

Isomorphisms!

(but first, homomorphisms!)

Spencer Bagley

With many thanks to Matthew Macauley,
<http://www.math.clemson.edu/~macaule/>

10 Mar 2025

Goals for today:

1. We have sure said the word “isomorphic” a lot
2. Let's figure out what that **actually** means
3. Lots of examples
4. Some problems to play with

Definition and notation time!

Functions!

Nothing on this slide is specific to abstract algebra.

Extremely technical definition

Let A, B be two **sets**. A **function** f is a subset of the Cartesian product $A \times B$ such that:

- for all $a \in A$, there exists $b \in B$ such that $(a, b) \in f$ *(existence of images)*
- if $(a, b) \in f$ and $(a, b') \in f$, then $b = b'$ *(uniqueness of images)*

This definition sucks and I hate it.

Less technical but more useful definition

Let A, B be two sets. A function f is a **map** from A to B such that:

- for all $a \in A$, there exists $b \in B$ such that $f(a) = b$ *(existence of images)*
- if $f(a) = b$ and $f(a) = b'$, then $b = b'$ *(uniqueness of images)*

(Just don't ask me to formally explain what a “map” is.)

Moral definition

- f sends elements of A (inputs) to elements of B (outputs) *(existence of images)*
- and it does so **reproducibly**: the same input always gets sent to the same output. *(uniqueness of images)*

Notation and vocabulary!

Again, nothing on this slide is specific to abstract algebra.

Notation

- To say f is a function **from** A **to** B , we write $f : A \rightarrow B$ or $A \xrightarrow{f} B$
 - (We are specifying the sets that f plays with)
- To denote that $f(a) = b$, we also write $f : a \mapsto b$
 - or maybe even $a \mapsto b$ if it's clear what function we're talking about
 - (We are specifying the *elements* that f plays with)

Definitions

Let $f : A \rightarrow B$.

- The set A is called the **domain** of f .
- The set B is called the **codomain** of f .
- The **image** (or range) of f is the set of all actual outputs:

$$\text{Im}(f) := \{b \in B \mid f(a) = b \text{ for some } a \in A\}.$$

“Isomorphic”

We can finally say what it means for two groups to be “isomorphic”!

Definition

Let G, H be groups. G is **isomorphic** to H ($G \cong H$) if there exists an **isomorphism** $\phi : G \rightarrow H$.

Okay, smartass, what’s an isomorphism?

Let G, H be groups. An **isomorphism** $\phi : G \rightarrow H$ is a **bijective homomorphism**.

Istg if you don’t tell me right now what a homomorphism is –

A **homomorphism** is a **structure-preserving** function between groups.

Homomorphisms!

Homomorphisms are structure-preserving functions

Since groups aren't just sets, they deserve maps that aren't just functions.

Formal definition

Let (G, \star) and (H, \odot) be two groups. A **homomorphism** is a function $\phi : G \rightarrow H$ that **respects the operations**:

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

Hey, c'mere

- Circle everything in that definition that is an element of G .
- Box everything in that definition that is an element of H .

Why this?

A common theme in various maths is that we study **objects** and then **maps between objects**.

When the **objects** are special in some way, we want the **maps** to be nice to that specialness.

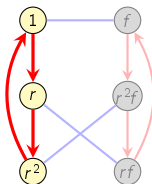
Example: in topology, we study **open sets**, so we use **continuous functions** because they are nice to open sets.

Morally:

- Homomorphisms **preserve structure** – specifically, the structure of a group.
- Homomorphisms **respect group operations**.
- Homomorphisms **send products to products**.

An example homomorphism

Here is D_3 but I'm highlighting a subgroup that “looks like” \mathbb{Z}_3 :



This can be formalized by a homomorphism $\phi: \mathbb{Z}_3 \rightarrow D_3$, defined by $\phi: n \mapsto r^n$.

Let's check that ϕ meets the definition of being a homomorphism,

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

What is the operation in \mathbb{Z}_3 ? in D_3 ?

$$\phi(n_1 + n_2) = r^{n_1+n_2} = r^{n_1} \cdot r^{n_2} = \phi(n_1) \cdot r^{n_2} = \phi(n_1) \cdot \phi(n_2)$$

