

## What do isomorphisms do?

I keep saying that **isomorphisms respect algebraic structure**. This is a hugely-encompassing idea and I want to unpack what I mean and what some of the consequences are.

### What is an isomorphism?

An isomorphism is a homomorphism that is also a bijection.

### Okay, smartass, what is a homomorphism?

Suppose that  $(G, \star)$  and  $(H, \odot)$  are two groups. Then  $\phi : G \rightarrow H$  is a homomorphism if

$$\phi(g_1 \star g_2) = \phi(g_1) \odot \phi(g_2).$$

**Exercise.** Circle three different things in that equation that are elements of  $H$ .

Morally what this means is that **a homomorphism is a function that respects the groups' operations**.

Another good maxim here is that **a homomorphism sends products to products**.

As a consequence of respecting the groups' **operations**, a homomorphism respects the groups' **algebraic structures**. Specifically:

**Exercise.** Prove each of the following statements:

- A homomorphism sends the identity to the identity.

*Proof.* Say that  $e_G$  is the identity in  $G$  and  $e_H$  is the identity in  $H$ . Consider  $\phi(e_G \star g)$ . On the one hand, since  $e_G \star g = g$ ,  $\phi(e_G \star g) = \phi(g)$ . On the other hand, using the homomorphism property,  $\phi(e_G \star g) = \phi(e_G) \odot \phi(g)$ . Therefore,

$$\phi(g) = \phi(e_G) \odot \phi(g).$$

Well,  $\phi(g)$  is some element of  $H$ , so it has an inverse. Let's  $H$ -multiply both sides of this equation by the inverse on the right:

$$\begin{aligned} \phi(g) \odot [\phi(g)]^{-1} &= \phi(e_G) \odot \phi(g) \odot [\phi(g)]^{-1} \\ e_H &= \phi(e_G) \odot \left( \phi(g) \odot [\phi(g)]^{-1} \right) \\ e_H &= \phi(e_G) \odot e_H \\ e_H &= \phi(e_G). \end{aligned}$$

So:  $\phi$  sends  $e_G$  to  $e_H$ . □

- A homomorphism sends inverses to inverses.
- A homomorphism sends  $G$  to a subgroup of  $H$ . (Vocabulary: the **image** of  $G$  under  $\phi$  is the set  $\text{im}(\phi) = \{\phi(g) \mid g \in G\}$ . Certainly this is a *subset* of  $H$ , but is it a *subgroup* of  $H$ ?)

- A homomorphism sends powers to powers.
- A homomorphism sends orbits to orbits.
- A homomorphism sends conjugates to conjugates.
- A homomorphism sends conjugacy classes to conjugacy classes.

Here are some examples of homomorphisms.

**Exercise.** Prove that each of these “sends products to products”:

- Squish everything in  $G$  down to the identity in  $H$ . (This is a rude homomorphism.)
  - Ponder: How does this map send orbits to orbits?
- Do nothing. (Define the “identity map”  $\text{id} : G \rightarrow G$  as  $\text{id}(g) = g$ .)
- If  $G \leq H$ , define the “inclusion map”  $\iota : G \rightarrow H$  as  $\iota(g) = g$ .
- Define the “exponential map”  $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, *)$  by  $\exp(x) = e^x$ .
- $\ln : (\mathbb{R}^+, *) \rightarrow (\mathbb{R}, +)$ .
  - This is, like, the best explanation for why the properties of logs are like that.
- Here is an interesting **non**-example: Let  $s : D_n \rightarrow D_n$  be the “squaring map”  $s(x) = x^2$ . (Hint: Remember that  $D_n$  isn’t abelian and compare  $s(fr)$  to  $s(f)s(r)$ .)
- If  $G$  is an **abelian** group, then the squaring map  $s : G \rightarrow G$  is indeed a homomorphism.
- Define  $\phi : Q_8 \rightarrow V_4$  as follows:  $\phi(\pm 1) = 1$ ,  $\phi(\pm i) = a$ ,  $\phi(\pm j) = b$ ,  $\phi(\pm k) = ab$ .
- Define the “projection map”  $\pi_A : A \times B \rightarrow A$  as  $\pi_A(a, b) = a$ . (Similar for  $\pi_B$ .)

## What about isomorphisms?

Okay, so to return to the top of this document, an isomorphism is a homomorphism that is also a bijection.

**Question.** Which of the example homomorphisms in the previous section are isomorphisms?

A general theme in math is that if you make something more special, you get stronger results. By adding “bijection” to “homomorphism,” you can thus expect to preserve even more structure.

