Homomorphisms

Casey Blacker
Math 300

Section 1

Informal idea

Informal Definition

A *homomorphism* from a structured set X to a structured set Y is a structure-preserving function $f : X \to Y$.

False definition

A homomorphism $f : X \to Y$ is called a

i. *monomorphism* if it is injective,
ii. *epimorphism* if it is surjective,
iii. *isomorphism* if it is bijective.

Definition

i. A homomorphism $f : X \to X$ is called an *endomorphism*.

ii. An isomorphism $f : X \to X$ is called an *automorphism*.

	$f : X \to Y$	$f : X \to X$
—	*homo-*	*endo-*
bijection	*iso-*	*auto-*
injection	*mono-*	—
surjection	*epi-*	—

Remark

i. Monomorphisms are occasionally denoted $f : X \hookrightarrow Y$, epimorphisms $f : X \twoheadrightarrow Y$, and isomorphisms $f : X \xrightarrow{\sim} Y$.

ii. We say that X and Y are *isomorphic* if there exists an isomorphism $f : X \xrightarrow{\sim} Y$.

Is it a homomorphism?

the inclusion $(\mathbb{Z}, +) \to (\mathbb{R}, +)$

Yes, monomorphism

Is it a homomorphism?

$$\begin{aligned} f : (\mathbb{Z}, +) &\to (\mathbb{Z}, +) \\ k &\mapsto -k \end{aligned}$$

Yes, isomorphism

Is it a homomorphism?

$$\begin{aligned} f : (\mathbb{Z}, +, \cdot) &\longrightarrow (\mathbb{Z}, +, \cdot) \\ k &\longmapsto -k \end{aligned}$$

No

Is it a homomorphism?

$$\begin{aligned} f : (\mathbb{R}, \leq) &\xrightarrow{\sim} (\mathbb{R}, \geq) \\ x &\longmapsto x \end{aligned}$$

No

Is it a homomorphism?

inclusion $(0, +, \cdot) \to (\mathbb{R}, +, \cdot)$

Yes, monomorphism

Is it a homomorphism?

$$\begin{aligned} f : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}, +) \\ x &\longmapsto 1 \end{aligned}$$

No

Is it a homomorphism?

projection $(\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +, \cdot)$

Yes, epimorphism

Is it a homomorphism?

$$\text{inclusion } (0, +, \cdot) \to (\mathbb{R}, +, \cdot)$$

Yes

Is it a homomorphism?

$$\begin{aligned} f : (\mathbb{Z}, I) &\longrightarrow (\mathbb{Z}, \cong_2) \\ k &\longmapsto k \end{aligned}$$

No

Is it a homomorphism?

Fix $n \in \mathbb{Z}$ and let

$$\begin{aligned} f_n : (\mathbb{Z}, +) &\xrightarrow{\sim} (\mathbb{Z}, +) \\ k &\longmapsto n \cdot k \end{aligned}$$

Yes, monomorphism

Is it a homomorphism?

$$\begin{aligned} f : (\mathbb{R}, \leq) &\xrightarrow{\sim} (\mathbb{R}, \geq) \\ x &\longmapsto -x \end{aligned}$$

Yes, isomorphism

Is it a homomorphism?

$$\begin{aligned} f : (\mathbb{Z}, I) &\longrightarrow (\mathbb{Z}, \cong_2) \\ k &\longmapsto k \end{aligned}$$

Yes, ???

Section 2

Formal definition

The definition of *homomorphism* depends on the context.

However, it should always be the case that

i. the identity $\mathrm{id} : X \to X$ is a homomorphism,
ii. if $f : X \to Y$ and $g : Y \to Z$ are homomorphisms, then $g \circ f : X \to Z$ is a homomorphism.

Definition

A homomorphism $f : X \to Y$ is called a

i. *monomorphism* if

$$\forall (g, g' : Z \to X) : (f \circ g = f \circ g') \implies g = g',$$

that is, f is *left-cancellative*,

ii. *epimorphism* if

$$\exists (h : Y \to X) : (h \circ f = h' \circ f) \implies h = h',$$

that is, f is *right-cancellative*,

iii. *isomorphism* if

$$\exists (k : Y \to X) : (f \circ k = \mathrm{id}_Y) \wedge (k \circ f = \mathrm{id}_X),$$

that is, f has an *inverse* k.

