Homomorphism, Isomorphisms of Groups

⇒ Let $(G, \cdot)$, $(G', *)$ be two group.
A mapping $f: G \longrightarrow G'$ is called a homomorphism, if

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

In other words, a homomorphism preserves the compositions in the group G and G'.
However, if we are not specific about the compositions of the group G and G', we say that a mapping $f: G \longrightarrow G'$ is a homomorphism,

$$\text{if } f(ab) = f(a) \cdot f(b) \quad \text{—— (1)}$$
$$\forall\, a, b \in G.$$

Note: In equation (1), the product ab on LHS takes place in G, while the product $f(a) \cdot f(b)$ on RHS takes place in G'.

⇒ If $f: G \longrightarrow G'$ is a homomorphism and onto then the group G' is said to be a homomorphic image of a group G. or f is said to be a homomorphism G onto G'. we write this as $f(G) = G'$.
In this case write $G \simeq G'$.
(read as G is homorphic to G')

⇒ Homomorphism onto sometimes called as ephimorphism.

⇒ Let G, G' be two groups. If $f: G \longrightarrow G'$ is homomorphism and one-one then 'f' is ided isomorphism from $G \longrightarrow G'$.

⇒ If $f: G \longrightarrow G'$ is homomorphism, one-one and onto then G' is called isomorphic image of G (or) G is isomorphic to G' and we write

$$G \cong G'$$

Note: If the group G is finite, then G can be isomorphic to G', only if G' is also finite and the number of elements in G is equal to the number of elements in G'.

otherwise there will exist no mapping from G to G' which is one-one and onto.

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

⇒ An isomorphism of a group into itself is called an automorphism.

1-1 homomorphism = Isomorphism.

1-1 Endomorphism = Automorphism.

Examples:

Let $G = (\mathbb{Z}, +)$ and $G' = \{2^n / n \in \mathbb{Z}\}$, where G' is a group w.r.t x^n.

Now, we define a mapping, $f: G \longrightarrow G'$ such that

$$f(n) = 2^n, \forall\, n \in \mathbb{Z}.$$

Now, for all $n_1, n_2 \in G$
$\Rightarrow n_1 + n_2 \in G$ and $f(n_1) = 2^{n_1}$, $f(n_2) = 2^{n_2}$

Now, we have
$f(n_1 + n_2) = 2^{n_1 + n_2}$ (by def^n)
$= 2^{n_1} \cdot 2^{n_2}$.
$\therefore f(n_1 + n_2) = f(n_1) \cdot f(n_2), \forall\, n_1, n_2 \in G$.
$\therefore$ f is homomorphism.

To show f is 1-1:
Let $n_1, n_2 \in G$, then we have $f(n_1) = f(n_2)$
$\Rightarrow 2^{n_1} = 2^{n_2} \Rightarrow n_1 = n_2$

$\therefore$ f is 1-1.

$\therefore f$ is an isomorphism.

Theorem: Prove that $G = R^+$ is a group under x^n and $G' = R$ is a group under $+^n$.

Solution: Now, we define a mapping
$f: G \longrightarrow G'$
such that $f(x) = \log_{10} x \quad \forall\, x \in G$.
Now, for all $x_1, x_2 \in G \Rightarrow x_1 x_2 \in G$ and $f(x_1) = \log_{10} x_1$
$f(x_2) = \log_{10} x_2$

Now, we have

$$f(x_1 \cdot x_2) = \log_{10}(x_1 \cdot x_2) \quad (\text{by def}^n)$$
$$= \log_{10} x_1 + \log_{10} x_2$$
$$= f(x_1) + f(x_2)$$

$\therefore$ f is homomorphism.

To show f is 1-1.

we have $f(x_1) = f(x_2)$, $\forall x_1, x_2 \in G$.

$\Rightarrow \log_{10} x_1 = \log_{10} x_2$

$\Rightarrow x_1 = x_2$

$\therefore$ f is 1-1.

$\therefore$ f is isomorphism.

To show f is onto.

Let $y \in G' = R$

$\therefore 10^y$ is a +ive real number.

$\Rightarrow 10^y \in G = R^+$.

$\therefore f(10^y) = \log_{10} 10^y = y \log_{10} 10 = y(1) = y$

$\therefore f(10^y) = y$

$\therefore$ for every $y \in G'$. $\exists$ $10^y \in G$ such that $f(10^y) = y$.

$\therefore$ f is onto.

G' is isomorphic image of G.

Properties of homomorphism:

Theorem ①:

Let $(G,\cdot)$, $(G',\circ)$ be two groups. Let f be a homomorphism from G into G', then

(i) $f(e) = e'$, where e' is the identity in G and e' is the identity.

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

Proof: (i) $f(e) = f(e\cdot e)$

$\Rightarrow f(e\cdot e) = f(e)$

$\Rightarrow f(e)\cdot f(e) = e' f(e)$ ($\because f$ is homomorphism and $e'\cdot f(e) \in G'$)

$\Rightarrow f(e) = e'$ (By RCL in G')

(ii) Let $a \in G \Rightarrow a^{-1} \in G$ and $a a^{-1} = e$

Now, we have

$f(a a^{-1}) = f(a)\cdot f(a^{-1})$

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

$= f(e)$

$= e'$, where $f(a), f(a^{-1}), f(e) \in G'$

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

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

Theorem:

Theorem (2) If f is a homomorphism from a group $(G, \cdot)$ into $(G', \cdot)$, then $(f(G), \cdot)$ is a subgroup of G'.

