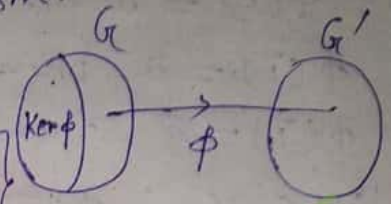
2SH
CC4

RAMSADAY COLLEGE

HOMOMORPHISM (2)

Swastika Das.

Definition:- Let $(G,\circ)$ and $(G',*)$ be two groups and $\phi: G \to G'$ be a homomorphism. Then the kernel of ϕ, denoted by $\ker\phi$, is a subset of G defined by $\ker\phi = \{a \in G : \phi(a) = e_{G'}\}$



Theorem-1:- Let $\phi: (G,\circ) \to (G',*)$ be a homomorphism. Then $\ker\phi$ is a normal subgroup of G.

Proof:- $e_G \in \ker\phi$, as $\phi(e_G) = e_{G'}$

So, $\ker\phi$ is a non-empty subset of G.

Let, $a, b \in \ker\phi$. Then $\phi(a) = e_{G'}$, $\phi(b) = e_{G'}$ and

$$\begin{aligned}\phi(a\circ b^{-1}) &= \phi(a) * \{\phi(b)\}^{-1} \\ &= e_{G'} * \{e_{G'}\}^{-1} \\ &= e_{G'}\end{aligned}$$

Therefore, $a\circ b^{-1} \in \ker\phi$.

So, $\ker\phi$ is a subgroup of G.

To prove that, $\ker\phi$ is normal in G, let $g \in G$, $h \in \ker\phi$. Then

$$\begin{aligned}\phi(g\circ h\circ g^{-1}) &= \phi(g) * \phi(h) * \phi(g^{-1}), \text{ since } \phi \text{ is a homomorphism} \\ &= \phi(g) * \phi(g^{-1}), \text{ since } \phi(h) = e_{G'} \\ &= \phi(g\circ g^{-1}) \\ &= \phi(e_G) = e_{G'}\end{aligned}$$

Therefore, $g\circ h\circ g^{-1} \in \ker\phi$ and this proves that $\ker\phi$ is normal in G.

Theorem-2:- Let $\phi: (G,\circ) \to (G',*)$ be a homomorphism. Then ϕ is one-to-one iff $\ker\phi = \{e_G\}$.

Proof:- Let ϕ be one-to-one.

Now, $\phi(e_G) = e_{G'} \Rightarrow e_G$ is a pre-image of $e_{G'}$.

Since ϕ is one-to-one, e_G is the only pre-image of $e_{G'}$. Therefore, $\ker\phi = \{e_G\}$.

- Conversely let, ϕ be a homomorphism and $\ker\phi = \{e_G\}$. To show ϕ is one-to-one.

Scanned with CamScanner

Let, $a, b \in G$ and $\phi(a) = \phi(b)$.

Then $\phi(a^{-1}b) = \{\phi(a)\}^{-1} * \phi(b) = \{\phi(b)\}^{-1} * \phi(b)$
$= e_{G'}$.

This shows that, $a^{-1}b \in \ker\phi$
and $\ker\phi = \{e_G\}$. So, $a^{-1}b = e_G$
$\Rightarrow a = b$.

Thus, $\phi(a) = \phi(b) \Rightarrow a = b$ and this proves that ϕ is one-to-one.

Example-1:- Let $G = (\mathbb{C}^*, \cdot)$, $G' = (\mathbb{R}^+, \cdot)$ and $\phi : G \to G'$ is defined by $\phi(z) = |z|$, $z \in \mathbb{C}^*$. Prove that ϕ is a homomorphism. Determine $\ker\phi$.

■ Let, $a, b \in G$. Then $ab \in G$.
Now, $\phi(a) = |a|$, $\phi(b) = |b|$ and $\phi(ab) = |ab|$
$= |a||b|$
$= \phi(a)\phi(b)$

So, $\phi(ab) = \phi(a)\phi(b)$, $\forall a, b \in G$.
So, ϕ is a homomorphism.

Now, $\ker\phi = \{z \in G : \phi(z) = 1\}$
$= \{z \in G : |z| = 1\}$.

• Definition:-(Isomorphism)
Let $(G, \circ)$ and $(G', *)$ be two groups and $\phi : G \to G'$ be a homomorphism. ϕ is said to be an isomorphism if ϕ is a monomorphism as well as an epimorphism.

Theorem-2:- Let $(G, \circ)$ and $(G', *)$ be two groups and $\phi : G \to G'$ be an epimorphism. ~~ϕ is said~~ Then ϕ is an isomorphism iff $\ker\phi = \{e_G\}$.

Theorem-3:- Let $(G, \circ)$ and $(G', *)$ be two groups and $\phi : G \to G'$ be an isomorphism. Then
(i) $o(a) = o(\phi(a))$ for every $a \in G$;
(ii) the sets G and G' have the same cardinality.

