Lecture 16

Homomorphisms

Definition 1: Homomorphism

Let $(G, *)$ and $(H, \cdot)$ be two groups. A map

$$f : G \to H$$

is called a *homomorphism* if for any elements $x, y \in G$ we have

$$f(x * y) = f(x) \cdot f(y).$$

If f is also bijective, we call it an *isomorphism*.

Example 1

- Let S_n be a permutation group, and $H = \{+1, -1\}$ be a group with respect to multiplication. Then *sign* of permutation defines a homomorphism

$$\mathrm{sgn}\colon S_n \to \{+1, -1\}.$$

  Indeed, sgn satisfies the key property:

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau).$$

- Consider $G = \mathbb{Z}_6$ and $H = \mathbb{Z}_3$. Define a map

$$f : \mathbb{Z}_6 \to \mathbb{Z}_3$$

  as follows. Take any integer x representing a congruence class in $\mathbb{Z}_6$. Then $a = (x \mod 3)$ represents a class in $\mathbb{Z}_3$. This gives a well-defined map $\mathbb{Z}_6 \to \mathbb{Z}_3$:

$$f(x) = (x \mod 3) \in \mathbb{Z}_3$$

  This map is an isomorphism, since

$$(x + y \mod 3) = (x \mod 3) + (y \mod 3).$$

- For any groups $(G, *)$ and $(H, \cdot)$ there is a trivial homomorphism:

$$f(x) = e_H$$

  for all $x \in G$, where $e_H \in H$ is the identity.

From now on, by default, we will use multiplication as the group operation.

Proposition 1

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

1. $f(e_G) = e_H$, where $e_G \in G$ and $e_H \in H$ are identities;
2. $f(x^{-1}) = f(x)^{-1}$, for any $x \in G$;
3. $\mathrm{Im}(f) \subset H$ is a subgroup.

Proof. 1. Let $a = f(e_G)$. By homomorphism property, we have

$$a = f(e_G) = f(e_G e_G) = f(e_G) f(e_G) = a^2.$$

Thus in H we have $a = a^2$, which implies $a = e_H$.

2. To prove that $f(x^{-1})$ is the inverse of $f(x) \in H$, we need to compute the product:

$$f(x^{-1})f(x) = f(x^{-1}x) = f(e_G) = e_H.$$

Thus $f(x^{-1})$ is the inverse of $f(x)$.
3. We need to verify two claims:

- Claim 1: for any $a, b \in \mathbb{Im}(f)$ we have $ab \in \mathbb{Im}(f)$. Indeed we know that there exists $x, y \in G$ such that

$$f(x) = a \quad f(y) = b.$$

  Thus $f(xy) = f(x)f(y) = ab$ implying that $ab \in \mathbb{Im}(f)$.

- Claim 2: for any $a \in \mathbb{Im}(f)$ we have $a^{-1} \in \mathbb{Im}(f)$. Indeed, if $a = f(x)$, then by part 2 of this proposition, $a^{-1} = f(x^{-1})$.

□

Definition 2: Kernel of a homomorphism

Let $f: G \to H$ be a homomorphism. A *kernel* of f

$$\mathrm{Ker}(f) \subset G$$

is the set

$$\mathrm{Ker}(f) = \{x \in G \mid f(x) = e_H\}.$$

Proposition 2

Kernel $\mathrm{Ker}(f) \subset G$ is a subgroup. Furthermore, it is a *normal* subgroup, meaning that for any $x \in \mathrm{Ker}(f)$ and any $g \in G$ we have

$$g^{-1}xg \in \mathrm{Ker}(f).$$

Proof. Let $x, y \in \mathrm{Ker}(f)$ be any two elements, i.e.,

$$f(x) = f(y) = e_H$$

Then

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

and

$$f(x^{-1}) = f(x)^{-1} = e_H.$$

This proves that $\mathrm{Ker}(f) \subset G$ is a subgroup. Now let us prove that $\mathrm{Ker}(f) \subset G$ is a normal subgroup. Indeed for any $x \in \mathrm{Ker}(f)$ and any $g \in G$ we have

$$f(g^{-1}xg) = f(g^{-1})\underbrace{f(x)}_{e_H}f(g) = f(g^{-1})f(g) = f(\underbrace{g^{-1}g}_{e_G}) = e_H.$$

Thus by definition $f^{-1}xg \in \mathrm{Ker}(f)$. □

Problem 1: Give an example of a group G and its subgroup $H \subset G$ which is not normal.

Example 2: Alternating group

Let $\mathrm{sgn}: S_n \to \{+1, -1\}$ be the sign homomorphism. Then $\mathrm{Ker}(\mathrm{sgn}) \subset S_n$ is the set of all *even permutations*, and by the above it forms a normal subgroup of S_n.
This group has a special name: *alternating group* ans is often denoted as

$$A_n := \mathrm{Ker}(\mathrm{sgn}).$$

Proposition 3

$|A_n| = n!/2$.

Proof. Since $|S_n| = n!$ and $S_n = \{\text{even permutations}\} \cup \{\text{odd permutations}\}$, it is enough to prove that

$$|\{\text{even permutations}\}| = |\{\text{odd permutations}\}|.$$

To this end we construct a bijection

$$f =: \{\text{even permutations}\} \to \{\text{odd permutations}\}.$$

We first define $F\colon S_n \to S_n$

$$F(\sigma) = (1,2)\sigma.$$

Since every transposition is odd, for σ even, $F(\sigma)$ is odd, and vice versa — for σ odd, $F(\sigma)$ is even. Finally $F \circ F = \mathrm{i}d_{S_n}$, i.e., F is its own inverse. Thus if we restrict F only on the subset {even permutations}, we will get a bijection between even and odd permutations. □