Proof: By def^n:

$$f(G) = \{f(a) / a \in G\} \text{ and } f(G) \subseteq G'.$$

Let $a', b' \in f(G)$

$\therefore \exists\ a, b \in G$ such that $f(a) = a'$ & $f(b) = b'$.

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

$= f(ab^{-1})$ ($\because f$ is homo.)

$\in f(G)$

($\because a, b \in G \Rightarrow ab^{-1} \in G$)

$\therefore a'(b')^{-1} \in f(G)$, $\forall\ a', b' \in f(G)$.

$\therefore f(G)$ is a subgroup of G'.

i.e the homomorphic image of the group G is a subgroup of G'.

i.e the homomorphic image of a group is a group.

Hence Proved

Theorem: (3)

Every homomorphic image of an abelian group G is abelian.

Proof: Let $(G,\cdot)$ be an abelian group and $(G',\cdot)$ be a group.

Let $f: G \longrightarrow G'$ be a homomorphism and onto.

$\therefore G'$ is the homomorphic image of G.

i.e $G' = f(G)$.

Let $a', b' \in G'$.

$\therefore \exists$ elements $a, b \in G$ such that $f(a) = a'$ & $f(b) = b'$.

Since G is abelian.

$\therefore ab = ba$.

Now $a'b' = f(a) \cdot f(b)$

$= f(ab)$.

$= f(ba)$.

$= f(b) \cdot f(a)$.

$= b' \cdot a'$

$\therefore a'b' = b'a'$, $\forall a', b' \in G'$

$\therefore G'$ is an abelian.

Hence Proved

Note: The converse of the above theorem need not be true. i.e If the homomorphic image of a group G is abelian then the group need not be abelian.

for EX:

X P_3 is non-abelian group.

A_3 is normal subgroup of P_3.

The quotient group $\frac{P_3}{A_3}$ is a homomorphic image of P_3.

Now $\frac{P_3}{A_3}$ is of order 2 and it abelian.

Note :→ Even f is an isomorphism:

(i) Substitute 'isomorphism' for homomorphism in Theorem (1) and it is true. The same proof holds.

(ii) Substitute 'isomorphism' for homomorphism in Theorem (2) and it is true. The same proof holds.

(iii) Substitute 'isomorphism onto' for homomorphism onto in Theorem (3) and it is true. The same proof holds. The converse of the theorem is true.

Theorem:

Let G be a group and G' be a non-empty set. If there exists a mapping 'f' from G onto G' such that $f(ab) = f(a) \cdot f(b)$ for $a, b \in G$ then G' is a group.

Proof: $f: G \to G'$ is onto such that $f(ab) = f(a) \cdot f(b)$ $\forall\ a, b \in G$.

To prove that G' is a group.

(i) closure Prop.

Let $a', b' \in G'$

Since f is onto, $\exists\ a, b \in G$, such that

$f(a) = a'$ & $f(b) = b'$

Also $a, b \in G \Rightarrow f(ab) \in G'$

$\therefore a'b' = f(a) f(b)$

$= f(ab) \in G'$.

$\therefore a'b' \in G'$

(ii) Associative Property.

Let $a', b', c' \in G'$

Since f is onto, $\exists\ a, b, c \in G$ such that

$f(a) = a'$, $f(b) = b'$, $f(c) = c'$.

Now $a'(b'c') = (f(a) \cdot f(b)) \cdot f(c)$

$= f(ab) \cdot f(c)$ by def^n.

$= f[(ab)c]$

$= f[a(bc)]$ ($\because G$ is group)

$= f(a) f(bc)$

$= f(a) \cdot [f(b) \cdot f(c)]$

$= a' \cdot (b'c')$ $\therefore G'$ is Associative.

Existenc of left Identity

Let $a' \in G'$

Let e be the identity element in G.

since f is onto.

$\therefore f(e) = e' \in G'$, $\exists\, a \in G$ such that $f(a) = a'$.

Now $e'a' = f(e) \cdot f(a) = f(ea) = f(a)$ $(\because ea = a \; \forall a \in G)$

$\therefore e'a' = a'$

$\therefore$ Identity exists in G' and it is $f(e) = e'$.

Existence of left Inverse.

Let $a' \in G'$ $\exists\, a \in G$ such that $f(a) = a'$,

$\therefore a^{-1} \in G$ and $f(a^{-1}) \in G'$.

Now $f(a^{-1})a' = f(a^{-1}) \cdot f(a) = f(a^{-1}a) = f(e) = e'$.

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

$\therefore f(a^{-1})$ is the inverse of a' in G'.

$\therefore$ Every element of G' is invertible.

$\therefore G'$ is a group.

Note: when f is a one-one mapping from G into G', this theorem is not true.