Homomorphism:

Let $\langle G, \cdot \rangle$ and $\langle G', * \rangle$ be two groups. A mapping $f : G \to G'$ is said to be a homomorphism if

$$f(g_1 \cdot g_2) = f(g_1) * f(g_2) \quad \forall\, g_1, g_2 \in G.$$

That is the mapping f is said to be a homomorphism, if f maps the composition of any two elements of G into the composition of the images of the elements. By this we say that f preserves composition.

If f is a homomorphism from the group G into G', we say G is homomorphic to the group G'.

Isomorphism

A homomorphism f from a group G into G' is said to be isomorphism if f is a bijection. i.e., f is both one-one and onto.

Two groups G and G' are said to be isomorphic, if there exists an isomorphism $f : G \to G'$. This we denote it by $G \approx G'$.

Endomorphism

A homomorphism f from a group G into itself is called Endomorphism.

Automorphism

An isomorphism f from a group G onto itself is called Automorphism.

Note: The identity map $I_g : G \to G$ from the group G onto itself, defined by $I_g(g) = g$ is a homomorphism. This shows that there exists atleast one homomorphism from G into itself. Further $I_g(g) = g$ is an automorphism.

Examples

1. Let $\langle G, \cdot \rangle$ and $\langle G', * \rangle$ be two groups and e' be the identity element of G'. Define $f: G \to G'$ by $f(g) = e' \ \forall\ g \in G$. Show that f is a homomorphism.

sol^n Consider, $f(g_1 \cdot g_2) = e'$, $g_1 \cdot g_2 \in G$.

Also, $f(g_1) * f(g_2) = e' * e' = e'$

$\therefore\ f(g_1 \cdot g_2) = f(g_1) * f(g_2)$.

Hence f is a homomorphism.

This homomorphism is called a trivial homomorphism.

2. Consider the additive group $\langle Z, + \rangle$ of all integers and the group $H = \{1, -1\}$ under multiplication. Define $\varphi: Z \to H$ by $\varphi(n) = \begin{cases} 1 & \text{if } n \text{ is even or zero} \\ -1 & \text{if } n \text{ is odd} \end{cases}$

Show that φ is a homomorphism.

sol^n let $m, n \in Z$

Case (i) Let m and n are both even.

Then $m+n$ is even $\Rightarrow \varphi(m+n) = 1$.

Also $\varphi(m) = 1$ and $\varphi(n) = 1$.

$\therefore\ \varphi(m+n) = \varphi(m) \cdot \varphi(n)$.

Case (ii) Let one of m and n be even, say m be even and n be odd. Then $m+n$ is odd $\Rightarrow \varphi(m+n) = -1$,

Also $\varphi(m) = 1$ and $\varphi(n) = -1$

$\therefore\ \varphi(m+n) = \varphi(m) \cdot \varphi(n)$.

Case (iii) Let m and n are both odd.

Then $m+n$ is even $\Rightarrow \varphi(m+n) = 1$.

Also $\varphi(m) = -1$ and $\varphi(n) = -1$

$\therefore\ \varphi(m+n) = \varphi(m) \cdot \varphi(n)$.

Hence φ is an homomorphism.

3. Let $M_n(\mathbb{R})$ be the group of all non-singular $n\times n$ matrices with real entries under matrix multiplication. Let $\mathbb{R}^*$ be the multiplicative group of non-zero real numbers. If $\varphi : M_n(\mathbb{R}) \to \mathbb{R}^*$ is defined by $\varphi(A) = |A|, \forall A \in M_n(\mathbb{R})$, show that φ is a homomorphism.

Sol.ⁿ Consider $\varphi(AB) = |AB|, \; \forall A, B \in M_n(\mathbb{R})$

$$= |A|\cdot|B|$$

$$\varphi(AB) = \varphi(A)\cdot\varphi(B).$$

Hence φ is a homomorphism.

4. Consider the multiplicative group $\langle \mathbb{R}^*, \cdot \rangle$ of all non-zero real numbers. Define $f : \mathbb{R}^* \to \mathbb{R}^*$ by $f(x) = 2^x \; \forall x \in \mathbb{R}^*$. Verify if f is a homomorphism.

Sol.ⁿ Consider $f(xy) = 2^{xy}$

and $f(x) = 2^x$, $f(y) = 2^y$ $\therefore$ $f(x)\cdot f(y) = 2^x \cdot 2^y = 2^{x+y}$

$\therefore$ $f(xy) \neq f(x)\cdot f(y)$

Hence f is not a homomorphism.

5. Define $f : \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}, + \rangle$ by $f(x) =$ greatest integer $\leq x$. Is f a homomorphism?