Some more fun examples

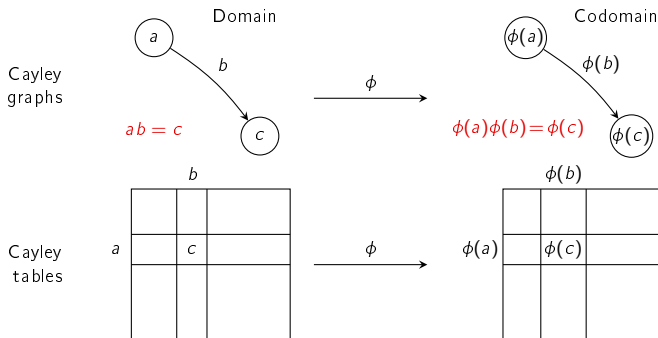
- Define a map $G \rightarrow H$ that just squishes everything down to the identity in H .
- Define the “exponential map” $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, *)$ by $\exp(x) = e^x$.
(\mathbb{R}^* means $\mathbb{R} - \{0\}$.)
- $\ln : (\mathbb{R}^+, *) \rightarrow (\mathbb{R}, +)$.
- The domain and the codomain can be the same:
consider the “squaring map” $s : C_6 \rightarrow C_6$ defined by $s : g \mapsto g^2$.
- What about the same squaring map, but in D_4 ?

Important caveat:

Not every function between groups is a homomorphism!

Preserving structure

The $\phi(ab) = \phi(a)\phi(b)$ condition has visual interpretations on the level of Cayley graphs and Cayley tables.



Note that in the Cayley graphs, b and $\phi(b)$ are **paths**; they need not just be edges.

An example

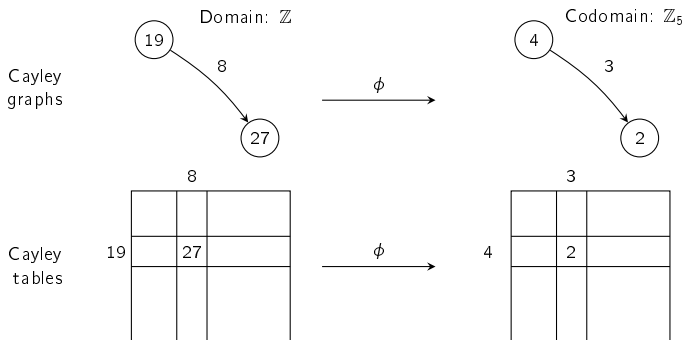
Consider the function ϕ that reduces an integer modulo 5:

$$\phi: \mathbb{Z} \longrightarrow \mathbb{Z}_5, \quad \phi(n) = n \pmod{5}.$$

Since the group operation is **additive**, the “homomorphism property” becomes

$$\phi(a + b) = \phi(a) + \phi(b).$$

In plain English, this just says that one can “first add and then reduce modulo 5,” OR “first reduce modulo 5 and then add.”



Properties of homomorphisms!

Some basic properties of homomorphisms

Proposition

For any homomorphism $\phi: G \rightarrow H$:

- (i) “ ϕ sends the identity to the identity”
- (ii) “ ϕ sends inverses to inverses”
- (iii) “ ϕ sends powers to powers”
- (iv) “ ϕ sends orbits to orbits”
- (v) “ ϕ sends conjugates to conjugates”
- (vi) “ ϕ is determined by what it does to generators”

$$\phi(1_G) = 1_H$$

$$\phi(g^{-1}) = \phi(g)^{-1}$$

What other properties along these lines can you conjecture?

Homework

If $|g|$ is finite, then $|\phi(g)|$ must divide $|g|$.

A word of caution

Just because a homomorphism $\phi: G \rightarrow H$ is determined by the image of its generators does *not* mean that every such image will work.

For example, let's try to define a homomorphism $\phi: \mathbb{Z}_3 \rightarrow \mathbb{Z}_4$ by $\phi(1) = 1$. Then we get

$$\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 2,$$

$$\phi(0) = \phi(1 + 1 + 1) = \phi(1) + \phi(1) + \phi(1) = 3 \neq 0.$$

This is *impossible*, because $\phi(0)$ must be $0 \in \mathbb{Z}_4$.

That's not to say that there isn't a homomorphism $\phi: \mathbb{Z}_3 \rightarrow \mathbb{Z}_4$; note that there is always the **trivial homomorphism** between two groups:

$$\phi: G \longrightarrow H, \quad \phi(g) = 1_H \quad \text{for all } g \in G.$$

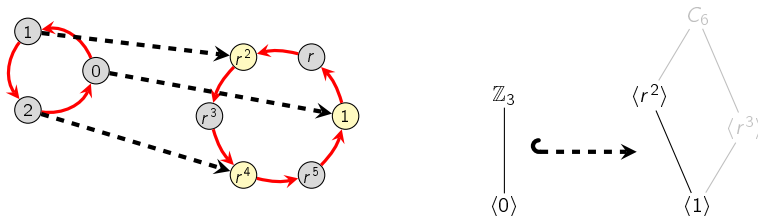
Exercise

Show that there is no **embedding** $\phi: \mathbb{Z}_n \hookrightarrow \mathbb{Z}$, for $n \geq 2$. That is, *any* such homomorphism must satisfy $\phi(1) = 0$.

