2Z,+)$ be two groups. Consider a mapping $f: G \to G'$ defined by $f(a) = -2a$, $a \in G$. Then $f(a) = -2a$, $f(b) = -2b$ $\forall a, b \in G$.

Now $a, b \in G \Rightarrow a + b \in G$.

$\therefore f(a+b) = -2(a+b) = -2a - 2b = f(a) + f(b)$

$\therefore f$ is a homomorphism.

Again $f(a) = f(b) \Rightarrow -2a = -2b \Rightarrow a = b$.

$\therefore f$ is one-one.

Let $b \in 2Z$. Then $-\frac{b}{2} \in Z$ and $f\left(-\frac{b}{2}\right) = (-2) \cdot \left(\frac{-b}{2}\right) = b$. So each element in Z has a pre-image under f.

$\therefore f$ is onto.

Combining all these we find that f is an isomorphism.

Theorem : Fundamental Theorem of Homomorphism.

Every homomorphic image of a group G is isomorphic to some quotient group of G.

Proof : Let G' be the homomorphic image of a group G and f be the corresponding homomorphism. We know that this G' is also group. Let $K = Ker\, f$. Then K is a normal subgroup of G.

We now consider the quotient group G/K and define a mapping $\phi: G/K \to G'$ such that $\phi(Ka) = f(a)$ $\forall a \in G$.

(i) First we shall show that the mapping ϕ is well defined i.e if $a, b \in G$ and $Ka = Kb$, then $\phi(Ka) = \phi(Kb)$.

Now $Ka = Kb \Rightarrow ab^{-1} \in K \Rightarrow f(ab^{-1}) = e'$, the identity of G'

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

$\Rightarrow f(a) = f(b) \Rightarrow \phi(Ka) = \phi(Kb)$

$\therefore \phi$ is well defined.

(ii) Now $\phi\{(Ka)(Kb)\} = \phi(Kab) = f(ab) = f(a)f(b)$

$= \phi(Ka)\,\phi(Kb)$

$\therefore \phi$ is a homomorphism.

(iii) Again $\phi(Ka) = \phi(Kb) \Rightarrow f(a) = f(b)$

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

$\Rightarrow f(a)f(b^{-1}) = e' \Rightarrow f(ab^{-1}) = e'$ [$\because f$ is homomorphism]

$\Rightarrow ab^{-1} \in K \Rightarrow Ka = Kb$ $\therefore \phi$ is one - to - one.

(iv) Lastly let $y \in G'$. Then $y = f(a)$ for some $a \in G$. Again $f(a) = \phi(Ka)$. This shows that for each $f(a) \in G'$, there exist $Ka \in G/K$ such that $\phi(Ka) = f(a)$. Hence ϕ is onto G'.

Thus ϕ is an isomorphism of G/K onto G'. Hence $G/K \approx G'$.

Illustrative Examples.

Ex.1. *Let $G = (C',\cdot)$, $G' = (R^+,\cdot)$ where $C' = C - \{0\}$, the set of all non-zero complex numbers. Show that the mapping $\phi: G \to G'$ defined by $\phi(z) = |z|$, $z \in C'$ is a homomorphism. Determine Ker ϕ and Im ϕ.*

Let $z_1, z_2 \in C'$. Then $\phi(z_1) = |z_1|$, $\phi(z_2) = |z_2|$.

Now $\phi(z_1 z_2) = |z_1 z_2| = |z_1||z_2| = \phi(z_1)\,\phi(z_2)$

$\therefore \phi$ is a homomorphism of G into G'

The identity of R^+ is 1.

Let $z \in C'$ such that $\phi(z)=1 \Rightarrow |z|=1$.

$\therefore$ Ker $\phi=\{z \in C' : |z|=1\}$ Obviously $Im\ \phi = R^+$.