**Exercise.** Let  $\phi : G \rightarrow H$  be an isomorphism. Prove that:

- $|\phi(g)| = |g|$ . (“ $\phi$  preserves orders.”)

*Proof.* Say that  $|g| = n$  – that is,  $g^n = e$ , but for any  $k < n$ ,  $g^k \neq e$ . We need to show those two things are also true for  $\phi(g)$ . The first part is easy: since  $\phi$  is a homomorphism, it sends powers to powers and the identity to the identity, so  $\phi(g)^n = \phi(g^n) = \phi(e) = e$ .

For the second part, consider the orbit of  $g$ ,  $\langle g \rangle = \{g, g^2, \dots, g^{n-1}, g^n = e\}$ . All these powers of  $g$  are distinct. (Why?) So, since  $\phi$  is a bijection (and in particular is 1-1), all their images  $\{\phi(g), \phi(g^2), \dots, \phi(g^{n-1}), \phi(g^n) = e\}$  are distinct. But since  $\phi$  sends powers to powers, that list of distinct elements is  $\{\phi(g), \phi(g)^2, \dots, \phi(g)^{n-1}, e\}$ . Therefore,  $\phi(g)^k \neq e$  for any  $k < n$  –  $e$  is in that list of distinct elements at the end, so nobody else gets to be  $e$ .  $\square$

- Corollary:  $\phi$  sends orbits to orbits *of the same size*.
- $\phi$  sends conjugacy classes to conjugacy classes *of the same size*.
- $\phi$  sends subgroups to subgroups *of the same size*.

If there is an isomorphism  $\phi : G \rightarrow H$ , we say that  $G$  and  $H$  are **isomorphic** and write  $G \cong H$ . Since an isomorphism  $\phi$  preserves *so much* algebraic structure, this is why it's our formal version of the idea that  $G$  and  $H$  are “basically the same” but maybe just got relabeled or re-presented.

**Exercise.** Suppose that  $G \cong H$ . Prove that:

- $G$  is abelian if and only if  $H$  is abelian.
- $|G| = |H|$ .

## Automorphisms

Certainly every group is isomorphic to itself. There's an obvious way to do this, but there may be more interesting ways as well. These are called **automorphisms**.

**Definition.** An **automorphism** is a map  $\phi : G \rightarrow G$  that is an isomorphism, ie., a bijective homomorphism.

**Examples.** Prove that each of these are automorphisms.

- The identity homomorphism is an automorphism.
- The complex-conjugate map  $\bar{\phantom{x}} : \mathbb{C} \rightarrow \mathbb{C}$  given by  $\overline{a + bi} = a - bi$  is an automorphism.

*Proof.* We need to check three things:

- First, that  $\bar{\phantom{x}}$  is a homomorphism:  $\overline{(a + bi)(c + di)} = \overline{a + bi} \cdot \overline{c + di}$ . Do some tedious complex-numbers multiplication to check that the thing on the left is indeed the same as the thing on the right. (They both end up being  $(ac - bd) - (ad - bc)i$ .)
- Second, that  $\bar{\phantom{x}}$  is injective (aka 1-1): Suppose that  $\overline{a + bi} = \overline{c + di}$ . Well, then  $a - bi = c - di$ . Equating real and imaginary parts, we see that  $a = c$  and  $-b = -d$ . Okay, so  $b = d$ . Therefore  $a + bi = c + di$ .

- Lastly, that  $\bar{\phantom{x}}$  is surjective (aka onto): Pick a generic complex number  $a + bi$ . Well, that's  $\overline{a - bi}$ , so yay.

(Aside: these properties are just as easy to check, and maybe even easier, if you write your complex numbers in polar form  $re^{i\theta}$ .)  $\square$

- We shall allow ourselves a moment of brief annoyance that the word “conjugation” means something different in different contexts, and now that we’ve gotten that out of our system: Pick a fixed element  $g \in G$ . The “ $g$ -conjugation map”  $\phi_g : G \rightarrow G$  given by  $\phi_g(h) = ghg^{-1}$  is an automorphism.
- Let’s say that  $G$  is an abelian group, so the squaring map  $s(g) = g^2$  (which I might also write as  $g \mapsto g^2$ ) is a homomorphism. Is it an automorphism? Prove that it is, or give an example where it’s not.
- Is the squaring map an automorphism of  $C_2$ ?  $C_3$ ?  $C_4$ ?
- The  $k$ -power map  $g \mapsto g^k$  is an automorphism of  $C_n$  **iff**  $n$  and  $k$  are relatively prime.