Isomorphism theorems!

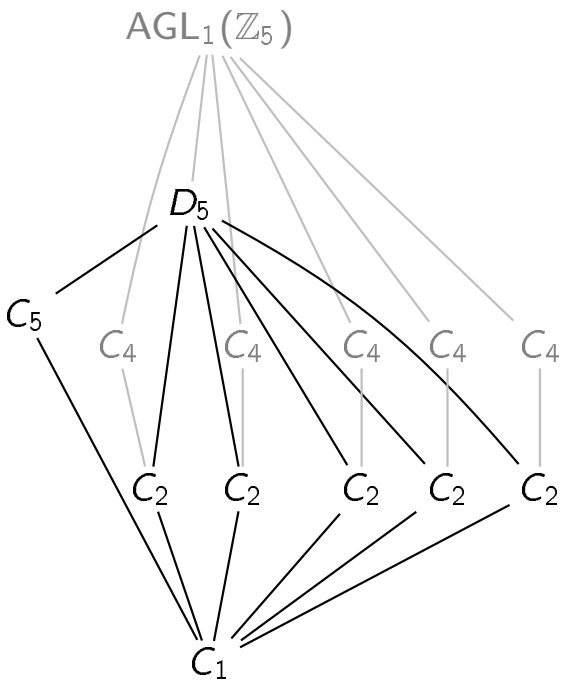
Spencer Bagley

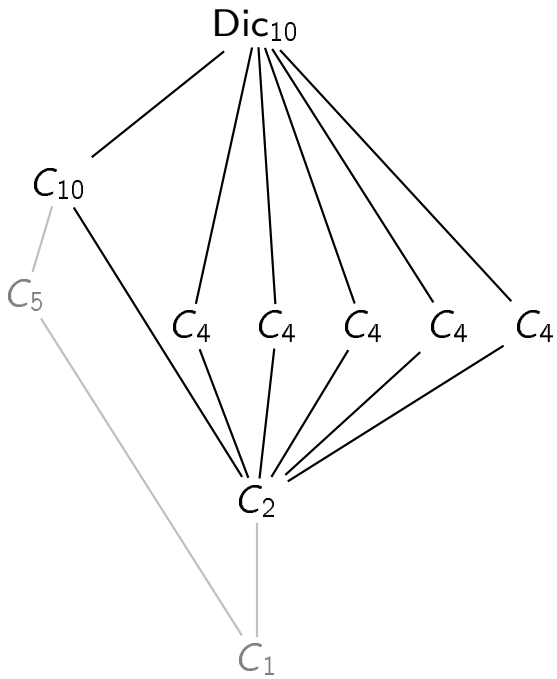
With many thanks to Matthew Macauley,
http://www.math.clemson.edu/~macaule/

31 Mar 2025

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 a subgroup, and it rises up from the floor.

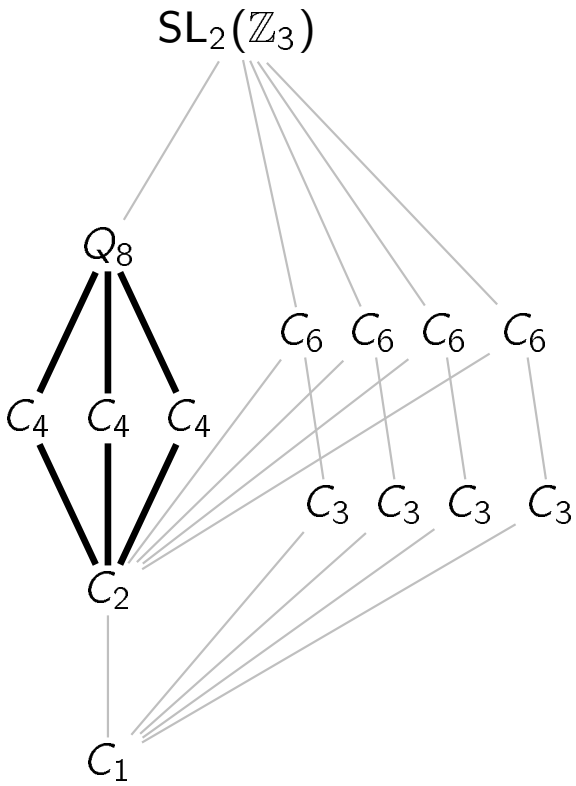
In the other, it arises as a quotient, and it descends from the ceiling.

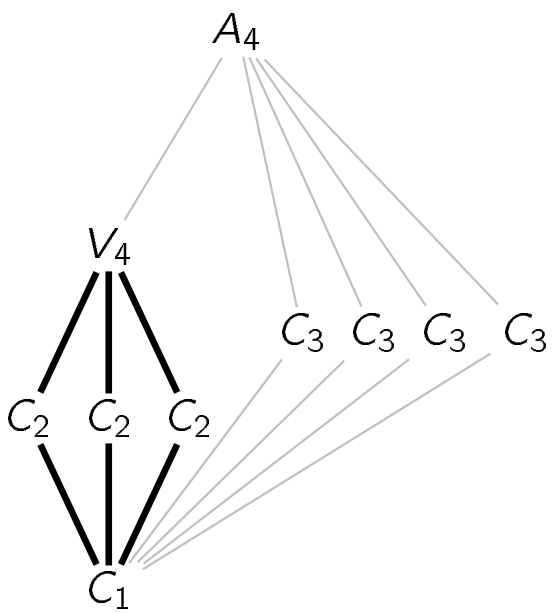
This, and much more, will be consequences of the celebrated **isomorphism theorems**.