Ex.2. *Let $G=S_3$ and $\phi : G \to G$ is defined by $\phi(x)=x^2, x\in S_3$. Examine whether the mapping ϕ is a homomorphism.*

Here $G=\{f_1, f_2, f_3, f_4, f_5, f_6\}$ where $f_1=I$, $f_2=(1, 2)$, $f_3=(2, 3)$, $f_4=(3, 1)$, $f_5=(123)$, $f_6=(132)$.

Let $f_2, f_3 \in G$. Then $f_2 f_3 = f_6 \in G$

$\therefore \phi(f_2)=f_2^2=f_2 f_2=f_1$ and $\phi(f_3)=f_3^2=f_3 f_3=f_1$

$\therefore \phi(f_2)\phi(f_3)=f_1 f_1=f_1$ but $\phi(f_2 f_3)=\phi(f_6)=f_6^2=f_6 f_6=f_5$

Hence $\phi(f_2 f_3)\neq\phi(f_2)\phi(f_3)$. $\therefore \phi$ is not a homomorphism.

Ex. 3. *Let $(Z,+)$ be the additive group of all integers and $(Q-\{0\},*)$ be the multiplicative group of non-zero rational numbers. Define $f : Z \to Q-\{0\}$ by $f(x)=3^x$ for all $n \in Z$. Show that f is a homomorphism but not an isomorphism.*

[W.B.U.Tech 2004]

Let $x_1, x_2 \in Z$. Then $f(x_1)=3^{x_1}$, $f(x_2)=3^{x_2}$

Now $f(x_1+x_2)=3^{x_1+x_2}=3^{x_1} * 3^{x_2}$

$\therefore f$ is a homomorphism.

Again, $f(x_1)=f(x_2) \Rightarrow 3^{x_1}=3^{x_2} \Rightarrow x_1=x_2$

$\therefore f$ is one-to-one.

Let $y_1 \in Q-\{0\}$.

Then $f(x_1)=y_1$ gives $3^{x_1}=y_1$ i.e. $x_1=\log_3 y_1$ which is not necessarily integer.

$\therefore x_1=\log_3 y_1 \notin Z$.

Thus each element of $Q-\{0\}$ has no pre-image under f.

$\therefore f$ is not onto.

Consequently f is not an isomorphism.

Ex. 4. *Show that every homomorphic image of an abelian group is abelian and converse is not true.*

Let G' be the homomorphic image of an abelian group G and f be the corresponding homomorphism.

Let $a_1, b_1 \in G'$. Then $f(a)=a_1, f(b)=b_1$ for some $a, b \in G$

Now $a_1 b_1 = f(a)f(b)=f(ab)$ [$\because f$ is a homomorphism]

$= f(ba)$ [$\because G$ is abelian]

$= f(b)f(a) = b_1 a_1$

$\therefore a_1 b_1 = b_1 a_1 \quad \forall a_1, b_1 \in G'$ $\therefore G'$ is abelian.

We know the symmetric group S_3 is a non-abelian group and the alternating group A_3 is a normal subgroup of S_3. Then the quotient group S_3/A_3 is a homomorphic image of S_3 (by Th-3) which is non-abelian. But S_3/A_3 is of the order 2 and hence is abelian.

Ex. 5. *Show that every homomorphic image of a cyclic group is cyclic and converse is not true.*

Let G' be the homomorphic image of a cyclic group G and f be the corresponding homomorphism.

Let $G=\langle a\rangle$. Also let $b_1 \in G'$. Then $f(b)=b_1$ for some $b\in G$.

Since $b\in G$; $b=a^n$ for some integer n.

$\therefore b_1=f(b)=f(a^n)=\{f(a)\}^n$ [$\because f$ is a homomorphism]

$\Rightarrow G'=\langle f(a)\rangle$

Hence G' is a cyclic group, generated by $f(a)$.

We know the symmetric group S_3 is not a cyclic and A_3 is a normal subgroup of S_3. Then the quotient group S_3/A_3 is a homomorphic image of S_3 which is not cyclic. But S_3/A_3 is of order 2 and it is cyclic which can be easily shown.

