Lecture 22: group homomorphism.

Wednesday, November 26, 2014
9:13 AM

Exp. $\mathbb{Z} \longrightarrow \mathbb{Z}_n$; $H \hookrightarrow G$ if $H \leq G$

Proposition. $G \curvearrowright X \Rightarrow \rho: G \longrightarrow S_X$, $\rho(g)(x) := g \cdot x$

is a group homomorphism.

Def. Suppose $\phi: G_1 \longrightarrow G_2$ is a group homomorphism.

Image of ϕ $= \operatorname{Im}(\phi) := \{\phi(g) \mid g \in G_1\}$.

kernel of ϕ $= \ker(\phi) := \{g \in G_1 \mid \phi(g) = e\}$.

Basic Properties of a Homomorphism

① $\phi(e_{G_1}) = e_{G_2}$.

② $\phi(g^{-1}) = \phi(g)^{-1}$.

③ $\operatorname{Im}(\phi) \leq G_2$

④ $\ker(\phi) \leq G_1$

Pf. ① $\phi(e_{G_1}) = \phi(e_{G_1} \cdot e_{G_1}) = \phi(e_{G_1}) \cdot \phi(e_{G_1})$

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

② $e_{G_2} = \phi(e_{G_1}) = \phi(g \cdot g^{-1}) = \phi(g) \cdot \phi(g^{-1})$

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

③ $e_{G_2} = \phi(e_{G_1}) \in \mathrm{Im}(\phi) \neq \emptyset$.

$h_1, h_2 \in \mathrm{Im}(\phi) \Rightarrow \exists\, g_1, g_2 \in G_1,\ \phi(g_1) = h_1$ and $\phi(g_2) = h_2$

$$\Rightarrow h_1 \cdot h_2^{-1} = \phi(g_1)\,\phi(g_2)^{-1}$$

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

$$= \phi(g_1 g_2^{-1}) \in \mathrm{Im}(\phi)$$

④ $\phi(e_{G_1}) = e_{G_2} \Rightarrow e_{G_1} \in \ker\phi \neq \emptyset$.

$g_1, g_2 \in \ker\phi \Rightarrow \phi(g_1) = e = \phi(g_2)$.

$$\Rightarrow \quad \phi(g_1 \cdot g_2^{-1}) = \phi(g_1)\,\phi(g_2)^{-1}$$

$$= e \cdot e^{-1} = e.$$

$\Rightarrow g_1 \cdot g_2^{-1} \in \ker\phi$. □

Exp. $\ker(\mathrm{sgn}) = A_n$, where $\mathrm{sgn}: S_n \longrightarrow \{\pm 1\}$.

Exp. $\phi: \mathbb{Z}_{20} \longrightarrow \mathbb{Z}_{20}$, $\phi(x) = 15x$.

Find $\mathrm{Im}(\phi)$ and $\ker(\phi)$. In particular find their size.

Solution. $[y]_{20} \in \text{Im}\,\phi \iff \exists\, x \in \mathbb{Z},\ 15\,[x]_{20} = [y]_{20}$

$\iff \exists\, x \in \mathbb{Z},\ 15x \equiv y \pmod{20}$

$\iff \gcd(15, 20) \mid y$

$\iff 5 \mid y.$

$\Rightarrow \text{Im}(\phi) = 5\,\mathbb{Z}_{20} = \{[0]_{20}, [5]_{20}, [10]_{20}, [15]_{20}\}.$

$\Rightarrow |\text{Im}(\phi)| = 4$

$[x]_{20} \in \ker\phi \iff 15\,[x]_{20} = [0]_{20}$

$\iff 20 \mid 15x$

$\iff 4 \mid 3x$

$\iff 4 \mid x$ (as $\gcd(4,3)=1$)

$\Rightarrow \ker\phi = 4\,\mathbb{Z}_{20} = \{[0], [4], [8], [12], [16]\}.$

$\Rightarrow |\ker\phi| = 5.$ ∎

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

ϕ is 1-1 $\iff \ker(\phi) = \{e\}.$

Pf ($\Rightarrow$) $x \in \ker\phi \Rightarrow \phi(x) = e_H = \phi(e_G)$

$\Rightarrow x = e.$

{ϕ is 1-1}

$(\Leftarrow)$ $\phi(x_1) = \phi(x_2) \Rightarrow \phi(x_1)\phi(x_2)^{-1} = e_H$

$\Rightarrow \phi(x_1 x_2^{-1}) = e_H$

$\Rightarrow x_1 x_2^{-1} \in \ker\phi$

$\Rightarrow x_1 x_2^{-1} = e$

{$\ker\phi = \{e\}$} $\Rightarrow x_1 = x_2$. □

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

$\Rightarrow$ $\overline{\phi} : G/\ker\phi \longrightarrow \operatorname{Im}\phi$,

$\overline{\phi}(g \ker\phi) := \phi(g)$

is a well-defined bijection.