Preview: subgroups, quotients, and subquotients

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

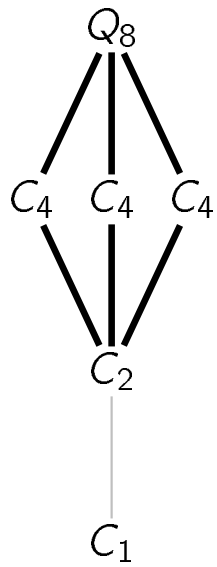
These are called **subquotients**.





subgroup of a quotient

quotient of a subgroup



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

The Fundamental Homomorphism Theorem!

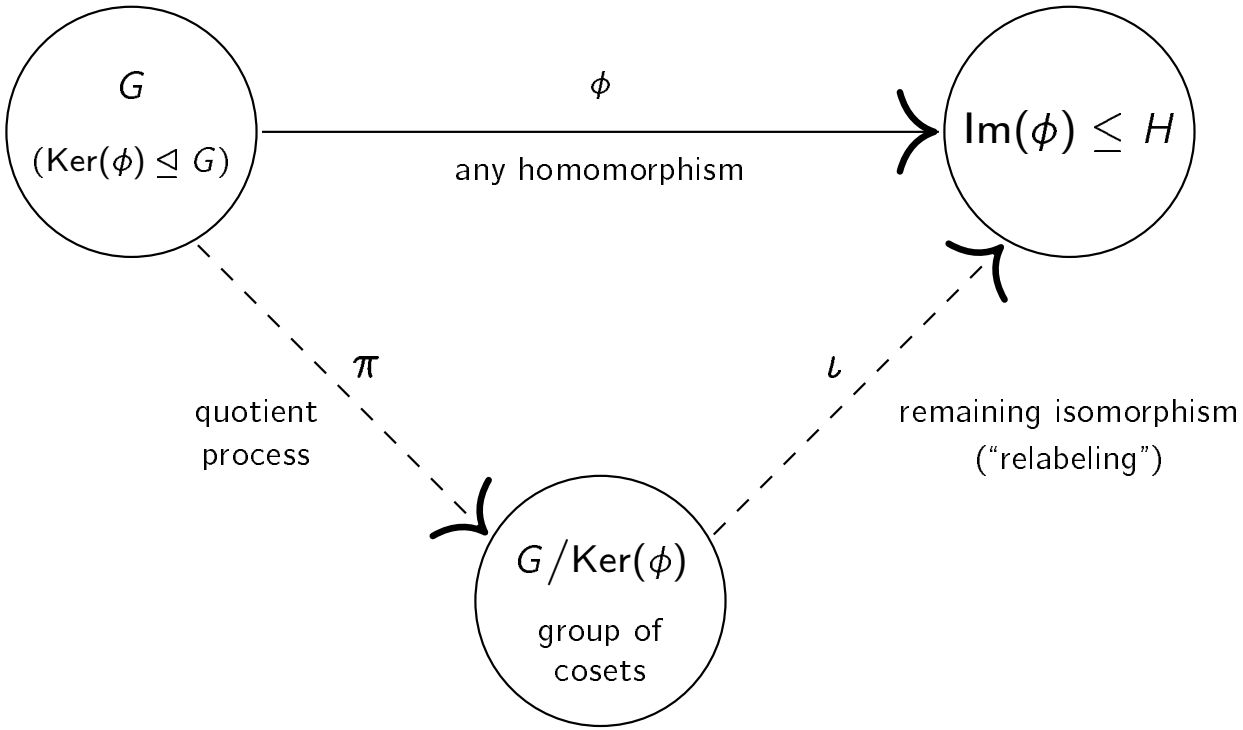
