e content for students of patliputra university

B. Sc. (Honrs) Part 2paper 3

Subject:Mathematics

Title/Heading of topic:Homomorphism and isomorphism

By Dr. Hari kant singh

Associate professor in mathematics

Rrs college mokama patna

What is a Homomorphism?

Definition: Let G and H be groups and suppose $f : G \longrightarrow H$ is a function such that for all $x, y \in G$,

$$f(xy) = f(x)f(y).$$

Then f is called a group homomorphism, or just homomorphism for short. In words, we say "f preserves products."

Note: to calculate xy we are using the operation in G, but to calculate $f(x)f(y)$ we are using the operation in H.

Examples

1. $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ by $f(x) = |x|$
   $f(xy) = |xy| = |x||y| = f(x)f(y)$.
2. $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ by $f(x) = x^2$
   $f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$.
3. $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ by $f(m) = m \bmod n$, with addition. Use the division algorithm to write

$$m_1 = p_1 n + q_1, m_2 = p_2 n + q_2.$$

Then $m_1 + m_2 = (p_1 + p_2)n + q_1 + q_2$, so

$$f(m_1+m_2) = (q_1+q_2) \bmod n \equiv q_1 \bmod n + q_2 \bmod n = f(m_1)+f(m_2$$

Not All Functions are Homomorphisms

Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ by $f(x) = x^2$. The operation is addition. Then

$$f(x + y) = (x + y)^2 = x^2 + 2xy + y^2$$

but

$$f(x) + f(y) = x^2 + y^2.$$

So it is not true that $f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$, so f is not a homomorphism.

Some More Interesting Examples

The determinant function, $\det : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$, is a homomorphism, since

$$\det(AB) = \det(A)\ \det(B).$$

Define $\text{sgn} : S_n \longrightarrow \{1, -1\}$ by

$$\text{sgn}\,(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is an even permutaton} \\ -1 & \text{if } \sigma \text{ is an odd permutaton} \end{cases}$$

You have to check that for all $\alpha, \beta \in S_n$,

$$\text{sgn}\,(\alpha\beta) = \text{sgn}\,(\alpha)\,\text{sgn}\,(\beta),$$

which boils down to checking four cases, namely even plus even is even, even plus odd is odd, odd plus even is odd, and odd plus odd is even.

Properties of Homomorphisms:

Let $f : G \longrightarrow H$ be a homomorphism. Then

1. $f(e_G) = e_H$
   Proof:
   $x = xe_G \Rightarrow f(x) = f(xe_G) = f(x)f(e_G) \Rightarrow e_H = f(e_G)$.
2. $f(x^n) = (f(x))^n$, for all $x \in G$ and all $n \in Z$
   Proof: $f(x^2) = f(x\,x) = f(x)\,f(x) = (f(x))^2$, etc for positive n. If $n = -1$, then
   $xx^{-1} = e_G \Rightarrow f(xx^{-1}) = f(e_G) \Rightarrow f(x)f(x^{-1}) = e_H \Rightarrow$
   $f(x^{-1}) = (f(x))^{-1}$.
3. If $|x|$ is finite, then $|f(x)|$ divides $|x|$
   Proof: let $|x| = n$. Then
   $x^n = e_G \Rightarrow f(x^n) = f(e_G) \Rightarrow (f(x))^n = e_H \Rightarrow$
   $|f(x)|$ divides n.

Kernels and Images

If $f : G \longrightarrow H$ is a homomorphism, define

1. $\ker(f) = \{x \in G \mid f(x) = e_H\}$
2. $\text{im}\,(f) = \{f(x) \mid x \in G\} = f(G)$

Then

$$\ker(f) \leq G \text{ and } \text{im}\,(f) \leq H.$$

Proof: (for kernel)

- $f(e_G) = e_H \Rightarrow e_G \in \ker(f)$.
- $x, y \in \ker(f)$
  $\Rightarrow f(xy^{-1}) = f(x)f(y^{-1}) = f(x)\,(f(y))^{-1} = e_H\, e_H = e_H$,
  so $xy^{-1} \in \ker(f)$.
- Proof that $\text{im}\,(f) \leq H$ is left as an exercise.