Special names for homomorphisms

	homomorphism	isomorphism
set	function	bijection
group, ring, field	(group, ...) homomorphism	(group, ...) isomorphism
vector space, module	linear map	linear isomorphism
partial order	monotone map	order isomorphism
topological space	continuous map	homeomorphism
metric space	cont. map	homeo.
alternatively	isometric embedding	isometry

Group homomorphisms

Definition

A *group homomorphism* from $(G, \cdot)$ to $(H, *)$ is a function $f : G \to H$ such that

$$\forall g, g' \in G \ : \ f(g \cdot g') = f(g) * f(g').$$

Example

Fix $n \in \mathbb{N}_+$. The map

$$\begin{aligned} f : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}_n, +) \\ k &\longmapsto k \mod n \end{aligned}$$

is a group homomorphism.

Ring homomorphisms

Definition

A *ring homomorphism* from $(R, +, \cdot)$ to $(S, \oplus, *)$ is a function $f : R \to S$ such that for all $r, r' \in R$,

i. $f(r + r') = f(r) \oplus f(r')$,

ii. $f(r \cdot r') = f(r) * f(r')$,

iii. $f(1_R) = 1_S$.

Remarks

i. A *field homomorphism* is a ring homomorphism between fields.

ii. If we omit the condition that $f(1_R) = 1_S$, then we have the definition of a *nonunital ring homomorphism* (or a *rng homomorphism*).

Example (ring homomorphism)

The map $f : \mathbb{Z} \to \mathbb{Z}_2$ given by

$$f(k) = \begin{cases} 0 & \text{if } k \text{ is even,} \\ 1 & \text{if } k \text{ is odd.} \end{cases}$$

is a ring homomorphism.

Example (ring homomorphism nonexample)

The map

$$\begin{aligned} f(k) : \mathbb{Z} &\to \mathbb{Z} \\ k &\mapsto 2k \end{aligned}$$

is neither a ring homomorphism nor a rng homomorphism.

Poset homomorphisms

Definition

A *monotone map* $f : (A, \leq) \to (B, \preccurlyeq)$ satisfies

$$\forall a, a' \in A : a \leq a' \implies f(a) \preccurlyeq f(a').$$

An *order embedding* is an injective monotone map, and an *order isomorphism* is a bijective monotone map.

Example

Let $A = \{0\}$ and $B = \{0, 1\}$. The map

$$\begin{aligned} f : (A, \leq) &\longrightarrow (B, \preccurlyeq) \\ 0 &\longmapsto 0 \end{aligned}$$

is an order embedding but not an order isomorphism.

Vector space homomorphisms

Definition

A *linear map* of k-vector spaces from U to V is a function $f : U \to V$ such that

i. $f(u+u') = f(u) + f(u')$ for all $u, u' \in U$, and
ii. $f(su) = sf(u)$ for all $u \in U$ and $s \in k$.

Equivalently, $f(u+su') = f(u) + f(su')$ for all $u, u' \in U$ and $s \in k$.

Example

The map $f : \mathbb{R}^3 \to \mathbb{R}^2$ where

$$f(x_1, x_2, x_3) = (2x_1 + x_2, x_2)$$

is linear.

Setoid homomorphisms

Example

Fix a set A with at least two elements. Let $I \subseteq A \times A$ be the identity relation on A and define the equivalence relation $R = A \times A$. The function

$$\begin{aligned} f : (A, I) &\longrightarrow (A, R) \\ a &\longmapsto a \end{aligned}$$

is both a monomorphism and an epimorphism, but not an isomorphism.

Section 3

Proofs with homomorphisms

group homomorphisms preserve identities

Proposition

If $\phi : G \to H$ is a group homomorphism, then $\phi(1_G) = 1_H$.

Proof.

We have

$$\phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1).$$

The result follows by multiplying each side by $\phi(1)^{-1}$. □

group homomorphisms preserve inverses

Proposition

If $\phi : G \to H$ is a group homomorphism, then $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.

Proof.

By the previous result, we have

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

Multiplying each side of this equality on the left by $\phi(g)^{-1}$, we obtain $\phi(g^{-1}) = \phi(g)^{-1}$. $\square$