Lecture 4.1: Homomorphisms and isomorphisms

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Motivation

Throughout the course, we've said things like:

- "This group has the same structure as that group."
- "This group is isomorphic to that group."

However, we've never really spelled out the details about what this means.

We will study a special type of function between groups, called a *homomorphism*. An *isomorphism* is a special type of homomorphism. The Greek roots "homo" and "morph" together mean "same shape."

There are two situations where homomorphisms arise:

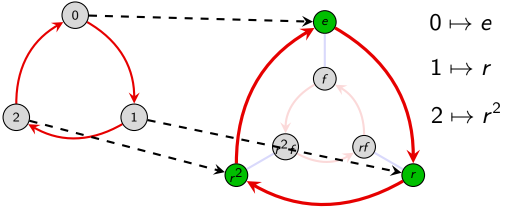
- when one group is a subgroup of another;
- when one group is a quotient of another.

The corresponding homomorphisms are called embeddings and quotient maps.

Also in this chapter, we will completely classify all finite abelian groups, and get a taste of a few more advanced topics, such as the the four "isomorphism theorems," commutators subgroups, and automorphisms.

A motivating example

Consider the statement: $\mathbb{Z}_3 < D_3$. Here is a visual:



The group D_3 contains a size-3 cyclic subgroup $\langle r \rangle$, which is identical to $\mathbb{Z}_3$ in structure only. None of the elements of $\mathbb{Z}_3$ (namely 0, 1, 2) are actually in D_3.

When we say $\mathbb{Z}_3 < D_3$, we really mean is that the structure of $\mathbb{Z}_3$ shows up in D_3.

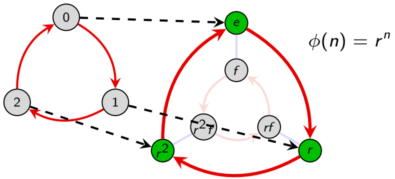
In particular, there is a bijective correspondence between the elements in $\mathbb{Z}_3$ and those in the subgroup $\langle r \rangle$ in D_3. Furthermore, the *relationship* between the corresponding nodes is the same.

A homomorphism is the mathematical tool for succinctly expressing precise structural correspondences. It is a *function* between groups satisfying a few "natural" properties.

Homomorphisms

Using our previous example, we say that this function maps elements of $\mathbb{Z}_3$ to elements of D_3. We may write this as

$$\phi\colon \mathbb{Z}_3 \longrightarrow D_3 \,.$$



The group *from* which a function originates is the domain ($\mathbb{Z}_3$ in our example). The group *into* which the function maps is the codomain (D_3 in our example).

The elements in the codomain that the function maps to are called the image of the function ($\{e, r, r^2\}$ in our example), denoted $\mathrm{Im}(\phi)$. That is,

$$\mathrm{Im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\} \,.$$

Definition

A homomorphism is a function $\phi\colon G \to H$ between two groups satisfying

$$\phi(ab) = \phi(a)\phi(b), \qquad \text{for all } a, b \in G \,.$$

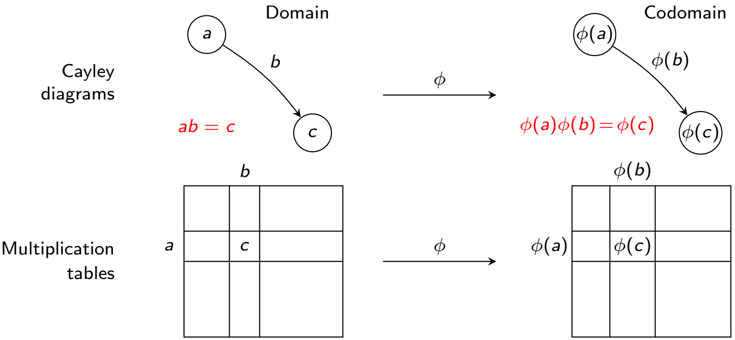
Note that the operation $a \cdot b$ is occurring in the domain while $\phi(a) \cdot \phi(b)$ occurs in the codomain.