Every homomorphism image is a quotient

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

Fundamental homomorphism theorem (FHT), or Noether's isomorphism theorem

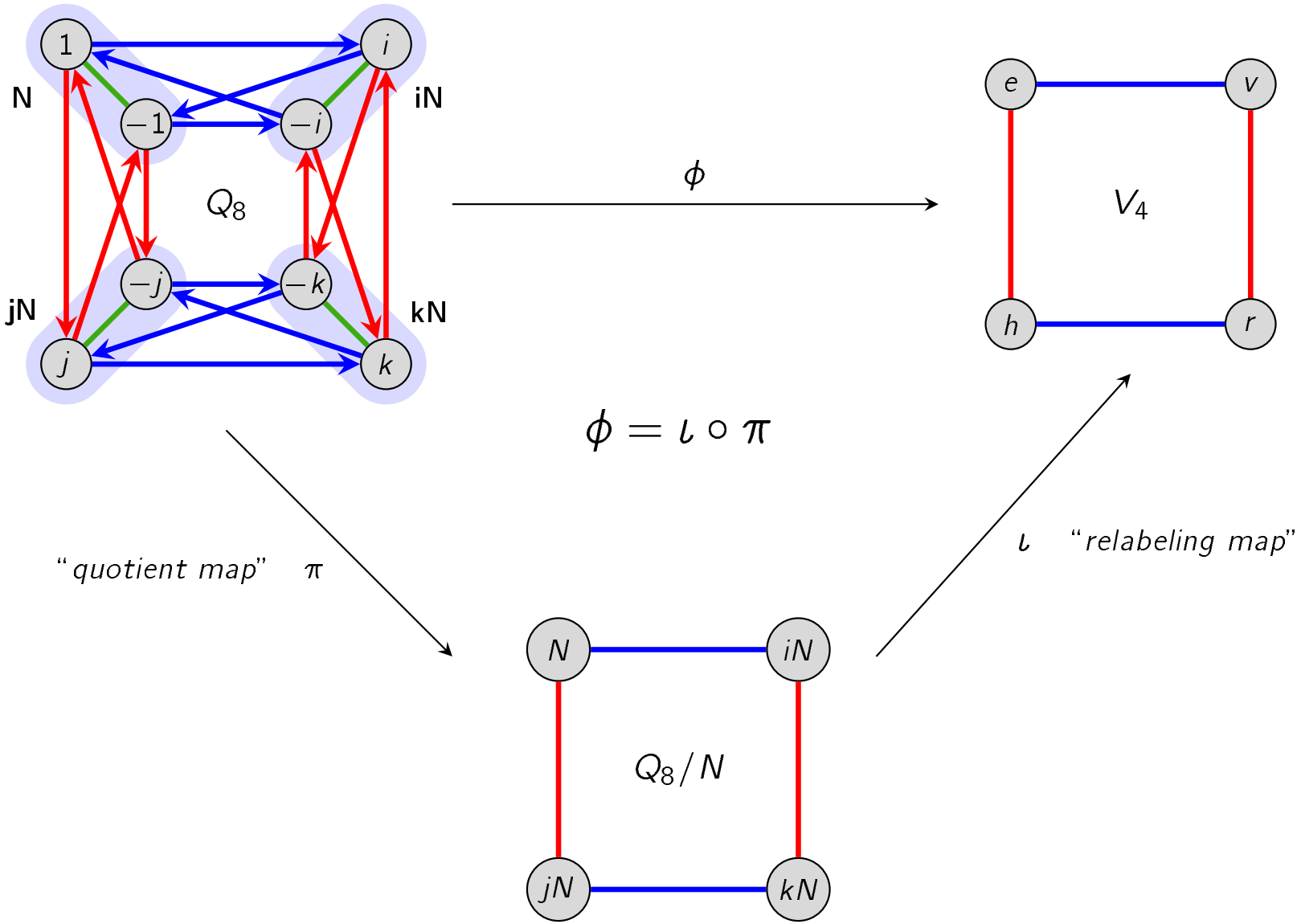
If $\phi\colon G \to H$ is a homomorphism, then $\mathsf{Im}(\phi) \cong G/\mathsf{Ker}(\phi)$.

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

(This is HW 8.14.)