Examples

1. For $\det : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$,
   $\ker(\det) = \{A \in GL(n, \mathbb{R}) \mid \det(A) = 1\} = SL(n, \mathbb{R})$.
2. For $\text{sgn} : S_n \longrightarrow \{1, -1\}$
   $\ker(\text{sgn}) = \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\} = A_n$.
3. For $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ by $f(m) = m \bmod n$, with addition,

$$\ker(f) = \{m \mid m \equiv 0 \bmod n\} = < n >$$

and

$$\text{im}(f) = \{m \bmod n \mid m \in \mathbb{Z}\} = \mathbb{Z}_n.$$

Properties of Subgroups Under Homomorphisms

First three parts of Theorem 10.2: let $f : G \longrightarrow H$ be a homomorphism and let K be a subgroup of G. Then

1. $f(K) = \{f(k) \mid k \in K\}$ is a subgroup of H.
2. If K is cyclic then $f(K)$ is cyclic.
3. If K is Abelian then $f(K)$ is Abelian.

Proof: 1. left as an exercise.

2. Suppose $K = \langle k \rangle$. Then $x \in K \Rightarrow x = k^n$. Then

$$f(x) = f(k^n) = (f(k))^n,$$

which means that $f(K) = \langle f(k) \rangle$.

3. Suppose $xy = yx$ for all $x, y \in K$. Then

$$f(xy) = f(yx) \Leftrightarrow f(x)f(y) = f(y)f(x),$$

which means all elements in $f(K)$ commute.

Example

Let $f : \mathbb{R} \longrightarrow GL(2, \mathbb{R})$ by $f(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$. f is a homomorphism because $f(\alpha)f(\beta) = f(\alpha + \beta)$:

$$\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix} = \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+ \\ \sin(\alpha+\beta) & \cos(\alpha \end{bmatrix}$$

using appropriate trig identities. Check that $\ker(f) = \langle 2\pi \rangle$ and $\mathrm{im}\,(f)$ is the group of 2×2 rotation matrices. In particular, $\mathbb{R}$ is Abelian, so $\mathrm{im}\,(f)$ is Abelian and $\mathrm{im}\,(f)$ is an Abelian subgroup of $GL(2, \mathbb{R})$. If the positive integer n is fixed and

$$K = \left\langle \frac{2\pi}{n} \right\rangle = \left\{ \frac{2\pi k}{n} \mid k \in \mathbb{Z} \right\},$$

then $f(K) = \langle f(2\pi/n) \rangle \leq D_n$, consisting of all rotations of a regular n-gon.

One-to-one and Onto Homomorphisms

Let $f : G \longrightarrow H$ be a group homomorphism.
Definition: f is called one-to-one if

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Defintion: f is called onto if every element in H is in $\mathrm{im}(f)$.
Theorem: let $f : G \longrightarrow H$ be a group homomorphism.

- f is one-to-one if and only if $\ker(f) = \{e_G\}$
- f is onto if and only if $\mathrm{im}(f) = H$

Proof: (for one-to-one) suppose f is one-to-one: Let $x \in \ker(f)$
Then $f(x) = e_H$ and $f(e_G) = e_H$. Therefore $x = e_G$.
Now suppose $\ker(f) = \{e_G\}$, and let $f(x_1) = f(x_2)$. Then

$$f(x_1x_2^{-1}) = f(x_1)f(x_2^{-1}) = f(x_1)(f(x_2))^{-1} = f(x_1)(f(x_1))^{-1} = e$$

Thus $x_1x_2^{-1} \in \ker(f) \Rightarrow x_1x_2^{-1} = e_G \Rightarrow x_1 = x_2$.

What is an Isomorphism?