Homomorphisms

Remark

Not every function from one group to another is a homomorphism! The condition $\phi(ab) = \phi(a)\phi(b)$ means that the map ϕ preserves the structure of G.

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



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

An example

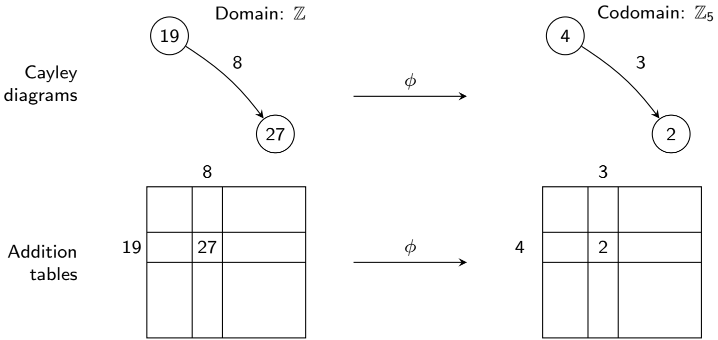
Consider the function ϕ that reduces an integer modulo 5:

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

Since the group operation is additive, the "homomorphism property" becomes

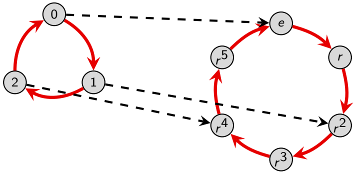
$$\phi(a+b) = \phi(a) + \phi(b) \,.$$

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



Types of homomorphisms

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



$0 \mapsto e$

$1 \mapsto r^2$

$2 \mapsto r^4$

It is easy to check that $\theta(a+b) = \theta(a)\theta(b)$: The red-arrow in $\mathbb{Z}_3$ (representing 1) gets mapped to the 2-step path representing r^2 in C_6.

A homomorphism $\phi\colon G \to H$ that is one-to-one or "injective" is called an embedding: the group G "embeds" into H as a subgroup. If θ is not one-to-one, then it is a quotient.

If $\phi(G) = H$, then ϕ is onto, or surjective.

Definition

A homomorphism that is both injective and surjective is an an **isomorphism**.

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

Homomorphisms and generators

Remark

If we know where a homomorphism maps the generators of G, we can determine where it maps *all* elements of G.

For example, suppose $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6$ was a homomorphism, with $\phi(1) = 4$. Using this information, we can construct the rest of ϕ:

$$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 4 + 4 = 2$$
$$\phi(0) = \phi(1+2) = \phi(1) + \phi(2) = 4 + 2 = 0.$$

Example

Suppose that $G = \langle a, b \rangle$, and $\phi \colon G \to H$, and we know $\phi(a)$ and $\phi(b)$. Using this information we can determine the image of any element in G. For example, for $g = a^3 b^2 ab$, we have

$$\phi(g) = \phi(aaabbab) = \phi(a)\,\phi(a)\,\phi(a)\,\phi(b)\,\phi(b)\,\phi(a)\,\phi(b).$$

What do you think $\phi(a^{-1})$ is?

Two basic properties of homomorphisms

Proposition

Let $\phi\colon G \to H$ be a homomorphism. Denote the identity of G by 1_G, and the identity of H by 1_H.

