Isomorphisms and Homomorphisms

23 July 2019

Jonathan Alcaraz

We've alluded to the idea of two groups being "the same." You might remember these two group tables being the same:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Here we want to formalize this idea.

Definition

An **isomorphism** from a group $(G, \cdot)$ to $(H, \star)$ is a bijection $f : G \to H$ such that

$$f(a \cdot b) = f(a) \star f(b)$$

We say a group G is **isomorphic** to a group H if there exists an isomorphism $G \to H$. We write $G \cong H$.

Tying together some examples we saw last week:

Example

Recall the examples we discussed last week: the set $S = \{1, i, -1, -i\}$ with complex multiplication and $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with the modular addition $+_4$ we described last week. Consider the map:

$$\begin{aligned} \varphi : \mathbb{Z}_4 &\to S \\ k &\mapsto i^k \end{aligned}$$

We claim that φ is an isomorphism.

Step 1: φ is a bijection. We *could* try to prove this by proving injectivity and surjectivity

abstractly, but with these small finite groups, we can show it by hand.

$$\begin{aligned} 0 &\mapsto i^0 = 1 \\ 1 &\mapsto i^1 = i \\ 2 &\mapsto i^2 = -1 \\ 3 &\mapsto i^3 = -i \end{aligned}$$

Step 2: $\varphi(a+b) = \varphi(a)\varphi(b)$. Indeed

$$\varphi(a+b) = i^{a+b} = i^a\, i^b = \varphi(a)\varphi(b)$$

On day 1, we introduced **sets** and **functions**. Since then we put structure on sets and studied that structure. Now we want to talk about functions which preserve this structure.

Definition
Given groups $(G, \cdot)$ and $(H, \star)$, a function $f : G \to H$ is called a **group homomorphism** if

$$f(a \cdot b) = f(a) \star f(b)$$

for all $a, b \in G$.

Let's see an example.

Example

Example Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 2n$. This is indeed a homomorphism because

$$f(m+n) = 2(m+n) = 2m + 2n = f(m) + f(n)$$

Claim 1: Prove that the image of the identity element under any homomorphism is the identity.

> Let $f : G \to H$ be a group homomorphism with $e_G \in G$ and $e_H \in H$ denote the respective identity elements. Then
>
> $$f(e_G) = f(e_G e_G) = f(e_G)\, f(e_G)$$
>
> By multiplying both sides by the inverse of $f(e_G)$.
>
> $$\begin{aligned} f(e_G)^{-1} f(e_G) &= f(e_G)^{-1} f(e_G)\, f(e_G) \\ e_H &= f(e_G) \end{aligned}$$

Claim 2: Prove that the image of inverse elements under any homomorphism are inverse elements.

Let $f : G \to H$ be a group homomorphism and $g \in G$. We want to show that $f(g)^{-1} = f(g^{-1})$. Indeed,

$$f(g)f(g^{-1}) = f(g\,g^{-1}) = f(e_G) = e_H$$

and

$$f(g^{-1})f(g) = f(g^{-1}\,g) = f(e_G) = e_H$$

Here are some cool subgroups we get from a homomorphism.

Definition

Given a homomorphism $f : G \to H$ we define the **kernel** of f to be the set

$$\ker(f) = \{g \in G \,:\, f(g) = e_H\}$$