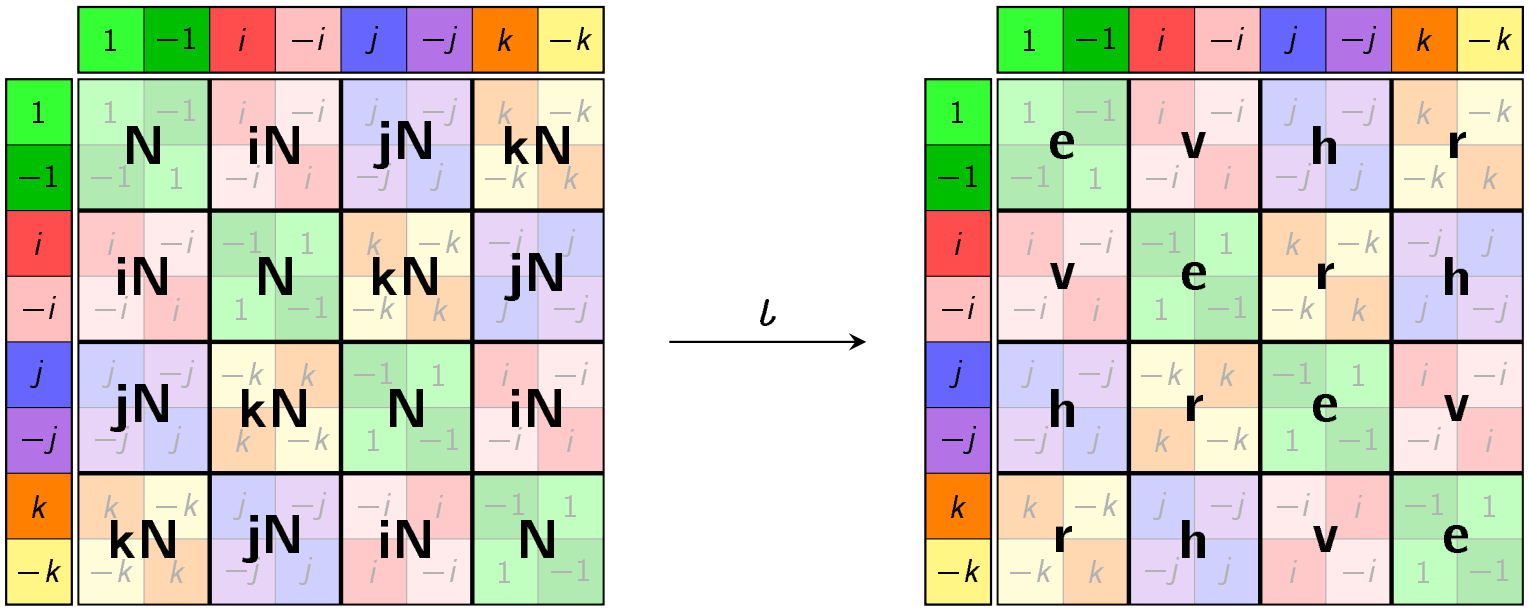
Visualizing the FHT via Cayley tables

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



FHT preliminaries

Proposition (HW 8.9)

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 $G/\mathrm{Ker}(\phi)$.

FHT preliminaries

Proposition (HW 8.10)

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

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

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

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

Proof of the FHT

Fundamental homomorphism theorem

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

Proof

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

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

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

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

Suppose $aN = bN$. We have

$$aN = bN \quad \Longrightarrow \quad b^{-1}aN = N \quad \Longrightarrow \quad b^{-1}a \in N\,.$$

By definition of $b^{-1}a \in \operatorname{Ker}(\phi)$,

$$1_H = \phi(b^{-1}a) = \phi(b^{-1})\,\phi(a) = \phi(b)^{-1}\,\phi(a) \quad \Longrightarrow \quad \phi(a) = \phi(b)\,.$$

By definition of ι: $\iota(aN) = \phi(a) = \phi(b) = \iota(bN)$. ✓

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

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. ✓

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

Proof (cont.)

- *Show ι is injective (1–1)*: We must show that $\iota(aN) = \iota(bN)$ implies $aN = bN$.

Suppose that $\iota(aN) = \iota(bN)$. Then

$$
\begin{aligned}
\iota(aN) = \iota(bN) &\implies \phi(a) = \phi(b) && \text{(by definition)} \\
&\implies \phi(b)^{-1}\phi(a) = 1_H \\
&\implies \phi(b^{-1}a) = 1_H && (\phi \text{ is a homom.}) \\
&\implies b^{-1}a \in N && (\text{definition of } \mathrm{Ker}(\phi)) \\
&\implies b^{-1}aN = N && (aH = H \iff a \in H) \\
&\implies aN = bN
\end{aligned}
$$

Thus, ι is injective. ✓

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

Therefore, $G/N \cong \mathrm{Im}(\phi)$, and the FHT is proven. □

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, ~~8~~, or ~~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

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

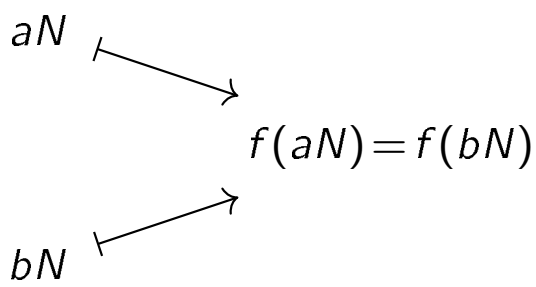
Remark

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

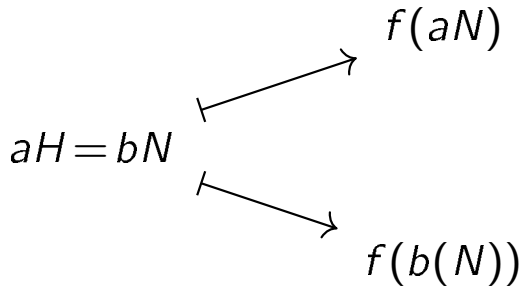
What does "well-defined" really mean?

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

- f is well-defined if the same input cannot map to different outputs
- (that is, f is a function!)
- f is injective if different inputs cannot map to the same output.



not allowed if 1-to-1



not allowed if well-defined

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

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

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.