Ex. 6. *Let G be a group and the mapping $f : G \to G$ be defined by $f(x)=x^{-1}, x\in G$. Show that f is an automorphism if and only if G is abelian.*

Let G be abelian. and $x, y \in G$.

Then $f(x) = f(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow \left(x^{-1}\right)^{-1} = \left(y^{-1}\right)^{-1} \Rightarrow x = y$.

$\therefore f$ is one-one.

Next let $x \in G$, the co-domain of f. Then $\exists\, x^{-1} \in G$, the domain of f such that $f\left(x^{-1}\right) = \left(x^{-1}\right)^{-1} = x$

$\therefore f$ is onto.

Lastly $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = f(y)f(x)$

Thus f is a homomorphism.

Hence f is an automorphism of G.

Conversely let f be an automorphism of G and $x, y \in G$.

Then $f(xy) = f(x)f(y) \Rightarrow (xy)^{-1} = x^{-1}y^{-1}$

$\Rightarrow \left((xy)^{-1}\right)^{-1} = \left(x^{-1}y^{-1}\right)^{-1} \Rightarrow xy = \left(y^{-1}\right)^{-1}\left(x^{-1}\right)^{-1} \Rightarrow xy = yx$,

$\therefore xy = yx \;\forall\; x, y \in G$,

$\therefore G$ is abelian.

EXERCISE

I. Short Answer Questions

1. Define the kernel of group homomorphism
2. Show that every homomorphic image of an abelian group under multiplication is also abelian.
3. Show that the function $\phi : G \to G$ defined by $\phi(a) = a^{-1}\, \forall a \in G$ is a homomorphism if G is commutative.
4. Determine the Kernel of the homomorphism $f : G \to G'$ where $G = (R, +)$, $G' = (R^+, \cdot)$ defined by $f(a) = 2^a\; \forall a \in R$.
5. Define Isomorphism of groups with example.
6. For any three groups G_1, G_2 and G_3 prove that $G_1 \times G_2$ is isomorphic to $G_2 \times G_1$.
7. Find the kernel of $f : (C - \{0\}, \cdot) \to (R - \{0\}, \cdot)$ defined by $f(z) = |z|$.

8. If $M = \left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \text{ are integers}\right\}$ show that $f : M \to Z$ defined by $f\begin{pmatrix} a & b \\ b & a \end{pmatrix} = a - b$ is a homomorphism
9. If $*$ is defined as $(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$ and if $f : (N \times N, *) \to (Z, +)$ is defined by $f(a, b) = a - b$, show that f is a homomorphism. Is it isomorphism?
10. $f : (C - \{0\}, \cdot) \to (C - \{0\}, \cdot)$ defined by $f(z) = z^4$.

    (i) Show that f is a homomorphism. (ii) find the kernel of f.

    [W.B.U. Tech 2008]
11. $C^* = \{z : z \text{ is a complex number and } |z| = 1\}$. Prove that $f : (R, +) \to (C^*, \cdot)$ defined by $f(x) = e^{ix}$ is a homomorphism. Find the kernel of f.

Answers

4. Ker$f = \{0\}$ 7. pts on the circumference of a unit circle

9. No 10. $\{1, -1, i, -i\}$ 11. $\{2n\pi : n \in z\}$

II. Long Answer Questions

1. Verify whether the following mapping is a homomorphism. If so, determine Ker f.

   (i) Let $G = (Z, +)$, $G' = (Z, +)$ and $f : G \to G'$ defined by $f(x) = 4x$.

   (ii) Let $G = GL(2, R)$, $G' = (R, +)$ and $f = G \to G'$ defined by $f\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right\} = a + b + c + d$.

   (iii) Let $G = (R, +)$, $G' = (\{z \in C; |z| = 1\}, \cdot)$ and $f : G \to G'$ defined by $f(x) = e^{2i\pi x}$.

   (iv) Let $G = (Z, +)$, $G' = (Z, +)$ and $f : G \to G'$ defined by $f(x) = |x|$.

   [W.B.U Tech 2005]

Scanned by CamScanner