Pf. and **well-defined**: $g_1 \ker\phi = g_2 \ker\phi \iff g_1^{-1} g_2 \in \ker\phi$

1-1

$\iff \phi(g_1^{-1} g_2) = e$

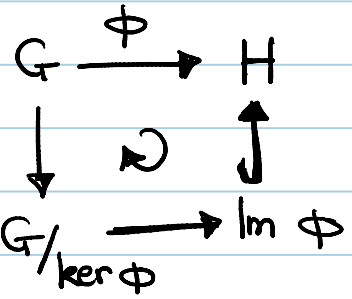
$\iff \phi(g_1)^{-1}\phi(g_2) = e$

$\iff \phi(g_1) = \phi(g_2)$.

Onto: It is clear from the definitions of $\operatorname{Im}(\phi)$

and $\overline{\phi}$. □

So any homomorphism ϕ induces a bijection $\overline{\phi}$ s.t. this diagram commutes.



Cor. If G is a finite group, and $\phi: G \to H$ is a group homomorphism, then

$$|G| = |\ker \phi| \, |\mathrm{Im}\, \phi| .$$

Pf: By the previous Proposition,

$$|G/\ker \phi| = |\mathrm{Im}\, \phi|$$

$\Rightarrow$ By Lagrange theorem,

$$|G|/|\ker \phi| = |\mathrm{Im}\, \phi|$$

$$\Rightarrow \quad |G| = |\ker \phi| \, |\mathrm{Im}\, \phi| . \qquad \blacksquare$$

Remark. Notice its similarity with the nullity theorem:

$$\dim V = \dim \ker T + \dim \mathrm{Im}\, T .$$

Can any subgroup be the image or the kernel of a homomorphism?

Can any subgroup be the image or the kernel of a homomorphism?

. $H \hookrightarrow G \mapsto H$ is the image of j

. Not any subgroup can be kernel of a homomorphism.

Main additional property.

$$g \in \ker\phi \Rightarrow \phi(g) = e$$

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

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

$$= e.$$

$$\Rightarrow g' g g'^{-1} \in \ker\phi$$

So $\ker\phi \subseteq g' \ker\phi\, g'^{-1}$ for any $g' \in G$

$\Rightarrow \ker\phi \subseteq g'^{-1} \ker\phi\, g'$

$\Rightarrow g' \ker\phi\, g'^{-1} \subseteq \ker\phi$

$\Rightarrow \ker\phi = g' \ker\phi\, g'^{-1}$ for any $g' \in G$.

Definition. A subgroup N of G is called a normal subgroup if $\forall g \in G$, $gNg^{-1} = N$

(or equiv. $gN = Ng$.)

Proposition. Suppose $N \triangleleft G$. Then $(G/N, \cdot)$,

$$g_1 N \cdot g_2 N := g_1 g_2 N$$

is a group.

Pf: *well-defined:* $\left.\begin{matrix} g_1 N = g_1' N \\ g_2 N = g_2' N \end{matrix}\right\} \overset{?}{\Longrightarrow} g_1 g_2 N = g_1' g_2' N$

$\left.\begin{matrix} g_1 N = g_1' N \Rightarrow g_1 = g_1' n_1 \\ g_2 N = g_2' N \Rightarrow g_2 = g_2' n_2 \end{matrix}\right\} \Rightarrow (g_1' g_2')^{-1}(g_1 g_2) =$

$g_2'^{-1} g_1'^{-1} g_1 g_2 =$

$g_2'^{-1} n_1 g_2 =$

$g_2'^{-1} n_1 g_2' g_2'^{-1} g_2 =$

$(g_2'^{-1} n_1 g_2') n_2 \in N.$

$\left.\begin{matrix} g_2'^{-1} n_1 g_2' \in g_2'^{-1} N g_2' = N \\ n_2 \in N \end{matrix}\right\}$ ⟹

Associativity: $(g_1 N \cdot g_2 N) \cdot g_3 N = (g_1 g_2) N \cdot g_3 N$

$= ((g_1 g_2) g_3) N$

$$g_1N \cdot (g_2N \cdot g_3N) = (g_1(g_2g_3))\,N$$

identity: $gN \cdot N = N \cdot gN = gN$

inverse: $g^{-1}N \cdot gN = N = gN \cdot g^{-1}N$. ∎

Proposition. Suppose $N \triangleleft G$. Then $\pi: G \to G/N$,

$$\pi(g) := gN$$

is an epimorphism and $\ker \pi = N$.

Pf. • $\pi(g_1g_2) = (g_1g_2)N = g_1N \cdot g_2N = \pi(g_1) \cdot \pi(g_2)$.

• $g \in \ker \pi \iff gN = N \iff g \in N$.

• Clearly it is onto. ∎

First Isomorphism Theorem Let $\phi: G \to H$ be a group homomorphism. Then $\overline{\phi}: G/\ker\phi \to \operatorname{Im}\phi$,

$$\overline{\phi}(g \ker \phi) = \phi(g)$$

is a group isomorphism.

Pf. We have already proved $\overline{\phi}$ is a well-defined bije.

So it is enough to show $\overline{\phi}$ is a group homomorphism

$$\overline{\Phi}(g_1 \ker\Phi \cdot g_2 \ker\Phi) = \overline{\Phi}(g_1 g_2 \ker\Phi)$$

$$= \Phi(g_1 g_2)$$

$$= \Phi(g_1)\,\Phi(g_2)$$

$$= \overline{\Phi}(g_1 \ker\Phi)\,\overline{\Phi}(g_2 \ker\Phi).$$

■