01/09

Homomorphism of Groups

Let G, G' be groups. A function $f: G \to G'$ is said to be a group homomorphism if

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

A group homomorphism is said to be an isomorphism if f is a bijection.

- If $f: G \to G'$ is an isomorphism, then so is f^{-1}.

Proof) Need to show that f^{-1} is a group homomorphism

So, $f^{-1}(g_1 g_2) = f^{-1}(g_1) f^{-1}(g_2)$

Since f is injective, there exist unique a_1, a_2 in G such that $f(a_1) = g_1$, $f(a_2) = g_2$

$$\Rightarrow f^{-1}(g_1 g_2) = f^{-1}(f(a_1) f(a_2))$$

$$f^{-1}(g_1 \cdot g_2) = f^{-1}(f(a_1, a_2)) = (a_1 \cdot a_2)$$

$$f^{-1}(g_1 \cdot g_2) = f^{-1}(g_1) f^{-1}(g_2)$$

Thus, a map $f: G \to G'$ is a group isomorphism if f is bijective and both f, f^{-1} are group homomorphisms.

Examples

(i) Any cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$

Let $G = \langle x \rangle$ where $|G| = \text{ord}(x) = n$

Define $f: G \to \mathbb{Z}/n\mathbb{Z}$

$$x^m \to \overline{m}$$

$$f(x^{m_1} x^{m_2}) = f(x^{\overline{m_1 + m_2}})$$

$$= \overline{m_1 + m_2}$$

$$= \overline{m_1} + \overline{m_2} = f(x^{m_1}) + f(x^{m_2})$$

Clearly f is surjective and one - one.

Thus, f is a bijection and hence a group isomorphism.

(ii) $\mathcal{G} = \{ G \mid G \text{ is a group} \}$

Define a relation $\simeq$ on $\mathcal{G}$

$G \simeq G' \iff$ there is an isomorphism $f : G \to G'$

Reflexive :- $Id : G \to G'$

Symmetric :- Bijection

To prove transitive, we use the following lemma

Lemma If $f : G_1 \to G_2$ and $g : G_2 \to G$ are group homomorphisms, then so is $g \circ f$

Let $x, y \in G_1$

$$g(f(x\,y)) = g(f(x)\,f(y))$$
$$= g\circ f(x)\ \ g\circ f(y)$$

$g \circ f$ is a homomorphism

Transitive : Follows from Lemma

Definition

Let G be a group and $f : G \to G$ be a group isomorphism. Then f is called an automorphism of the group G.

$\text{Aut}(G) = \{ f : G \to G \mid f \text{ is an automorphism} \}$

Lemma

$\text{Aut}(G)$ is a group under composition of maps

We prove that $\text{Aut}(G)$ is a subgroup of $\text{Bij}(G, G)$

- $\text{Aut}(G) \neq \emptyset$ as $id \in \text{Aut}(G)$
- $f, g \in \text{Aut}(G) \Rightarrow g \circ f \in \text{Aut}(G)$
- $g \in \text{Aut}(G) \Rightarrow g^{-1} \in \text{Aut}(G)$

Examples

(i) $f : \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ $\quad (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$

$x \longmapsto e^x$ is an isomorphism

(ii) Let G be a group and $a \in G$

Define $\gamma_a : G \longrightarrow G$

$g \longmapsto a g a^{-1}$

$$\gamma_a(g_1 g_2) = a g_1 g_2 a^{-1}$$
$$= (a g_1 a^{-1})(a g_2 a^{-1})$$
$$= \gamma_a(g_1)\, \gamma_a(g_2)$$

One – one : $\gamma_a(g_1) = \gamma_a(g_2)$

$$\Rightarrow a g_1 a^{-1} = a g_2 a^{-1}$$
$$\Rightarrow a^{-1} a g_1 a^{-1} a = a^{-1} a g_2 a^{-1} a$$
$$\Rightarrow g_1 = g_2$$

Onto :

For any $g \in G$, $\gamma_a(a^{-1} g a) = g$

$\Rightarrow \gamma_a$ is surjective

Thus γ_a is an automorphism of G.

It is also called an inner automorphism of G.

$$\mathrm{Inn}(G) = \{ \gamma_a : G \to G \}$$

(Exercise!)

Is $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$?

(iii) Let G be a group and $a \in G$. We define

$t_a : G \longrightarrow G$ (called left multiplication by a)

$g \longmapsto ag$

t_a is a bijection (Trivial!)

$\Rightarrow t_a \in S_a$

Let G be a group

We define $\phi : G \to S_G$

$a \mapsto t_a$

<u>Claim</u> : ϕ is a homomorphism

$\phi(ab) = \phi(a)\phi(b)$

$t_{ab}(x) = t_a \circ t_b(x)$

$abx = t_a(bx) = abx$

<u>Claim</u> : ϕ is injective

$\phi(a) = \phi(b)$

$\Rightarrow t_a = t_b$

$\Rightarrow a(e) = b(e)$

$\Rightarrow a = b$

Injective map :- $G \hookrightarrow S_G$

<u>Lemma</u>

If $\phi : G_1 \to G_2$ is a group homomorphism,

then $\phi(G_1) \leq G_2$

<u>Proof</u> :-

$\phi(e) \in G_2$ where e is identity of G_1

Lemma : If $\phi : G_1 \to G_2$ is a group homomorphism

Then (i) $\phi(e_{G_1}) = e_{G_2}$

(ii) $\phi(g^{-1}) = (\phi(g))^{-1}$

(i) $\phi(e_{G_1}) = \phi(e_{G_1} \cdot e_{G_1}) = \phi(e_{G_1})\phi(e_{G_1})$

$\Rightarrow \phi(e_{G_1}) = e_{G_2}$

(ii) $gg^{-1} = e_{G_1}$

$\phi(g)\phi(g^{-1}) = e_{G_2}$

$\phi(g^{-1}) = (\phi(g))^{-1}$

Now, we show inverse exists in $\phi(G_1)$ because

$(\phi(g))^{-1} = \phi(g^{-1})$ and $g^{-1} \in G_1$

Cayley's Theorem

Every group G is isomorphic to a subgroup of S_G.

In particular, if $|G| = n$ then $G \cong$ a subgroup of S_n

Definition

Let $\phi : G \to G'$ be a group homomorphism.

We define kernel of ϕ, denoted by $\ker \phi$

as $\ker(\phi) = \{ x \in G \mid \phi(x) = 1_{G'} \}$

Proposition

(i) $\ker(\phi) \leq G$

$\ker(\phi) \neq \phi$ ← null set

Since ϕ is a homomorphism $\phi(xy) = \phi(x)\,\phi(y)$

$= 1_{G'}$

If $x \in \ker(\phi)$, then $\phi(x^{-1}) = (\phi(x))^{-1}$

$= 1_{G'}^{-1} = 1_{G'}$

(ii) ϕ is injective $\iff \ker(\phi) = \{1_{G'}\}$

ϕ is injective $\Rightarrow \ker(\phi) = \{1_{G'}\}$

Let us assume that $\ker(\phi) = \{1_G\}$

$\phi(x) = \phi(y)$

$\phi(x)(\phi(y))^{-1} = 1_{G'}$

$\phi(x)\,\phi(y^{-1}) = 1_{G'}$

$\phi(xy^{-1}) = 1_{G'}$

$\Rightarrow xy^{-1} \in \ker(\phi)$

But $\ker(\phi) = \{1_G\}$

$\Rightarrow xy^{-1} = 1_G \Rightarrow \boxed{x = y}$