Let $f : G \longrightarrow H$ be a group homomorphism.
Definition: f is called an isomorphism if f is one-to-one and onto
Thus f is an isomorphism if $\ker(f) = \{e_G\}$ and $\text{im}\,(f) = H$.
Note: every isomorphism $f : G \longrightarrow H$ has an inverse
$f^{-1} : H \longrightarrow G$, defined by

$$f^{-1}(x) = y \Leftrightarrow x = f(y),$$

which is also an isomorphism.
Definition: if there is an isomorphism $f : G \longrightarrow H$, then we say the groups G and H are isomorphic, and we write

$$G \approx H.$$

Example 1

Let $H = \left\{ \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \in GL(2,\mathbb{R}) \mid m \in \mathbb{Z} \right\}$ and define $f : \mathbb{Z} \longrightarrow H$ by

$$f(m) = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}.$$

Then f is an isomorphism:

1. f is a homomorphism since

$$f(m+n) = \begin{bmatrix} 1 & m+n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = f(m)f(n$$

2. f is one-to-one since $f(m) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow m = 0$
3. f is onto since obviously $\mathrm{im}\,(f) = H$.

Example 2

Let $G = \langle a \rangle$ be a cyclic group of order n. Then $G \approx \mathbb{Z}_n$.
Proof: for $k \in \mathbb{Z}$, define $f : G \longrightarrow \mathbb{Z}_n$ by $f(a^k) = k \bmod n$.

- f is well-defined: $a^j = a^k \Rightarrow n$ divides $j - k \Rightarrow j \equiv k \bmod n$.
- f is a homomorphism: $f(a^j a^k) = f(a^{j+k}) = (j + k) \bmod n$; and $f(a^j) + f(a^k) = j \bmod n + k \bmod n = (j + k) \bmod n$.
- f is one-to-one:
  $f(a^k) = 0 \Rightarrow k \equiv 0 \bmod n \Rightarrow k = qn \Rightarrow a^k = (a^n)^q = e_G$.
- f is onto: this is obvious since $k \in \mathbb{Z}$, so $\mathrm{im}\,(f) = \mathbb{Z}_n$.

Alternate Proof: use $g : \mathbb{Z}_n \longrightarrow G$ defined by $g(m) = a^m$. ($g = f^{-1}$.) This makes the algebra easier since g is obviously well-defined.

Properties of Isomorphisms

Let $f : G \longrightarrow H$ be an isomorphism.

Then

1. $f^{-1} : H \longrightarrow G$ is also an isomorphism
2. $f(e_G) = e_H$
3. for all $x \in G, f(x^n) = (f(x))^n$
4. x, y commute in G if and only if $f(x), f(y)$ commute in H
5. $G = \langle x \rangle$ if and only if $H = \langle f(x) \rangle$
6. for all $x \in G, |x| = |f(x)|$
7. if G and H are finite groups, then $|G| = |H|$
8. G is Abelian if and only if H is Abelian
9. G is cyclic if and only if H is cyclic
10. $f(Z(G)) = Z(H)$

Some Proofs:

Properties 2 and 3 are true for all homomorphisms.

4. $xy = yx \Rightarrow f(xy) = f(yx) \Rightarrow f(x)f(y) = f(y)f(x)$; this is true for any homomorphism. But if f is an isomorphism, then $f(x)f(y) = f(y)f(x) \Rightarrow f(xy) = f(yx) \Rightarrow xy = yx$, since f is one-to-one

6. let $|x| = n, |f(x)| = m$. For any homomorphism f we know m divides n. If f is also an isomorphism: $(f(x))^m = e_H \Rightarrow$ $f(x^m) = e_H \Rightarrow x^m = e_G$, since f is one-to-one. Thus n divides m. So $m = n$.