Scanned with CamScanner

Theorem-4:- Let $\phi : (G, \circ) \to (G', *)$ be an isomorphism. Then (i) G' is commutative iff G is commutative,
(ii) G' is cyclic iff G is cyclic.

Note:- If a be a generator of G, then $\phi(a)$ is a generator of G'.

Theorem-5:- Let $\phi : (G, \circ) \to (G', *)$ be an isomorphism. Then $\phi^{-1} : (G', *) \to (G, \circ)$ is also an isomorphism.

Proof:- $\phi : G \to G'$ is an isomorphism. So, $\phi : G \to G'$ is bijective. So, $\phi : G \to G'$ is invertible, i.e., ϕ^{-1} exists and ϕ^{-1} is a bijective mapping.

Let, $a', b' \in G'$. Let; $\phi^{-1}(a') = a$, $\phi^{-1}(b') = b$.
Then $\phi(a) = a'$, $\phi(b) = b'$.

$$\begin{aligned}
\phi^{-1}(a' * b') &= \phi^{-1}[\phi(a) * \phi(b)] \\
&= \phi^{-1}[\phi(a \circ b)], \text{ since } \phi \text{ is a homomorphism} \\
&= a \circ b, \text{ since } \phi^{-1}\phi \text{ is the identity mapping on } G. \\
&= \phi^{-1}(a') \circ \phi^{-1}(b').
\end{aligned}$$

This proves that, ϕ^{-1} is a homomorphism.
Since ϕ^{-1} is a bijection, ϕ^{-1} is an isomorphism.

Example-2:- G is a multiplicative commutative group of order 8. Prove that $\phi : G \to G$ defined by $\phi(x) = x^3$, $x \in G$ is an isomorphism.

Ans:- Let, $a, b \in G$. So, $ab \in G$.
Now, $\phi(a) = a^3$, $\phi(b) = b^3$ and

$$\begin{aligned}
\phi(ab) &= (ab)^3 \\
&= a^3 b^3, \text{ since } G \text{ is commutative} \\
&= \phi(a)\,\phi(b).
\end{aligned}$$

So, $\phi(ab) = \phi(a)\,\phi(b)$, $\forall\, a, b \in G$.
So, ϕ is a homomorphism.

Now, $\ker \phi = \{x \in G : \phi(x) = e_G\}$
$= \{x \in G : x^3 = e_G\}$.

Now, $x^3 = e_G \Rightarrow o(x) \mid 3$.
Again, $o(G) = 8$ and $x \in G \Rightarrow o(x) \mid 8$.

Scanned with CamScanner

So, $o(x)$ is a common divisor of 3 and 8.

So, $o(x) = 1 \Rightarrow x = e_G$.

So, $\ker\phi = \{e_G\}$.

Therefore ϕ is one-to-one.

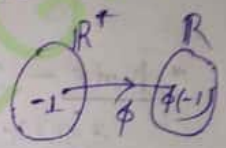
Thus, G is a finite group and $\phi: G \to G$ is one-to-one. So, ϕ is onto.

Therefore ϕ is an isomorphism.

Example-3:- Show that the groups $(\mathbb{R}^*, \cdot)$ and $(\mathbb{R}, +)$ are not isomorphic. $[\mathbb{R}^* = \mathbb{R} \setminus \{0\}]$.

Ans:- If possible let, $\phi: (\mathbb{R}^*, \cdot) \to (\mathbb{R}, +)$ be an isomorphism.

$-1 \in \mathbb{R}^*$ and $o(-1) = 2$. $\phi(-1) \in \mathbb{R}$



Since ϕ is an isomorphism, $o(\phi(-1))$ must be 2. But there is no element of order 2 in $(\mathbb{R}, +)$.

Therefore ϕ does not exist.

So, the groups are not isomorphic.

Theorem-6:- Two finite cyclic groups of the same order are isomorphic.

Proof:- Let $G = \langle a \rangle$ and $G' = \langle b \rangle$ be two cyclic groups of order n.

Then, $o(a) = n$ and $G = \{e_G, a, a^2, \cdots, a^{n-1}\}$.

$o(b) = n$ and $G' = \{e_{G'}, b, b^2, \cdots, b^{n-1}\}$.

Let us define a mapping $\phi: G \to G'$ by $\phi(a^s) = b^s$, $s = 0, 1, 2, \cdots, n-1$.

Then ϕ is obviously a bijection.

First we prove that, $\phi(a^k) = b^k$ for every integer k (not merely for $k = 0, 1, 2, \cdots, n-1$).

By division algorithm, let $k = nq + r$, where q and r are integers and $0 \le r \le n-1$.

Then $a^k = a^r$ and $b^k = b^r$ and

$\phi(a^k) = \phi(a^r) = b^r$, since $0 \le r \le n-1$

$= b^k \longrightarrow (1)$

To prove that, ϕ is a homomorphism, let $a^p \in G$, $a^q \in G$, where $0 \le p \le n-1$, $0 \le q \le n-1$.

