Visual Algebra

Lecture 4.3: The fundamental homomorphism theorem

Dr. Matthew Macauley

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

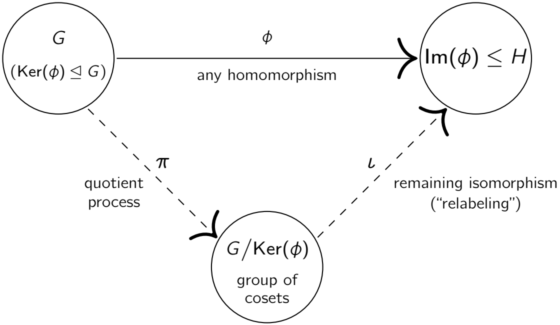
Every homomorphic image is a quotient

The following is one of the central results in group theory.

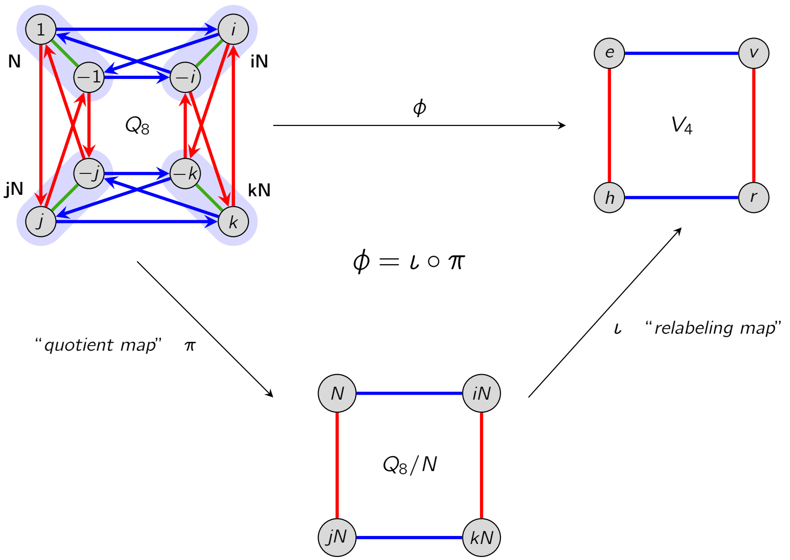
Fundamental homomorphism theorem (FHT)

If $\phi\colon G \to H$ is a homomorphism, then $G/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$.

The FHT says that every homomorphism can be decomposed into two steps: (i) quotient out by the kernel, and then (ii) relabel the nodes via ϕ.



Visualizing the FHT via Cayley graphs



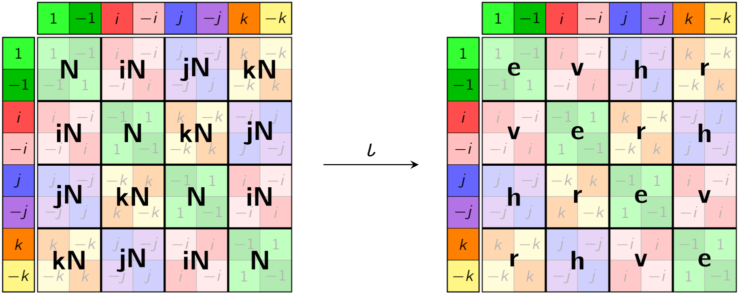
Visualizing the FHT via Cayley tables

Here's another way to think about the homomorphism

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

as the composition of:

- a quotient by $N=\mathrm{Ker}(\phi)=\langle -1\rangle=\{\pm 1\}$,
- a *relabeling map* $\iota\colon Q_8/N \to V_4$.



Proof of the FHT

Fundamental homomorphism theorem

If $\phi\colon G \to H$ is a homomorphism, then $\mathrm{Im}(\phi) \cong G/\operatorname{Ker}(\phi)$.

Proof

We'll construct an explicit map $\iota\colon G/\operatorname{Ker}(\phi) \longrightarrow \mathrm{Im}(\phi)$ and prove that it's an isomorphism.