8. follows from 4

9. follows from 5

10. $x \in Z(G) \Rightarrow xg = gx$, for all $g \in G \Rightarrow f(x)f(g) = f(g)f(x)$ $\Rightarrow f(x) \in Z(\text{im}\,(f))$. So, for any homomorphism, $f(Z(G)) \subset Z(\text{im}\,(f))$. If f is an isomorphism, then $\text{im}\,(f) = H$. For the other inclusion, repeat the argument for $f^{-1} : H \longrightarrow G$.

Example 3

Show $U(8) \approx \{(1), (12)(34), (13)(24), (23)(14)\}$
Solution: $U(8) = \{1, 3, 5, 7\}$. Define
$f : U(8) \longrightarrow \{(1), (12)(34), (13)(24), (23)(14)\}$ by

$$f(1) = (1),\ f(3) = (12)(34),\ f(5) = (13)(24),\ f(7) = (23)(14).$$

Now consider the multiplication tables of both groups:

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\circ$	(1)	(12)(34)	(13)(24)	(2
(1)	(1)	(12)(34)	(13)(24)	(2
(12)(34)	(12)(34)	(1)	(23)(14)	(1
(13)(24)	(13)(24)	(23)(14)	(1)	(1
(23)(14)	(23)(14)	(13)(24)	(12)(34)	

Observe that f maps the multiplication table on the left precisely
to the multiplication table on the right: i.e. $f(xy) = f(x)f(y)$. W
say, isomorphic groups have the same group structure.

Example 4

Finite groups that are isomorphic have the same order. But group can have the same order and not be isomorphic. For example, her are three groups of order 12: $\mathbb{Z}_{12}, D_6$, and A_4, no two of which ar isomorphic. There are many ways to show this:

- the largest order of any element in $\mathbb{Z}_{12}, D_6$ or A_4 is 12, 6, or 3, respectively.
- compare the number of elements of order 2: $\mathbb{Z}_{12}$ has 1, D_6 has 7, and A_4 has 3.
- $\mathbb{Z}_{12}$ is Abelian and cyclic; the biggest cyclic subgroup D_6 has is of order 6; the biggest cyclic subgroup A_4 has is of order 3

There are only five non-isomorphic groups of order 12: the three above, plus one other Abelian group and one other non-Abelian group.

Cayley's Theorem

Theorem 6.1: Every group is isomorphic to a group of permutations. If $|G| = n$, then G is isomorphic to a subgroup S_n.

Proof: given a group G we shall construct a group of permutations, H, and then show that $G \approx H$. For $g \in G$, defi $T_g : G \longrightarrow G$ by $T_g(x) = gx$. Since $T_g(g^{-1}y) = y$, T_g is on since $T_g(x) = T_g(y) \Rightarrow gx = gy \Rightarrow x = y$, T_g is one-to-one. Thus T_g is a permutation of all the elements of G. Let

$$H = \{T_g \mid g \in G\},$$

with function composition, and define $\phi : G \longrightarrow H$ by

$$\phi(g) = T_g.$$

We claim ϕ is an isomorphism:

1. ϕ is a homomorphism: $\phi(ab) = \phi(a) \circ \phi(b)$. To show two functions are equal you have to evaluate them at a point.
   $(\phi(ab))(x) = T_{ab}(x) = abx$ and
   $(\phi(a) \circ \phi(b))(x) = T_a(T_b(x)) = T_a(bx) = abx$.
2. ϕ is one-to-one: $\phi(a) = \phi(b) \Rightarrow T_a(x) = T_b(x)$, for all $x \in G$
   $\Rightarrow ax = bx \Rightarrow a = b$.
3. ϕ is onto: by definition of ϕ. For any $T_g \in H, \phi(g) = T_g$.

Finally, if $|G| = n$, then you can number the elements of G as $x_1, x_2, \ldots, x_n$ and each element $T_g \in H$ can be considered as a permutation $\sigma \in S_n$ defined by

$$T_g(x_i) = x_{\sigma(i)}.$$

Note: Example 3 above showed that $U(8)$ is isomorphic to a subgroup of S_4.