Types of homomorphisms!

Injective homomorphisms aka embeddings

Consider the following homomorphism $\theta: \mathbb{Z}_3 \rightarrow C_6$, defined by $\theta(n) = r^{2n}$:



Note that $\theta(a + b) = \theta(a)\theta(b)$. The red arrow in \mathbb{Z}_3 gets mapped to the 2-step path in C_6 .

A homomorphism $\phi: G \rightarrow H$ that is **one-to-one** or **injective** is an **embedding**: the group G “embeds” into H as a subgroup. **Optional**: write $\phi: G \hookrightarrow H$.

Formally:

A homomorphism $\phi: G \rightarrow H$ is **1-1** or **injective** if “every output comes from only one input”:

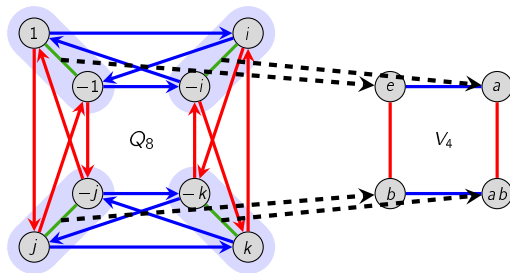
$$\text{if } \phi(g_1) = \phi(g_2), \text{ then } g_1 = g_2.$$

“If two outputs are the same, then actually the two inputs were the same.”

Surjective homomorphisms

Consider the homomorphism $\alpha : Q_8 \rightarrow V_4 = \langle a, b \rangle$, defined by $\alpha(i) = a$ and $\alpha(j) = b$.

Where does α send everything else in Q_8 ?



If $\phi(G) = H$ (“the image of ϕ is the entire codomain”), then ϕ is **onto**, or **surjective**.

We call ϕ a **quotient map** (yes, it’s related!). **Optional:** write $\phi: G \twoheadrightarrow H$.

Formal definition

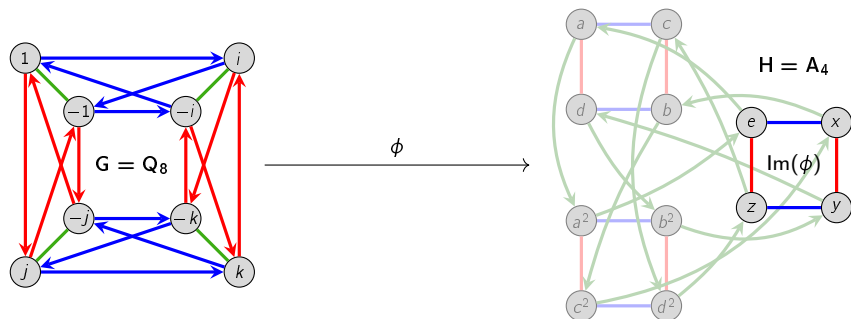
The homomorphism $\phi : G \rightarrow H$ is **onto**, or **surjective**, if for all $h \in H$, there is some $g \in G$ such that $\phi(g) = h$.

An example that is neither an embedding nor a quotient

Consider the homomorphism $\phi: Q_8 \rightarrow A_4$ defined by

$$\phi(i) = (12)(34), \quad \phi(j) = (13)(24).$$

Using the property of homomorphisms, compute ϕ of every other element of Q_8 .



Isomorphisms and automorphisms

Note that the words **injective** and **surjective** aren't only used in abstract algebra.

Definition

If a function is both **injective** and **surjective**, then it is called **bijective** (or a **bijection**).

Okay, smartass, what's an isomorphism?

Let G, H be groups. An **isomorphism** $\phi : G \rightarrow H$ is a **bijective homomorphism**.

G is **isomorphic** to H , written $G \cong H$, if there is an isomorphism between G and H .

Definition

An **automorphism** is an isomorphism from a group to itself.

An example of an isomorphism

We have already seen that D_3 is isomorphic to S_3 .

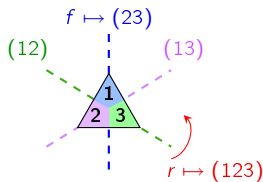
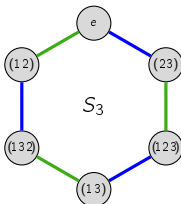
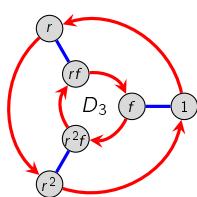
This means that there's a bijective correspondence $f: D_3 \rightarrow S_3$.

But not just any bijection will do. Intuitively (but also for order reasons),

- (123) and (132) should be the rotations
- (12) , (13) , and (23) should be the reflections
- The identity permutation must be the identity symmetry.