Let $N = \operatorname{Ker}(\phi)$, and recall that $G/N = \{gN \mid g \in G\}$. Define

$$\iota\colon G/N \longrightarrow \mathrm{Im}(\phi)\,, \qquad \iota\colon gN \longmapsto \phi(g)\,.$$

- *Show ι is well-defined*: We must show that if $aN = bN$, then $\iota(aN) = \iota(bN)$.

$$\begin{array}{rcll}
aN = bN & \Longrightarrow & b^{-1}aN = N & (\text{left-multiply by } b^{-1}) \\
& \Longrightarrow & b^{-1}a \in N & (xH = H \;\Leftrightarrow\; x \in H) \\
& \Longrightarrow & \phi(b^{-1}a) = 1_H & (\text{definition of } \operatorname{Ker}(\phi)) \\
& \Longrightarrow & \phi(b)^{-1}\,\phi(a) = 1_H & (\phi \text{ is a homom.}) \\
& \Longrightarrow & \phi(a) = \phi(b) & (\text{left-multiply by } \phi(b)) \\
& \Longrightarrow & \iota(aN) = \iota(bN) & (\text{by definition}) \qquad \checkmark
\end{array}$$

- *Show ι is injective (1–1)*: $\big[\,\iota(aN) = \iota(bN) \Rightarrow aN = bN.\big]$ Replace each $\Longrightarrow$ with $\Longleftrightarrow$. $\checkmark$

Proof of FHT (cont.) [Recall: $\iota\colon G/N \to \mathrm{Im}(\phi)$, $\iota\colon gN \mapsto \phi(g)$]

Proof (cont.)

- *Show ι is a homomorphism*: We must show that $\iota(aN \cdot bN) = \iota(aN)\,\iota(bN)$.

$$\begin{aligned}
\iota(aN \cdot bN) &= \iota(abN) && (aN \cdot bN := abN) \\
&= \phi(ab) && (\text{definition of } \iota) \\
&= \phi(a)\,\phi(b) && (\phi \text{ is a homomorphism}) \\
&= \iota(aN)\,\iota(bN) && (\text{definition of } \iota)
\end{aligned}$$

Thus, ι is a homomorphism. ✓

- *Show ι is surjective (onto)*:

Take any element in the codomain (here, $\mathrm{Im}(\phi)$). We need to find an element in the domain (here, G/N) that gets mapped to it by ι.

Pick any $\phi(a) \in \mathrm{Im}(\phi)$. By defintion, $\iota(aN) = \phi(a)$, hence ι is surjective. ✓

In summary, since $\iota\colon G/N \to \mathrm{Im}(\phi)$ is a well-defined homomorphism that is injective (1–1) and surjective (onto), it is an **isomorphism**. □

Consequences of the FHT

Corollary

If $\phi\colon G \to H$ is a homomorphism, then $\operatorname{Im}\phi \leq H$.

The two "extreme cases"

- If $\phi\colon G \hookrightarrow H$ is an embedding, then $\operatorname{Ker}(\phi) = \{1_G\}$. The FHT says that

$$\operatorname{Im}(\phi) \cong G/\{1_G\} \cong G.$$

- If $\phi\colon G \to H$ is the trivial map $\phi(g) = 1_H$ for all $h \in G$, then $\operatorname{Ker}(\phi) = G$. The FHT says that

$$\{1_H\} = \operatorname{Im}(\phi) \cong G/G.$$

Let's use the FHT to determine all homomorphisms $\phi\colon C_4 \to C_3$.

- By the FHT, $G/\operatorname{Ker}\phi \cong \operatorname{Im}\phi \leq C_3$, and so $|\operatorname{Im}\phi| = 1$ or 3.
- Since $\operatorname{Ker}\phi \leq C_4$, Lagrange's Theorem also tells us that $|\operatorname{Ker}\phi| \in \{1, 2, 4\}$, and hence $|\operatorname{Im}\phi| = |G/\operatorname{Ker}\phi| \in \{1, 2, 4\}$.

Thus, $|\operatorname{Im}\phi| = 1$, and so the *only* homomorphism $\phi\colon C_4 \to C_3$ is the trivial one.

Consequences of the FHT

Let's do a more complicated example: find all homomorphisms $\phi\colon \mathbb{Z}_{44} \to \mathbb{Z}_{16}$.

By the FHT,

$$\mathbb{Z}_{44}/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi) \leq \mathbb{Z}_{16}.$$

This means that $44/|\operatorname{Ker}(\phi)|$ must be 1, 2, 4, $\cancel{8}$, or $\cancel{16}$.

Also, $|\operatorname{Ker}(\phi)|$ must divide 44. We are left with three cases: $|\operatorname{Ker}(\phi)| = 44$, 22, or 11.