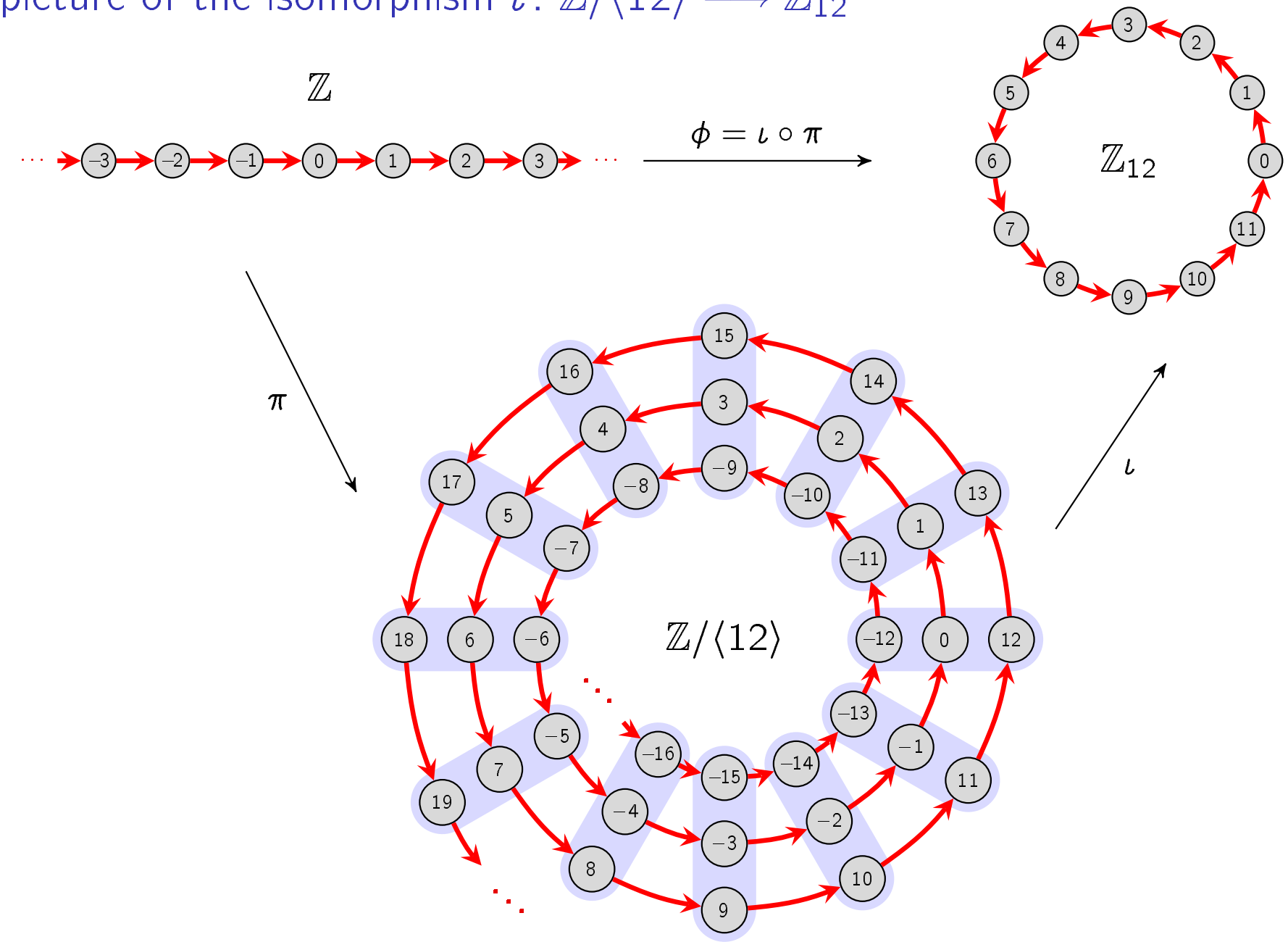
(ii) Define a map $\phi\colon G \to H$ and prove that it is a homomorphism, a surjection (onto), and that $\operatorname{Ker}\phi = N$.

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

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

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

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



The Isomorphism Theorems!

The Isomorphism Theorems

The fundamental homomorphism theorem (FHT), or Noether's isomorphism theorem, is the first of four basic theorems about homomorphisms and their structure.

These are commonly called "The Isomorphism Theorems."

- Fundamental homomorphism theorem: "*All homomorphic images are quotients*"
- Correspondence theorem or lattice theorem: Characterizes "*subgroups of quotients*"
- Fraction theorem: Characterizes "*quotients of quotients*"
- Diamond theorem: "*Duality of subquotients*."

These all have analogues for other algebraic structures, e.g., rings, vector spaces, modules, Lie algebras.

All of these theorems can look messy and unmotivated algebraically.

However, they all have beautiful visual interpretations, especially involving subgroup lattices.

For time reasons, we'll only really talk about the FHT and the lattice theorem.

The correspondence theorem: subgroups of quotients

Given $N \trianglelefteq G$, the quotient G/N has a group structure, via $aN \cdot bN = abN$.

Moreover, by the FHT, *every* homomorphism image is a quotient.

Natural question

What are the subgroups of a quotient?

Fortunately, this has a simple answer that is easy to remember.

Correspondence theorem (informal)

The subgroups of the quotient G/N are quotients of the subgroups $H \leq G$ that contain N.

Moreover, "most properties" of $H/N \leq G/N$ are inherited from $H \leq G$.

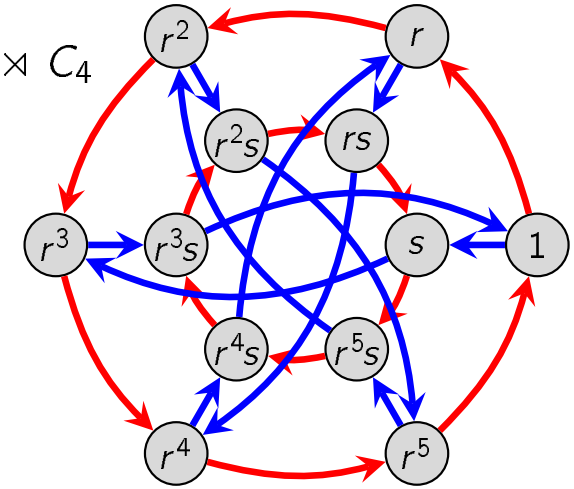
This is best understood by interpreting the subgroup lattices of G and G/N.