It is easy to verify that the following is an isomorphism:

$$\phi: D_3 \longrightarrow S_3, \quad \phi(r) = (123), \quad \phi(f) = (23).$$



However, there are other isomorphisms between these groups.

Kernels!

Definition

Let $\phi : G \rightarrow H$. The **kernel** of ϕ is “everybody who gets squished down to the identity.”

$$\ker(\phi) := \{x \in G \mid \phi(x) = 1\}.$$

(I am just going to quickly say the word “**nullspace**” from linear algebra.)

Properties of the kernel

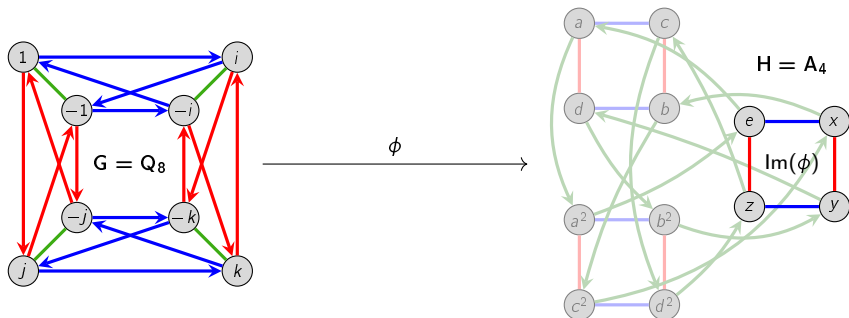
- (i) $\ker(\phi) \leq G$.
- (ii) In fact, $\ker(\phi) \trianglelefteq G$!
- (iii) $\ker(\phi)$ is trivial **iff** ϕ is injective.

Example: Find the kernel!

Consider the homomorphism $\phi: Q_8 \rightarrow A_4$ defined by

$$\phi(i) = (12)(34), \quad \phi(j) = (13)(24).$$

Who all is in $\ker \phi$?



Preimages

Here's a slightly more general version of the idea of the kernel:

Definition

Let $\phi : G \rightarrow H$ and choose a fixed element $h \in H$.

The **preimage** of h is “everybody who gets sent to h .”

$$\phi^{-1}(h) := \{g \in G \mid \phi(g) = h\}.$$

Alternative names: **fiber** above h , **pullback** of h

Let's go back and look at our example again.

A word of caution:

ϕ^{-1} is in general not a function! (Unless. . .)

Theorem (homework)

- (i) The kernel of ϕ is the fiber above 1.
- (ii) For every element $h \in H$, the fiber above h is a coset of $\ker(\phi)$.

An example of a quotient

Let's write $C_2 = \langle -1 \rangle = \{1, -1\}$. Consider the following quotient map:

$$\phi: D_4 \longrightarrow C_2, \quad \text{defined by } \phi(r) = 1 \text{ and } \phi(f) = -1.$$

(Check: Is this a homomorphism?) Note that:

$$\phi(r^k) = \phi(r)^k = 1^k = 1, \quad \phi(r^k f) = \phi(r^k)\phi(f) = \phi(r)^k \phi(f) = 1^k(-1) = -1.$$

	1	r	r ²	r ³	f	rf	r ² f	r ³ f
1	1	r	r ²	r ³	f	rf	r ² f	r ³ f
r	r	r ²	r ³	1	rf	r ² f	r ³ f	f
r ²	r ²	r ³	1	r	r ² f	r ³ f	f	rf
r ³	r ³	1	r	r ²	r ³ f	f	rf	r ² f
f	f	r ³ f	r ² f	rf	1	r ³	r ²	r
rf	rf	f	r ³ f	r ² f	r	1	r ³	r ²
r ² f	r ² f	rf	f	r ³ f	r ²	r	1	r ³
r ³ f	r ³ f	r ² f	rf	f	r ³	r ²	r	1

	1	r	r ²	r ³	f	rf	r ² f	r ³ f
1	1	r	r ²	r ³	f	rf	r ² f	r ³ f
r	r	r ²	r ³	1	rf	r ² f	r ³ f	f
r ²	r ²	r ³	1	r	r ² f	r ³ f	f	rf
r ³	r ³	1	r	r ²	r ³ f	f	rf	r ² f
f	f	r ³ f	r ² f	rf	1	r ³	r ²	r
rf	rf	f	r ³ f	r ² f	r	1	r ³	r ²
r ² f	r ² f	rf	f	r ³ f	r ²	r	1	r ³
r ³ f	r ³ f	r ² f	rf	f	r ³	r ²	r	1

$$\text{Ker}(\phi) = \phi^{-1}(1) = \langle r \rangle \quad (\text{"rotations"}),$$

$$\phi^{-1}(-1) = f \langle r \rangle \quad (\text{"reflections"}).$$

The end!