Reminder

For each $d \mid n$, the group $\mathbb{Z}_n$ has a unique subgroup of order d, which is $\langle n/d \rangle$.

- **Case 1**: $|\operatorname{Ker}(\phi)| = 44$, which forces $|\operatorname{Im}(\phi)| = 1$, and so $\phi(1) = 0$ is the trivial homomorphism.
- **Case 2**: $|\operatorname{Ker}(\phi)| = 22$. By the FHT, $|\operatorname{Im}(\phi)| = 2$, which means $\operatorname{Im}(\phi) = \{0, 8\}$, and so $\phi(1) = 8$.
- **Case 3**: $|\operatorname{Ker}(\phi)| = 11$. By the FHT, $|\operatorname{Im}(\phi)| = 4$, which means $\operatorname{Im}(\phi) = \{0, 4, 8, 12\}$.

  There are two subcases: $\phi(1) = 4$ or $\phi(1) = 12$.

What does "well-defined" really mean?

Recall that we've seen the term "**well-defined**" arise in different contexts:

- a well-defined binary operation on a set G/N of cosets,
- a well-defined function $\iota\colon G/N \to H$ from a set (group) of cosets.

In both of these cases, well-defined means that:

"*our definition doesn't depend on our choice of coset representative*."

Formally:

- If $N \trianglelefteq G$, then $aN \cdot bN := abN$ is a well-defined binary operation on the set G/N of cosets, because

$$\text{if } \; a_1N = a_2N \; \text{ and } \; b_1N = b_2N, \; \text{ then } \; a_1b_1N = a_2b_2N.$$

- The map $\iota\colon G/N \to H$, where $\iota(aN) = \phi(a)$, is a well-defined homomorphism, meaning that

$$\text{if } \; aN = bN, \; \text{ then } \; \iota(aN) = \iota(bN) \; \text{ (that is, } \phi(a) = \phi(b)\text{) holds.}$$

Remark

Whenever we define a map and the domain is a *quotient*, we must show it's well-defined.

What does "well-defined" really mean?

In some sense, well-defined and injective are "dual" concepts:

- f is well-defined if the same input cannot map to different outputs
- f is injective if different inputs cannot map to the same output.

$$\begin{tikzcd}
aN \arrow[dr, mapsto] & \\
& f(aN)=f(bN) \\
bN \arrow[ur, mapsto] &
\end{tikzcd}$$

not allowed if 1-to-1

$$\begin{tikzcd}
& f(aN) \\
aH=bN \arrow[ur, mapsto] \arrow[dr, mapsto] & \\
& f(b(N))
\end{tikzcd}$$

not allowed if well-defined

Let's revisit the proof of the FHT, and the map

$$\iota\colon G/N \to H, \qquad \iota(aN) = \phi(a), \qquad \text{where } N = \mathrm{Ker}(\phi).$$

Showing ι is well-defined is done as follows:

$$aN=bN \;\Rightarrow\; b^{-1}aN=N \;\Rightarrow\; b^{-1}a \in N \;\Rightarrow\; \phi(b^{-1}a)=1 \;\Rightarrow\; \phi(a)=\phi(b) \;\Rightarrow\; \iota(aN)=\iota(bN).$$

Reversing each $\Rightarrow$ shows ι is 1-to-1.

How to show two groups are isomorphic

The standard way to show $G \cong H$ is to construct an isomorphism $\phi \colon G \to H$.

When the domain is a quotient, there is another method, due to the FHT.

Useful technique

Suppose we want to show that $G/N \cong H$. There are two approaches:

(i) Define a map $\phi \colon G/N \to H$ and prove that it is well-defined, a homomorphism, and a bijection.