Let's do some examples for intuition, and then state the correspondence theorem formally.

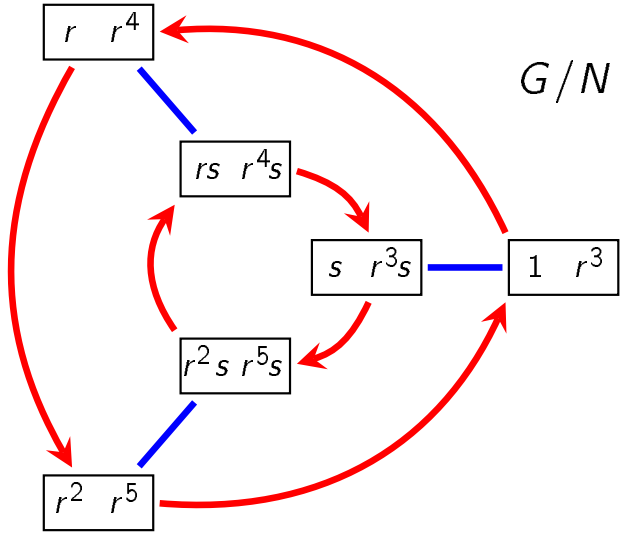
The correspondence theorem: subgroups of quotients

Compare $G = C_3 \rtimes C_4$ with the quotient by $N = \langle r^3 \rangle$. (This is HW 7.7.)

$G = C_3 \rtimes C_4$



G/N



We know the subgroups structure of $G/N = \{N,\ rN,\ r^2N,\ sN,\ rsN,\ r^2sN\} \cong D_3$.

"*The subgroups of the quotient G/N are the quotients of the subgroups that contain N.*"

"*shoes out of the box*"

r^2	r^5	r^2s	r^5s
r	r^4	rs	r^4s
1	r^3	s	r^3s

$\langle r \rangle \leq G$

"*shoeboxes; lids off*"

r^2	r^5	r^2s	r^5s
r	r^4	rs	r^4s
1	r^3	s	r^3s

$\langle r \rangle / N \leq G/N$

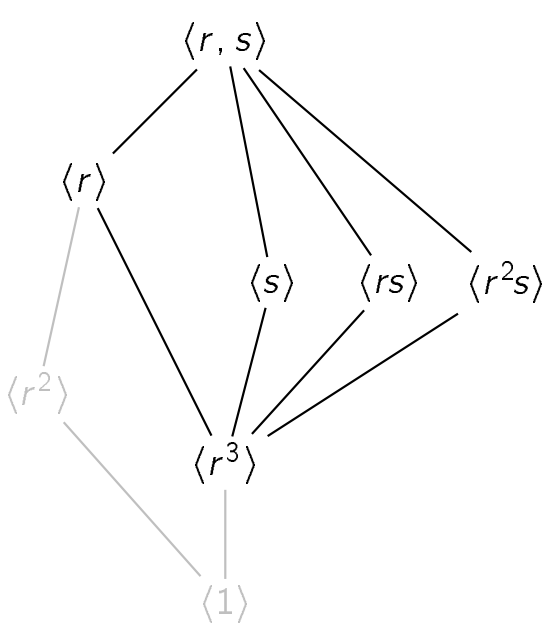
"*shoeboxes; lids on*"

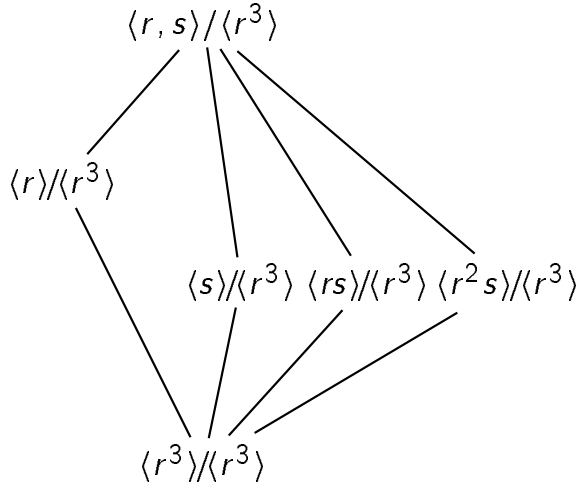
r^2N	r^2sN
rN	rsN
N	sN

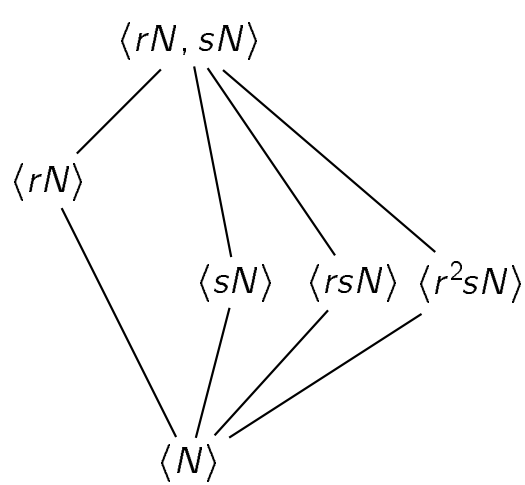
$\langle rN \rangle \leq G/N$

The correspondence theorem: subgroups of quotients

Here is the subgroup lattice of $G = C_3 \rtimes C_4$, and of the quotient G/N, where $N = \langle r^3 \rangle$.







