Homomorphisms and Isomorphisms

(Section 2.4)

Recall: (isomorphisms) If G and H are groups, $\varphi : G \to H$ is an isomorphism if φ is bijective and

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

$$\forall \; x, y \in G.$$

Up to isomorphism, we classified all cyclic groups as isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}_n$ ($n \in \mathbb{N}, n \geq 2$) or $\{e\}$.

Cyclic groups are determined by a single generator. Finite dihedral groups are determined by two "generators" R, J.

We say a subset S of a group G **generates** G if

$$\langle S \rangle = G.$$

Problem: Classify all groups, up to isomorphism, using generators!

Can we even do this for groups with 2 generators?

A more general notion than isomorphism will be helpful!

Definition: (homomorphism) Let G and H be groups. We say $\varphi: G \to H$ is a (group) **homomorphism** if

$$\boxed{\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)}$$

$\forall\ x, y \in G$.

Example 1: ($\mathbb{Z}$ to $\mathbb{Z}_2$)

Define $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ by

$$\varphi(n) = [n]_2$$

Then since we know

$$[n]+[m] = [n+m] \quad \forall\, n,m \in \mathbb{Z}$$

and for any modulus,

$$\varphi(n+m) = [n+m]_2$$

$$= [n]_2 + [m]_2$$

$$= \varphi(n) + \varphi(m)$$

So φ is a homomorphism!

However, since $\mathbb{Z}_2$ has finite cardinality but $\mathbb{Z}$ does not, φ is not an isomorphism.

Example 3: (determinants)

Define

$$\varphi : GL_2(\mathbb{R}) \to \mathbb{R}^\times$$ (units of $\mathbb{R}$ $= \mathbb{R} \setminus \{0\}$)

$$\varphi(A) = \det(A).$$

Then since we know

$$\det(A \cdot B) = \det(A) \cdot \det(B),$$

$$\begin{aligned} \varphi(A \cdot B) &= \det(A \cdot B) \\ &= \det(A) \cdot \det(B) \\ &= \varphi(A) \cdot \varphi(B) \end{aligned}$$

so φ is a homomorphism!

However, φ is not an isomorphism. φ is surjective

$$\left(\text{if } x \in \mathbb{R}^\times, \ \det \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} = x \right)$$

but not injective, since

$$2 = \varphi\left(\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \right) = \varphi\left(\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \right)$$

but $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$

Example 3: (identity and trivial homomorphisms)

If G is any group, G admits two homomorphisms from G to itself.

1) Identity homomorphism:

$$\varphi(x) = x \quad \forall \ x \in G$$

2) Trivial homomorphism:

$$\varphi(x) = e \quad \forall \ x \in G$$

Here, $\forall \ x, y \in G$,

$$\varphi(x) \cdot \varphi(y) = e \cdot e = e = \varphi(x \cdot y).$$

Definition: (endomorphism, automorphism)

Let G be any group. An **endomorphism** is a homomorphism from G to itself. An **automorphism** is a bijective endomorphism (an isomorphism from G to itself).

If every nontrivial endomorphism of G is an automorphism, we say that G is **simple**.