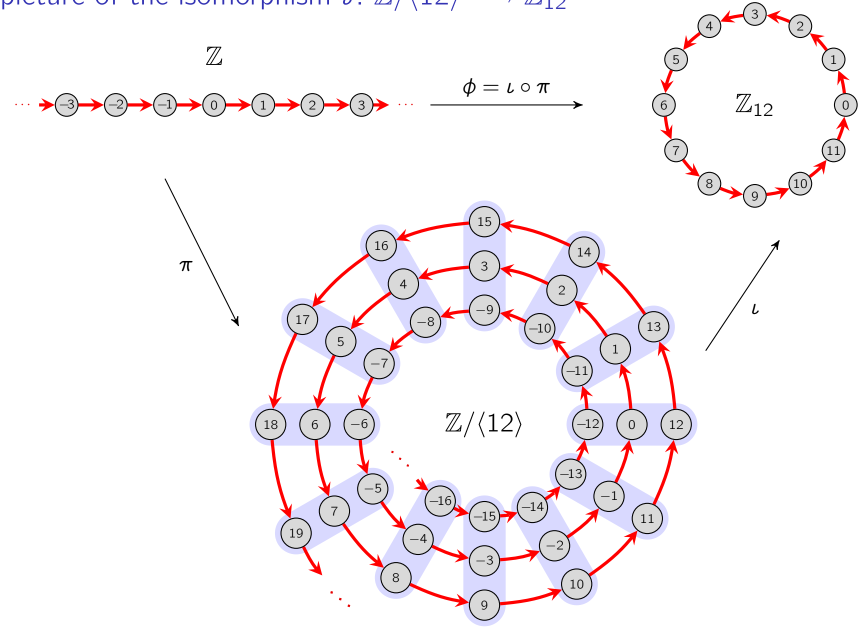
(ii) Define a map $\phi \colon G \to H$ and prove that it is a homomorphism, a surjection (onto), and that $\operatorname{Ker} \phi = N$.

Usually, Method (ii) is easier. Showing well-definedness and injectivity can be tricky.

For example, Method (ii) works quite well in showing the following:

- $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$;
- $\mathbb{Q}^*/\langle -1 \rangle \cong \mathbb{Q}^+$;
- $AB/B \cong A/(A \cap B)$
- $G/(A \cap B) \cong (G/A) \times (G/B) \quad$ (if $G = AB$).

A picture of the isomorphism $\iota\colon \mathbb{Z}/\langle 12\rangle \longrightarrow \mathbb{Z}_{12}$



An example that is neither an embedding nor quotient

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

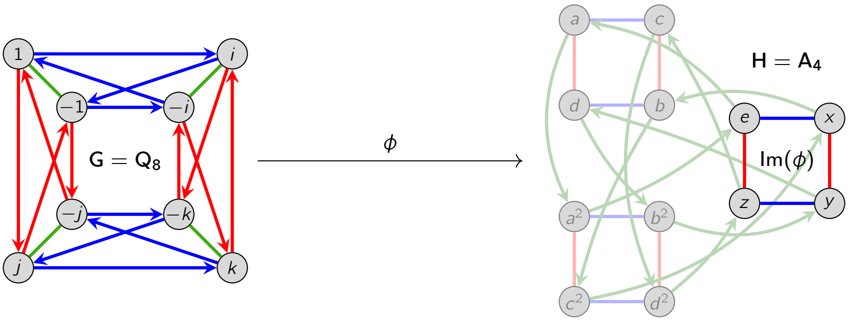
$$\phi(i) = (12)(34), \qquad \phi(j) = (13)(24).$$

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 $g = i, j, k$.

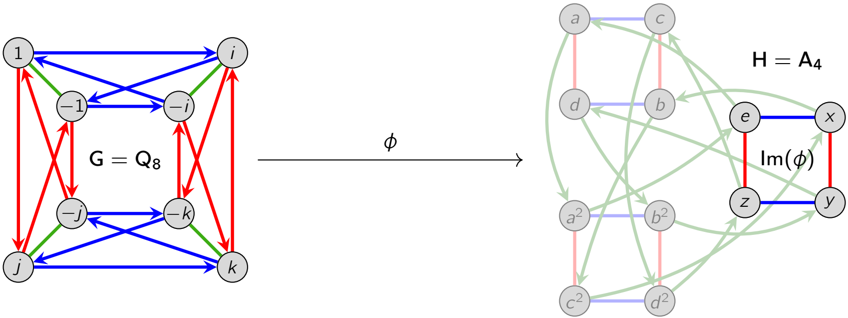


An example that is neither an embedding nor quotient

Theorem (exercise)

Every homomorphism $\phi\colon G \to H$ can be factored as a quotient and embedding:

$$\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, two heads, "\pi"'] & & H \\ & G/N \arrow[ur, hook, dashed, "\iota"'] & \end{tikzcd} \qquad \begin{tikzcd} g \arrow[rr, mapsto, "\phi"] \arrow[dr, mapsto, "\pi"'] & & \phi(g) \\ & gN \arrow[ur, mapsto, dashed, "\iota"'] & \end{tikzcd}$$



A generalization of the FHT