(i) $\phi(1_G) = 1_H$ "ϕ sends the identity to the identity"

(ii) $\phi(g^{-1}) = \phi(g)^{-1}$ "ϕ sends inverses to inverses"

Proof

(i) Pick any $g \in G$. Now, $\phi(g) \in H$; observe that that

$$\phi(1_G)\,\phi(g) = \phi(1_G \cdot g) = \phi(g) = 1_H \cdot \phi(g)\,.$$

Therefore, $\phi(1_G) = 1_H$. ✓

(ii) Take any $g \in G$. Observe that

$$\phi(g)\,\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1_G) = 1_H\,.$$

Since $\phi(g)\phi(g^{-1}) = 1_H$, it follows immediately that $\phi(g^{-1}) = \phi(g)^{-1}$. ✓ □

A word of caution

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

For example, suppose we try to define a homomorphism $\phi\colon \mathbb{Z}_3 \to \mathbb{Z}_4$ by $\phi(1) = 1$. Then we get

$$\begin{aligned}\phi(2) &= \phi(1+1) = \phi(1) + \phi(1) = 2, \\ \phi(0) &= \phi(1+1+1) = \phi(1) + \phi(1) + \phi(1) = 3\,.\end{aligned}$$

This is *impossible*, because $\phi(0) = 0$. (Identity is mapped to the identity.)

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

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

Exercise

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

Isomorphisms

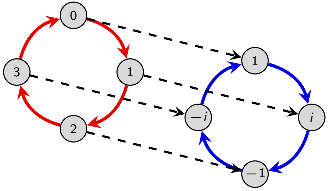
Two isomorphic groups may name their elements differently and may look different based on the layouts or choice of generators for their Cayley diagrams, but the isomorphism between them guarantees that they have the same structure.

When two groups G and H have an isomorphism between them, we say that G and H are isomorphic, and write $G \cong H$.

The roots of the polynomial $f(x) = x^4 - 1$ are called the 4th roots of unity, and denoted $R(4) := \{1, i, -1, -i\}$. They are a subgroup of $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$, the nonzero complex numbers under multiplication.

The following map is an isomorphism between $\mathbb{Z}_4$ and $R(4)$.

$$\phi\colon \mathbb{Z}_4 \longrightarrow R(4)\,, \qquad \phi(k) = i^k\,.$$

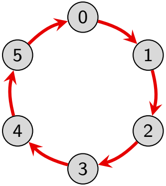


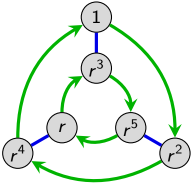
Isomorphisms

Sometimes, the isomorphism is less visually obvious because the Cayley graphs have different structure.

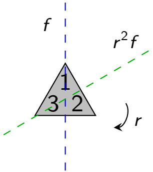
For example, the following is an isomorphism:

$$\phi\colon \mathbb{Z}_6 \longrightarrow C_6$$
$$\phi(k) = r^k$$

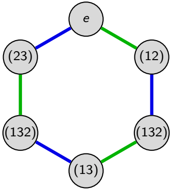


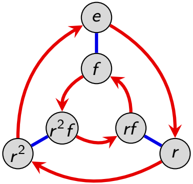


Here is another non-obvious isomorphism between $S_3 = \langle (12), (23) \rangle$ and $D_3 = \langle r, f \rangle$.



$$\phi\colon S_3 \longrightarrow D_3$$
$$\phi\colon (12) \longmapsto r^2 f$$
$$\phi\colon (23) \longmapsto f$$





Another example: the quaternions

Let $\mathrm{GL}_n(\mathbb{R})$ be the set of invertible $n \times n$ matrices with real-valued entries. It is easy to see that this is a group under multiplication.

Recall the quaternion group $Q_4 = \langle i, j, k \mid i^2 = j^2 = k^2 = -1,\ ij = k \rangle$.

The following set of 8 matrices forms an isomorphic group under multiplication, where I is the 4×4 identity matrix:

$$\left\{ \pm I,\quad \pm \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},\quad \pm \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix},\quad \pm \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \right\}.$$

Formally, we have an embedding $\phi\colon Q_4 \to \mathrm{GL}_4(\mathbb{R})$ where

$$\phi(i) = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},\quad \phi(j) = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix},\quad \phi(k) = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

We say that Q_4 is represented by a set of matrices.

Many other groups can be represented by matrices. Can you think of how to represent V_4, C_n, or S_n, using matrices?