"The subgroups of the quotient G/N are the quotients of the subgroups that contain N."

"shoes out of the box"

r^2	r^5	r^2s	r^5s
r	r^4	rs	r^4s
1	r^3	s	r^3s

$\langle s \rangle \leq G$

"shoeboxes; lids off"

r^2	r^5	r^2s	r^5s
r	r^4	rs	r^4s
1	r^3	s	r^3s

$\langle s \rangle / N \leq G/N$

"shoeboxes; lids on"

r^2N	r^2sN
rN	rsN
N	sN

$\langle sN \rangle \leq G/N$

The correspondence theorem: subgroups of quotients

Correspondence theorem (informally)

There is a bijection between subgroups of G/N and subgroups of G that contain N.

"Everything that we want to be true" about the subgroup lattice of G/N is inherited from the subgroup lattice of G.

Most of these can be summarized as:

"*The* _____ *of the quotient is just the quotient of the* _____"

Correspondence theorem (formally)

Let $N \leq H \leq G$ and $N \leq K \leq G$ be chains of subgroups and $N \trianglelefteq G$. Then

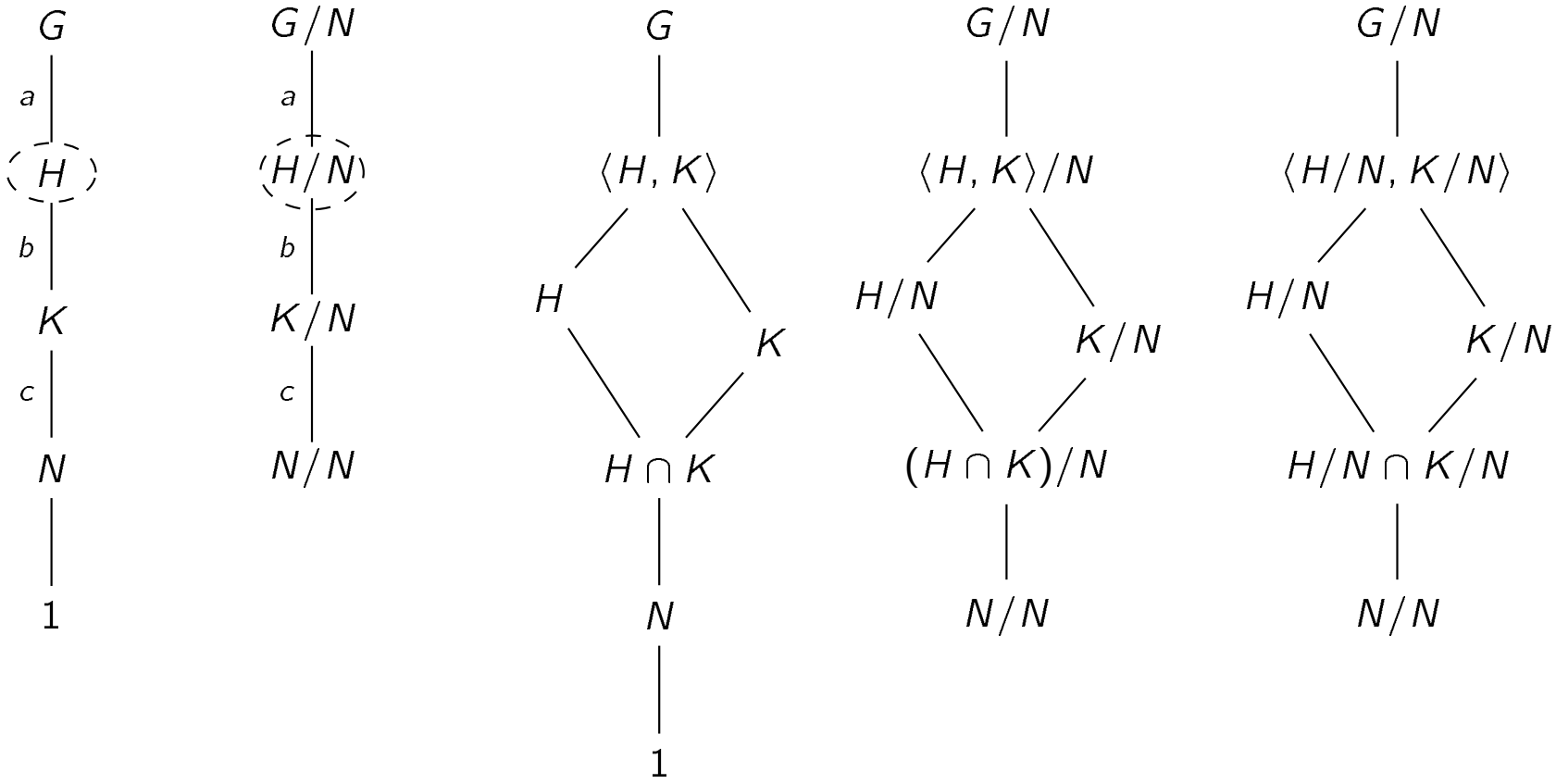
1. Subgroups of the quotient G/N are quotients of the subgroup $H \leq G$ that contain N.
2. $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$
3. $[G/N : H/N] = [G : H]$
4. $H/N \cap K/N = (H \cap K)/N$
5. $\langle H/N, K/N \rangle = \langle H, K \rangle / N$
6. H/N is conjugate to K/N in G/N iff H is conjugate to K in G.

