Lecture 23: group homomorphism

Recall. \( \phi : G \to H \) is called a group homomorphism if
\[
\phi(g_1 g_2) = \phi(g_1) \phi(g_2).
\]

Basic Properties

- \( \phi(e) = e \); \( \phi(g^{-1}) = \phi(g)^{-1} \); \( \phi(g^n) = \phi(g)^n \);
- \( o(\phi(g)) | o(g) \) if \( o(g) < \infty \);
- \( \text{Im}(\phi) = \{ \phi(g) | g \in G \} \subseteq H \);
- \( \ker(\phi) = \{ g \in G | \phi(g) = e \} \subseteq G \);
- \( N \leq G \) is called a normal subgroup if
  \[
  \forall g \in G, \quad gNg^{-1} = N.
  \]
- \( \text{Im} \phi = H \iff \phi \) is an epimorphism
- \( \ker \phi = \{ e \} \iff \phi \) is a monomorphism

The main part of the argument was
\[
\phi(g_1 g_2) = e \iff \phi(g_1^{-1} g_2) = e
\]
\[
\iff \phi(g_1^{-1} g_2) = e
\]
\[ \iff g_1^{-1} g_2 \in \ker \phi \]
\[ \iff g_1 \ker \phi = g_2 \ker \phi. \]

**Proposition.** Let \( \phi : G \to H \) be a group homomorphism.

Then \( \overline{\phi} : G/\ker \phi \to \text{Im} \ \phi, \)
\[ \overline{\phi} (g \ker \phi) = \phi(g) \]
is a well-defined bijection.

**Proof.** The above argument shows that \( \overline{\phi} \) is well-defined and 1-1. And by the definitions of \( \text{Im}(\phi) \) 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
\[ |G| = |\ker \phi| |\text{Im} \ \phi|. \]

**Proof.** By the previous proposition, we have
\[ |G/\ker \phi| = |\text{Im} \ \phi|. \]
By Lagrange theorem,
\[ |G/\ker \phi| = \frac{|G|}{|\ker \phi|}. \]
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 \( \text{Im}(\phi) \), \( \omega \log \),
we can look for an epimorphism: \( H = \text{Im} \phi \). So the above Proposition says that \( H \) can be identified with \( G/\ker \phi \)

\( = \frac{G}{N} \) as a set. Can we make \( \frac{G}{N} \) into a group in a "natural" way?

\[(g_1N) \cdot (g_2N) := (g_1g_2)N\]

**Proposition** Let \( N \trianglelefteq G \). Then \( (g_1N) \cdot (g_2N) = (g_1g_2)N \)

is a well-defined group operation. And \( \pi : G \to \frac{G}{N}, \pi(g) := gN \)

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

**Pf.** \underline{well-defined.} \( g_1N = g_1'N \) \( \Rightarrow \) \( g_1g_2N = g_1'g_2N \)

\( g_2N = g_2'N \)
\[ g_1N = g_1'N \implies g_1 = g_1'n_1 \]
\[ g_2N = g_2'N \implies g_2 = g_2'n_2 \]
\[
(g_1'g_2')^{-1} (g_1g_2) = g_2'^{-1} g_1'^{-1} g_1 g_2 \\
= g_2'^{-1} g_1'^{-1} g_1' n_1 g_2 n_2 \\
= (g_2'^{-1} n_1 g_2') n_2 \in N.
\]

Associativity
\[
(g_1N \cdot g_2N) \cdot g_3N = (g_1g_2)N \cdot g_3N \\
= (g_1g_2g_3)N \\
= g_1N \cdot (g_2g_3)N \\
= g_1N \cdot (g_2N \cdot g_3N)
\]

Identity
\[ N \cdot gN = gN \cdot N = gN \]

Inverse
\[ gN \cdot g'^{-1}N = g'^{-1}N \cdot gN = N. \]

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

\[ q \in \ker \pi \iff \pi(q) = N \\
\iff gN = N \\
\iff g \in N. \]
The First Isomorphism Theorem

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

\[
\overline{\phi} : G / \ker \phi \to \text{Im} \phi,
\]

\[
\overline{\phi} (g \ker \phi) = \phi(g)
\]

is an isomorphism.

\[\begin{proof}
\text{We already know that } \overline{\phi} \text{ is a bijection. So it is enough to show it is a group homomorphism:}
\end{proof}\]

\[
\overline{\phi} (g_1 \ker \phi \cdot g_2 \ker \phi) = \overline{\phi} (g_1 g_2 \ker \phi)
\]

\[
= \phi(g_1 g_2)
\]

\[
= \phi(g_1) \phi(g_2)
\]

\[
= \overline{\phi} (g_1 \ker \phi) \overline{\phi} (g_2 \ker \phi).
\]

\[\square\]

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

\[\begin{proof}
\mathbb{R} \to S^1
\end{proof}\]

\[
\phi \text{ is an epimorphism}
\]

\[
\ker \phi = \mathbb{Z}.
\]
Exp. \( \langle g \rangle \) is a finite group \( \Rightarrow \) \( \langle g \rangle \cong \mathbb{Z}_{o(g)} \).

\[ \text{Pr.} \quad \mathbb{Z} \rightarrow \langle g \rangle \quad \text{ker } \phi = \{ n \in \mathbb{Z} \mid g^n = e \} = o(g) \mathbb{Z} \]

\( n \mapsto g^n \)

is a group homomorphism.

\[ \Rightarrow \mathbb{Z}/o(g) \mathbb{Z} \cong \langle g \rangle \]

\[ \Rightarrow \mathbb{Z}_{o(g)} \cong \langle g \rangle. \]

Exp. \( \mathbb{R}^{x} / \mathbb{Q}^{1,-1} \cong \mathbb{R}^{+} \).

\[ \text{Pr.} \quad x \mapsto x^2 \]

\( \text{ker } \phi = \mathbb{Q}^{\pm 1} \).

Exp. \( \mathbb{Z} \times \mathbb{Z} / \langle (0,1) \rangle \cong \mathbb{Z} \)

\( (x, y) \mapsto x \)

Exp. \( \mathbb{Z} \times \mathbb{Z} / \langle (1,1) \rangle \cong \mathbb{Z} \)

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

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

\[ \text{Pr.} \quad \text{it is generated by } (a,b) + \langle (2,2) \rangle. \]

\[ \Leftrightarrow \forall (x,y) \in \mathbb{Z} \times \mathbb{Z} \exists n \in \mathbb{Z} \text{ st.} \]
\[(x, y) \in n(a, b) + \langle (2, 2) \rangle\]

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

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

has an integer solution

\[\iff \begin{bmatrix} a & 2 \\ b & 2 \end{bmatrix}^{-1}\]

exists and has integer entries

\[\iff \det \begin{bmatrix} a & 2 \\ b & 2 \end{bmatrix} = \pm 1 \Rightarrow 2a - 2b = \pm 1\]

which is a contradiction.