Visual Algebra

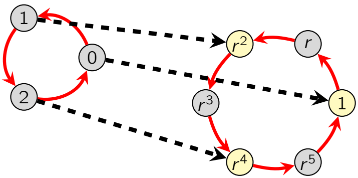
Lecture 4.2: Embeddings and quotients

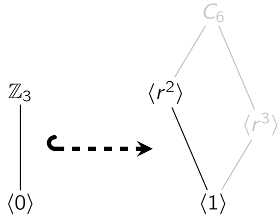
Dr. Matthew Macauley

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

Types of homomorphisms

Consider the following homomorphism $\theta\colon \mathbb{Z}_3 \to C_6$, 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 $\phi\colon G \to H$ that is one-to-one or "injective" is an embedding: the group G "embeds" into H as a subgroup. Optional: write $\phi\colon G \hookrightarrow H$.

If $\phi(G) = H$, then ϕ is onto, or surjective. We call it a quotient. Optional: $\phi\colon G \twoheadrightarrow H$.

Definition

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

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

An example that is neither an embedding nor quotient

Consider the homomorphism $\phi\colon Q_8 \to A_4$ defined by

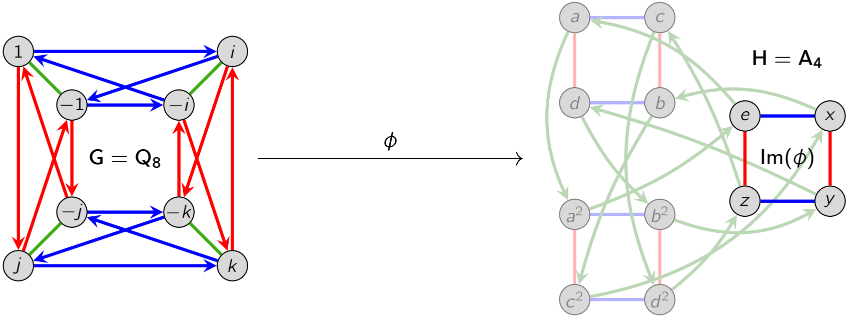
$$\phi(i) = (12)(34), \qquad \phi(j) = (13)(24).$$

Using the property of homomorphisms,

$$\phi(k) = \phi(ij) = \phi(i)\phi(j) = (12)(34) \cdot (13)(24) = (14)(23),$$

$$\phi(-1) = \phi(i^2) = \phi(i)^2 = \big((12)(34)\big)^2 = e,$$

and $\phi(-g) = \phi(g)$ for $g = i, j, k$.



An example of an isomorphism

We have already seen that D_3 is isomorphic to S_3.

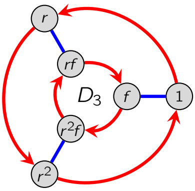
This means that there's a bijective correspondence $f\colon D_3 \to S_3$.

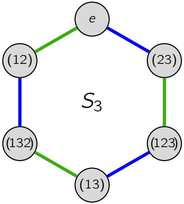
But not just any bijection will do. Intuitively,

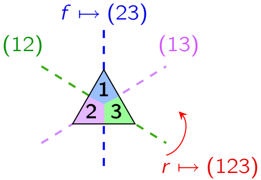
- (123) and (132) should be the rotations
- (12), (13), and (23) should be the reflections
- The identity permutation must be the identity symmetry.

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

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







However, there are other isomorphisms between these groups.

Group representations

We've already seen how to represent groups as collections of matrices.

Formally, a (faithful) representation of a group G is a (one-to-one) homomorphism

$$\phi\colon G \longrightarrow \mathrm{GL}_n(K)$$

for some field K (e.g., $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, etc.)

For example, the following 8 matrices form group under multiplication, isomorphic to Q_8.

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

Formally, we have an embedding $\phi\colon Q_8 \hookrightarrow \mathbf{GL}_4(\mathbb{R})$ where

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

Notice how we can use the homomorphism property to find the image of the other elements.

Kernels and quotient maps

If $\phi \colon G \to H$ is onto, it is a quotient map.

We'll see how these arise from our quotient process.

Definition

The kernel of a homomorphism $\phi \colon G \to H$ is the set

$$\text{Ker}(\phi) := \phi^{-1}(1_H) = \{k \in G \mid \phi(k) = 1_H\}.$$

The kernel is the "group theoretic" analogue of the nullspace of a matrix.

Another way to define the kernel is as the preimage of the identity.