Sol.ⁿ By definition of f, $f(1) = 1$, $f(\frac{1}{2}) = 0$, $f(\frac{3}{2}) = 1$, ---- so on

Consider $f(\frac{3}{2}) = 1$ and $f(\frac{5}{2}) = 2$

$$f\left(\tfrac{3}{2} + \tfrac{5}{2}\right) = f(4) = 4$$

Also $f(\frac{3}{2}) + f(\frac{5}{2}) = 1 + 2 = 3$

$$\therefore f\left(\tfrac{3}{2} + \tfrac{5}{2}\right) \neq f\left(\tfrac{3}{2}\right) + f\left(\tfrac{5}{2}\right)$$

$\therefore$ f is not a homomorphism.

Elementary properties of Homomorphism

1. Let $f: G \to G'$ be a homomorphism from the group $\langle G, \cdot \rangle$ into the group $\langle G', * \rangle$. Then

   (i) $f(e) = e'$ where e and e' are the identity elements of the group G and G' respectively.

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

2. If f is a homomorphism of a group G into G', then the range $f(G) = \{f(g) \mid g \in G\}$ is a subgroup of G'.

   The set $f(G) = \{f(g) \mid g \in G\}$ is called the homomorphic image of G in G'.

3. If $f: G \to G'$ is a homomorphism of a group G into G' and H is a subgroup of G, then $f(H)$ is again a subgroup of G'.

4. If $f: G \to G$ be a homomorphism from the group G into itself and H is a cyclic subgroup of G, then $f(H)$ is again a cyclic subgroup of G.

Kernel of a Homomorphism.

Let $f: G \to G'$ be a homomorphism from the group G into G' and e' be the identity element of G'.

The subset K of G defined by $K = \{a \in G \mid f(a) = e'\}$ is called the Kernel of the Homomorphism f and is denoted by $\ker f$.

Results related to Isomorphism

1. If $f: G \to G'$ be an isomorphism of a group G onto a group G' and a is any element of G, then the order of $f(a)$ equals the order of a.
2. Let $f: G \to G'$ be an isomorphism. If G is abelian, then G' is also abelian.
3. Any infinite cyclic group is isomorphic to the group $\mathbb{Z}$ of integers, under addition.
4. Any finite cyclic group of order n is isomorphic to additive group of integers modulo n.

Examples

1. Show that the additive group $\langle \mathbb{R}, + \rangle$ of all real numbers and the multiplicative group $\langle \mathbb{R}^+, \cdot \rangle$ of all positive real numbers are isomorphic.

Sol^n Define $f: \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}^+, \cdot \rangle$ by $f(x) = e^x \; \forall x \in \mathbb{R}$.

Now $f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$

$\therefore$ f is a homomorphism.

Again, $f(x) = f(y) \Rightarrow e^x = e^y$

$\Rightarrow e^{x-y} = 1 = e^0$

$\Rightarrow x - y = 0$

$\Rightarrow x = y$

$\therefore$ f is one-one.

Let $y \in \mathbb{R}^+$, Consider $f(\log_e y) = e^{\log_e y} = y$

$\therefore \forall y \in \mathbb{R}^+ \; \exists \; \log_e y \in \mathbb{R}$ such that $f(\log_e y) = y$

$\therefore$ f is onto

Hence f is a isomorphism.

2. Let $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{R}^+ \right\}$. show that $f: \langle G, \cdot \rangle \to \mathbb{R}^+$ defined by $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$ is an isomorphism.

Soln

$$f\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}\right) = f\begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = ab = f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot f\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$$

$\therefore f$ is a homomorphism.

Let $f(a) = f(b) \Rightarrow \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow a = b$.

$\therefore f$ is one-one.

Let $a \in \mathbb{R}^+$, Consider $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$;

$\therefore \forall a \in \mathbb{R}^+, \exists \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in \langle G, \cdot \rangle$ such that $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$.

$\therefore f$ is onto.

Hence f is an isomorphism.

Exercise!

1. Verify if the following maps are homomorphisms?. If the map is a homomorphism, find its kernel.

(i) $f: \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}^+, \cdot \rangle$ defined by $f(x) = e^x \ \forall x \in \mathbb{R}$

(ii) $f: \langle \mathbb{Z}, + \rangle \to \langle \mathbb{Z}_n, +_n \rangle$ defined by $f(a) = r, \forall a \in \mathbb{Z}$, where r is the unique least non negative remainder when a is divided by n.

(iii) $g: \langle \mathbb{Q}^*, \cdot \rangle \to \langle \mathbb{Q}, \cdot \rangle$ defined by $g(x) = |x|, \forall x \in \mathbb{Q}^*$.

(iv) $f: \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}, + \rangle$ defined by $f(x) = 3x + 1, \forall x \in \mathbb{R}$

2. Show that the following mappings are isomorphisms.

(i) $T: \langle G, + \rangle \to \langle G, + \rangle$, where $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, defined by $T(a + b\sqrt{2}) = a - b\sqrt{2}$.

(ii) G is any group of g a fixed element of G. $T: G \to G$ defined by $T(x) = gxg^{-1}$.