Scanned with CamScanner

Then $\phi(a^p a^q) = \phi(a^{p+q}) = b^{p+q}$, by (1)

$= b^p b^q$

$= \phi(a^p)\phi(a^q)$

This shows that ϕ is a homomorphism.
Since ϕ is a bijection, ϕ is an isomorphism.
Thus G and G' are isomorphic.
This completes the proof.

- **Corollary** – A finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$.
- **Note** – Since all groups of a prime order p are cyclic and all cyclic group of the same order are isomorphic, so we can say that, there is only one group of a prime order p upto isomorphism.

Theorem – 7 → Two infinite cyclic groups are isomorphic.

Note:- Any infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.

** **Permutation groups.**

Let A be a nonempty set. A bijective mapping on A is said to be a permutation on A.

Let S be the set of all bijective mappings on A. Then $(S, \circ)$ is a group, where $\circ$ is the composition of mappings. This group is called the group of all permutations on A.

In particular, if A be a finite set containing n elements, then the group of all permutations on A is the symmetric group S_n.

A subgroup of the group of all permutations on A is called a permutation group.

Scanned with CamScanner

Theorem-8 (Cayley) :-

A finite group G of order n is isomorphic to a subgroup of S_n.

Proof:- Let, $G = \{g_1, g_2, \cdots, g_n\}$.

Let g be an arbitrary element of G.

Then the elements $gg_1, gg_2, \cdots, gg_n$ all belong to G and no two of these are equal, because $gg_r = gg_s \Rightarrow g_r = g_s$, by left cancellation law

Therefore $\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix}$ is a permutation on the set $\{g_1, g_2, \cdots, g_n\}$.

We denote this permutation by π_g.

Let S_n be the set of all permutations on the set $\{g_1, g_2, \cdots, g_n\}$.

Let us define a mapping $\phi : G \to S_n$ by $\phi(g_i) = \pi_{g_i}$

i.e., $\phi(g_i) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_ig_1 & g_ig_2 & \cdots & g_ig_n \end{pmatrix}$ for $i = 1, 2, \cdots, n$.

To prove that ϕ is a homomorphism, let $g_i, g_j \in G$

Then $g_ig_j \in G$.

$$\phi(g_ig_j) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_ig_jg_1 & g_ig_jg_2 & \cdots & g_ig_jg_n \end{pmatrix}$$

$$= \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_ig_1 & g_ig_2 & \cdots & g_ig_n \end{pmatrix} \circ \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_jg_1 & g_jg_2 & \cdots & g_jg_n \end{pmatrix}$$

$$= \phi(g_i) \circ \phi(g_j)$$

Therefore ϕ is a homomorphism.

- For $x \in G$, $x \in \ker\phi \Leftrightarrow \phi(x) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 & g_2 & \cdots & g_n \end{pmatrix}$

$$\Leftrightarrow \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ xg_1 & xg_2 & \cdots & xg_n \end{pmatrix} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 & g_2 & \cdots & g_n \end{pmatrix}$$

$\Leftrightarrow xg_k = g_k$, for $k = 1, 2, \cdots, n$.

$\Leftrightarrow x = e_G$.

Therefore, $\ker\phi = \{e_G\}$ and therefore ϕ is a monomorphism.

Scanned with CamScanner

Also $\phi(G)$ is a subgroup of S_n and therefore $G \simeq \phi(G)$.

It follows that G is isomorphic to a subgroup of S_n.

This completes the proof.

Note:- The subgroup $\phi(G)$ is $\{\pi_{g_1}, \pi_{g_2}, \dots, \pi_{g_n}\}$

Example-4: Find the permutation group isomorphic to the group $G = (\{1, i, -1, -i\}, \cdot)$.

Ans: G is isomorphic to the permutation group $\{\pi_1, \pi_i, \pi_{-1}, \pi_{-i}\}$, where

$$\pi_1 = \begin{pmatrix} 1 & i & -1 & -i \\ 1\cdot 1 & 1\cdot i & 1\cdot(-1) & 1\cdot(-i) \end{pmatrix} = \begin{pmatrix} 1 & i & -1 & -i \\ 1 & i & -1 & -i \end{pmatrix};$$

$$\pi_i = \begin{pmatrix} 1 & i & -1 & -i \\ i\cdot 1 & i\cdot i & i\cdot(-1) & i\cdot(-i) \end{pmatrix} = \begin{pmatrix} 1 & i & -1 & -i \\ i & -1 & -i & 1 \end{pmatrix};$$

$$\pi_{-1} = \begin{pmatrix} 1 & i & -1 & -i \\ -1\cdot 1 & -1\cdot i & (-1)\cdot(-1) & (-1)\cdot(-i) \end{pmatrix} = \begin{pmatrix} 1 & i & -1 & -i \\ -1 & -i & 1 & i \end{pmatrix}$$

$$\pi_{-i} = \begin{pmatrix} 1 & i & -1 & -i \\ (-i)\cdot 1 & (-i)\cdot i & (-i)(-1) & (-i)(-i) \end{pmatrix} = \begin{pmatrix} 1 & i & -1 & -i \\ -i & 1 & i & -1 \end{pmatrix}$$

Scanned with CamScanner