Definition

If $\phi \colon G \to H$ is a homomorphism and $h \in \text{Im}(\phi)$, define the preimage of h to be the set

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

Note that ϕ^{-1} is generally *not* a function!

Let's do some examples, and observe what the kernels and preimages are.

An example of a quotient

Recall that $C_2 = \{e^{0\pi i}, e^{1\pi i}\} = \{1, -1\}$. Consider the following quotient map:

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

Note that

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

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

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

$\mathbf{1}$	$\mathbf{-1}$
$\mathbf{-1}$	$\mathbf{1}$

$$\operatorname{Ker}(\phi) = \phi^{-1}(1) = \langle r \rangle \quad (\text{“}\textit{rotations}\text{”}), \qquad \phi^{-1}(-1) = f\langle r \rangle \quad (\text{“}\textit{reflections}\text{”}).$$

An example of a quotient

Define the homomorphism

$$\phi\colon Q_8 \twoheadrightarrow V_4, \qquad \phi(i) = v, \;\; \phi(j) = h.$$

Since $Q_8 = \langle i, j \rangle$, we can determine where ϕ sends the remaining elements:

$$\phi(1) = e$$

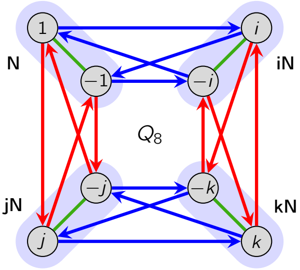
$$\phi(-1) = \phi(i^2) = \phi(i)^2 = v^2 = e$$

$$\phi(k) = \phi(ij) = \phi(i)\phi(j) = vh = r$$

$$\phi(-k) = \phi(ji) = \phi(j)\phi(i) = hv = r$$

$$\phi(-i) = \phi(-1)\phi(i) = ev = v$$

$$\phi(-j) = \phi(-1)\phi(j) = eh = h$$



Note that the kernel is the normal subgroup $N := \mathrm{Ker}(\phi) = \phi^{-1}(e) = \langle -1 \rangle$, and all preimages are cosets:

$$\phi^{-1}(v) = iN, \qquad \phi^{-1}(h) = jN, \qquad \phi^{-1}(r) = kN.$$

Properties of the kernel

Proposition

The kernel of any homomorphism $\phi\colon G \to H$, is a normal subgroup.

Proof

Let $N := \mathrm{Ker}(\phi)$. First, we'll show that it's a subgroup. Take any $a, b \in N$.

Identity: $\phi(e) = e$. ✓

Closure: $\phi(ab) = \phi(a)\,\phi(b) = e \cdot e = e$. ✓

Inverse: $\phi(a^{-1}) = \phi(a)^{-1} = e^{-1} = e$. ✓

Now we'll show it's normal. Take any $n \in N$. We'll show that $gng^{-1} \in N$ for all $g \in G$.

By the homomorphism property,

$$\phi(gng^{-1}) = \phi(g)\,\phi(n)\,\phi(g^{-1}) = \phi(g) \cdot e \cdot \phi(g)^{-1} = e.$$

Therefore, $gng^{-1} \in \mathrm{Ker}(\phi)$. □

Key observation

Given any homomorphism $\phi\colon G \to H$, we can *always* form the quotient group $G/\,\mathrm{Ker}(\phi)$.

Properties of the kernel

Proposition

Let $\phi\colon G \to H$ be a homomorphism. Then each preimage $\phi^{-1}(h)$ is a coset of $\mathrm{Ker}(\phi)$.

Proof

Let $N = \mathrm{Ker}(\phi)$ and take any $g \in \phi^{-1}(h)$. (This means $\phi(g) = h$.)

We claim that $\phi^{-1}(h) = gN$. We need to verify both $\subseteq$ and $\supseteq$.

"$\subseteq$": Take $a \in \phi^{-1}(h)$, i.e., $\phi(a) = h$. We need to show that $a \in gN$.

From basic properties of cosets, we have the equivalences

$$a \in gN \quad \Longleftrightarrow \quad aN = gN \quad \Longleftrightarrow \quad g^{-1}aN = N \quad \Longleftrightarrow \quad g^{-1}a \in N.$$

This last condition is true because

$$\phi(g^{-1}a) = \phi(g)^{-1}\phi(a) = h^{-1} \cdot h = 1_H. \qquad \checkmark$$

"$\supseteq$": Pick any $gn \in gN$. This is in $\phi^{-1}(h)$ because

$$\phi(gn) = \phi(g)\phi(n) = h \cdot 1_H = h. \qquad \checkmark$$