Visual Algebra

Lecture 4.1: Homomorphisms

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

Homomorphisms

Throughout this course, we've said that two groups are isomorphic if for some generating sets, they have Cayley graphs with the same structure.

This can be formalized by a "structure-preserving" function $\phi\colon G \to H$ between groups, called a homomorphism.

An **isomorphism** is simply a bijective homomorphism.

What we called a *re-wiring* when constructing semidirect products is an automorphism: an isomorphism $\phi\colon G \to G$.

The Greek roots "*homo*" and "*morph*" together mean "same shape."

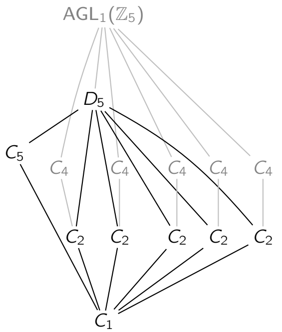
The homomorphism $\phi\colon G \to H$ is an

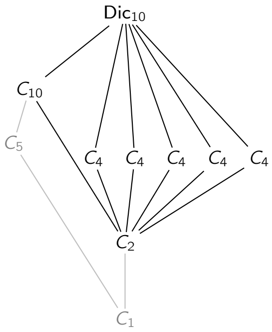
- embedding if ϕ is one-to-one: "*G is a subgroup of H.*"
- quotient map if ϕ is onto: "*H is a quotient of G.*"

We'll see that even if ϕ is neither, it can be decomposed as a *composition* $\phi = \iota \circ \pi$ of quotient followed by an embedding.

Preview: embeddings vs. quotients

The difference between embeddings and quotient maps can be seen in the subgroup lattice:





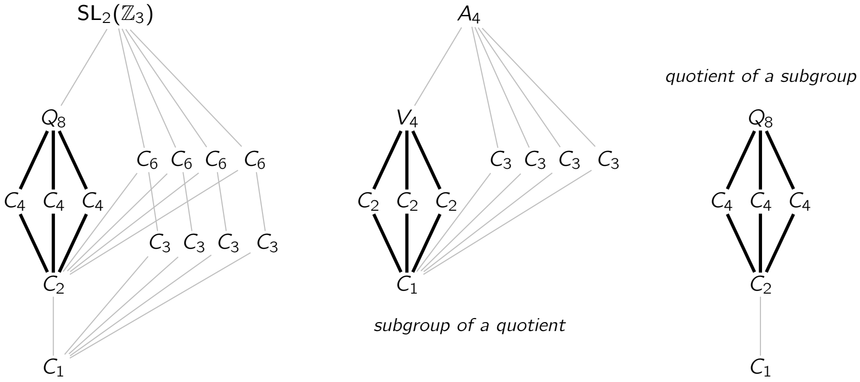
In one of these groups, D_5 is subgroup. In the other, it arises as a quotient.

This, and much more, will be consequences of the celebrated **isomorphism theorems**.

Preview: subgroups, quotients, and subquotients

Often, we'll see familiar subgroup lattices in the middle of a larger lattice.

These are called **subquotients**.

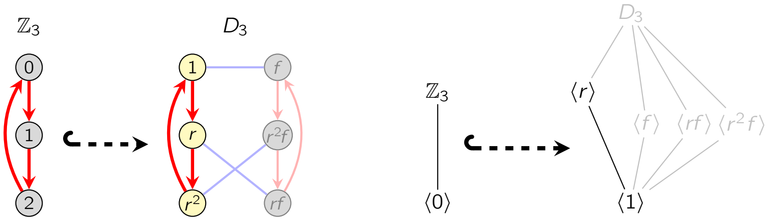


The *isomorphism theorems* relates the structure of a group to that of its quotients and subquotients.

A example embedding

When we say $\mathbb{Z}_3 \leq D_3$, we really mean that *the structure of* $\mathbb{Z}_3$ *appears in* D_3.

This can be formalized by a map $\phi\colon \mathbb{Z}_3 \to D_3$, defined by $\phi\colon n \mapsto r^n$.



In general, a homomorphism is a function $\phi\colon G \to H$ with some extra properties.

We will use standard function terminology:

- the group G is the domain
- the group H is the codomain
- the image is what is often called the *range*:

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

The formal definition

Definition

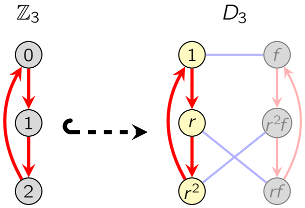
A homomorphism is a function $\phi \colon G \to H$ between two groups satisfying

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

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

In this example, the homomorphism condition is $\phi(a+b) = \phi(a) \cdot \phi(b)$. (*Why?*)

$$\phi \colon \mathbb{Z}_3 \longrightarrow D_3$$
$$k \longmapsto r^k$$

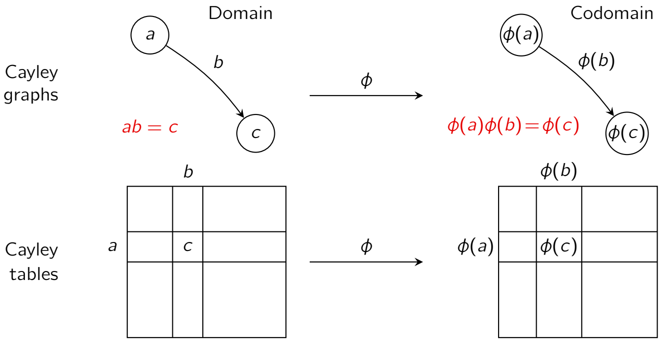


Not only is there a bijective correspondence between the elements in $\mathbb{Z}_3$ and those in the subgroup $\langle r \rangle$ of D_3, but the relationship between the corresponding nodes is the same.

Remark

Not every function between groups 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 graphs and Cayley tables.



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

An example

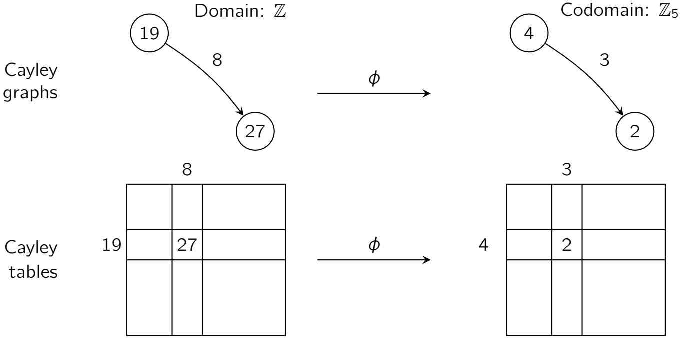
Consider the function ϕ that reduces an integer modulo 5:

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

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."



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, if $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6$ is a homomorphism with $\phi(1) = 4$, we can deduce:

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

Example

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

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

Note that if $k \in \mathbb{N}$, then $\phi(a^k) = \phi(a)^k$. What do you think $\phi(a^{-1})$ is?

Two basic properties of homomorphisms

Proposition

For any homomorphism $\phi\colon G \to H$:

(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

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

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 $\phi(g^{-1}) = \phi(g)^{-1}$. ✓

Corollary

If ϕ is a homomorphism, then $\phi(g^n) = \phi(g)^n$ for all $n \in \mathbb{Z}$.

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, let's try to define a homomorphism $\phi\colon \mathbb{Z}_3 \to \mathbb{Z}_4$ 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 $\phi\colon \mathbb{Z}_3 \to \mathbb{Z}_4$; 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 $\phi(1) = 0$.