Lecture 23: group homomorphism

Monday, December 01, 2014
8:46 AM

Recall. $\phi: G \to H$ is called a group homomorphism

if $\phi(g_1 g_2) = \phi(g_1)\,\phi(g_2)$.

Basic Properties

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

  $o(\phi(g)) \mid o(g)$ if $o(g) < \infty$;
- $\mathrm{Im}(\phi) = \{\phi(g) \mid g \in G\} \leq H$.
- $\ker(\phi) = \{g \in G \mid \phi(g) = e\} \trianglelefteq G$
- $N \leq G$ is called a normal subgroup if

$$\forall g \in G, \qquad g N g^{-1} = N.$$

- $\mathrm{Im}\,\phi = H \iff \phi$ is an epimorphism

  $\ker \phi = \{e\} \iff \phi$ is a monomorphism

The main part of the argument was

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

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

$$\iff g_1^{-1} g_2 \in \ker \phi$$

$$\iff g_1 \ker\phi = g_2 \ker\phi .$$

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

Then
$$\overline{\Phi} : G/_{\ker\phi} \longrightarrow \operatorname{Im}\phi,$$
$$\overline{\Phi}(g \ker\phi) = \phi(g)$$

is a well-defined bijection.

Pf. The above argument shows that $\overline{\Phi}$ is well-defined and 1-1. And by the definitions of $\operatorname{Im}(\phi)$ and $\overline{\Phi}$ it is clear that $\overline{\Phi}$ is onto. ∎

Cor. Let G be a finite group, and $\phi : G \to H$ be a group homomorphism. Then

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

Pf. By the previous proposition, we have

$$\left|G/_{\ker\phi}\right| = |\operatorname{Im}\phi| .$$

By Lagrange theorem, $\left|G/_{\ker\phi}\right| = |G|/_{|\ker\phi|}$. ∎

Can any normal subgroup be kernel of a homomorphism?

$N \trianglelefteq G$. We'd like to find a group H and a group homomorphism $\phi: G \to H$ s.t. $N = \ker\phi$.

Since we can restrict ourselves to $\mathrm{Im}(\phi)$, w.l.o.g. we can look for an epimorphism: $H = \mathrm{Im}\,\phi$. So the above Proposition says that H can be identified with $G/_{\ker\phi} = G/_N$ as a set. Can we make $G/_N$ into a group in a "natural" way?

multiply two representatives of left cosets.

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

Proposition Let $N \trianglelefteq G$. Then $(g_1 N)\cdot(g_2 N) = g_1 g_2 N$ is a well-defined group operation. And

$$\pi: G \to G/_N \,, \quad \pi(g) := gN$$

$G/_N$ is called a factor group

is an onto group homomorphism and $\ker \pi = N$.

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

$$g_1N = g_1'N \Rightarrow g_1 = g_1' n_1$$

$$g_2N = g_2'N \Rightarrow g_2 = g_2' n_2$$

$$(g_1'g_2')^{-1}(g_1g_2) = g_2'^{-1} g_1'^{-1} g_1 g_2$$

$$= g_2'^{-1} g_1'^{-1} g_1' n_1 g_2' n_2$$

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

<u>associativity</u> $(g_1N \cdot g_2N) \cdot g_3N = (g_1g_2)N \cdot g_3N$

$$= ((g_1g_2)g_3)N$$

$$= (g_1(g_2g_3))N$$

$$= g_1N \cdot (g_2g_3)N$$

$$= g_1N \cdot (g_2N \cdot g_3N)$$

<u>identity</u> $N \cdot gN = gN \cdot N = gN$

<u>inverse</u> $gN \cdot g^{-1}N = g^{-1}N \cdot gN = N.$

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

$$g \in \ker \pi \iff \pi(g) = N$$

$$\iff gN = N$$

$$\iff g \in N. \quad \blacksquare$$

The First Isomorphism Theorem

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

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

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

is an isomorphism.

Pf. We already know that $\overline{\Phi}$ is a bijection. So it is enough to show it is a group homomorphism:

$$\begin{aligned}\overline{\Phi}(g_1\ker\phi \cdot g_2\ker\phi) &= \overline{\Phi}((g_1g_2)\ker\phi)\\ &= \phi(g_1g_2)\\ &= \phi(g_1)\,\phi(g_2)\\ &= \overline{\Phi}(g_1\ker\phi)\,\overline{\Phi}(g_2\ker\phi).\end{aligned}$$

■

Exp. $\mathbb{R}/_{\mathbb{Z}}$ is isomorphic to $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$.

Pf. $$\left.\begin{aligned}\mathbb{R} &\longrightarrow S^1\\ x &\longmapsto e^{2\pi i x}\end{aligned}\right\}$$ ϕ is an epimorphism

$\ker\phi = \mathbb{Z}$.

■

Exp. $\langle g\rangle$ is a finite group $\Rightarrow$ $\langle g\rangle \simeq \mathbb{Z}_{o(g)}$.

Pf. $\mathbb{Z} \to \langle g\rangle$

$n \mapsto g^n$

is a group homomorphism.

$\ker\phi = \{n\in\mathbb{Z} \mid g^n = e\}$

$= o(g)\mathbb{Z}$

$\Rightarrow \mathbb{Z}/_{o(g)\mathbb{Z}} \simeq \langle g\rangle$

$\Rightarrow \mathbb{Z}_{o(g)} \simeq \langle g\rangle$. ∎

Exp. $\mathbb{R}^\times/_{\{1,-1\}} \simeq \mathbb{R}^+$.

Pf. $x \mapsto x^2$

$\ker\phi = \{\pm 1\}$.

Exp. • $\mathbb{Z}\times\mathbb{Z}/_{\langle(0,1)\rangle} \simeq \mathbb{Z}$

$(x,y) \mapsto x$

Exp • $\mathbb{Z}\times\mathbb{Z}/_{\langle(1,1)\rangle} \simeq \mathbb{Z}$

$(x,y) \mapsto x-y$

Exp. • $\mathbb{Z}\times\mathbb{Z}/_{\langle(2,2)\rangle}$ is NOT cyclic.

Pf it is generated by $(a,b)+\langle(2,2)\rangle$.

$\Leftrightarrow \forall (x,y)\in\mathbb{Z}\times\mathbb{Z}\ \exists n\in\mathbb{Z}$ s.t.

$(x,y) \in n(a,b) + \langle (2,2) \rangle$

$\iff \exists\, n,m \in \mathbb{Z}$ s.t. $(x,y) = n(a,b) + m(2,2)$

$\iff \forall\, x,y \in \mathbb{Z}$, $\begin{bmatrix} a & 2 \\ b & 2 \end{bmatrix} \begin{bmatrix} n \\ m \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$

has an integer solution

$\iff$ $\begin{bmatrix} a & 2 \\ b & 2 \end{bmatrix}^{-1}$ exists and has integer entries

$\iff$ $\det \begin{bmatrix} a & 2 \\ b & 2 \end{bmatrix} = \pm 1 \implies 2a - 2b = \pm 1$

which is a contradiction.