The correspondence theorem: subgroups of quotients

All parts of the correspondence theorem have nice subgroup lattice interpretations.

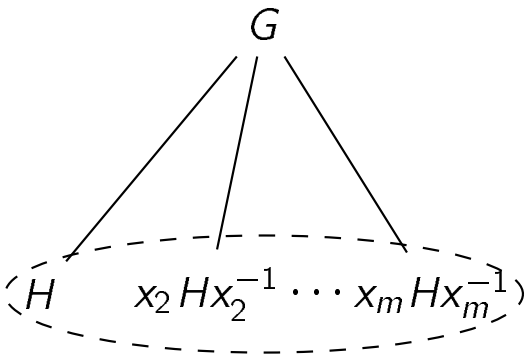
We've already interpreted the the first part.

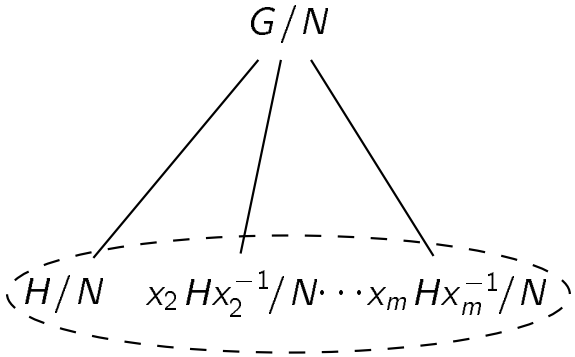
Here's what the next four parts say.



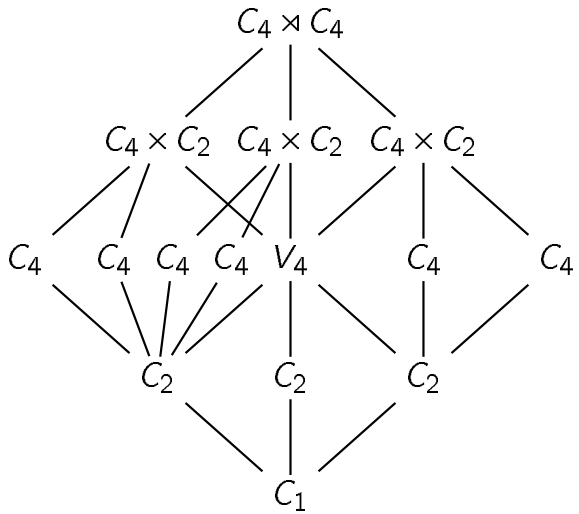
The correspondence theorem: subgroups of quotients

The last part says that we can characterize the conjugacy classes of G/N from those of G.



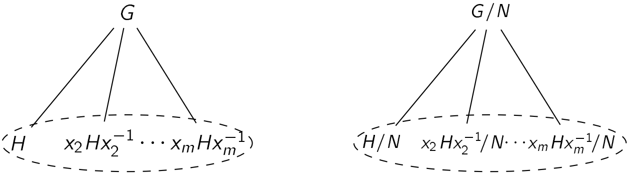


Let's apply that to find the conjugacy classes of $C_4 \rtimes C_4$ by inspection alone. Start by finding unicorns.

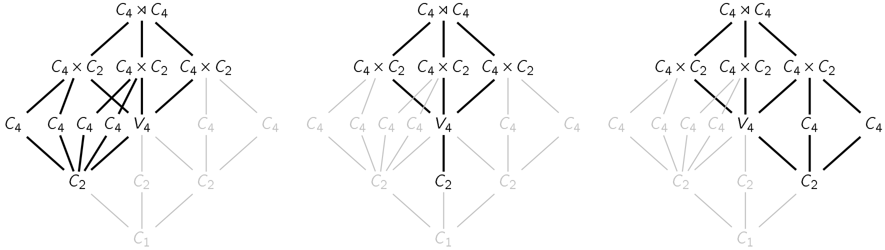


The correspondence theorem: subgroups of quotients

The last part says that we can characterize the conjugacy classes of G/N from those of G.



Let's apply that to find the conjugacy classes of $C_4 \rtimes C_4$ by inspection alone.



The correspondence theorem: subgroups of quotients

Let's prove the first (main) part of the correspondence theorem.

Correspondence theorem (first part)

The subgroups of the quotient G/N are quotients of the subgroup $H \leq G$ that contain N.

Proof

Let S be a subgroup of G/N. Then S is a collection of cosets, i.e.,

$$S = \{hN \mid h \in H\},$$

for some subset $H \subseteq G$. We just need to show that H is a subgroup.

We'll use the one-step subgroup test: take h_1N, $h_2N \in S$. Then S must also contain

$$(h_1N)(h_2N)^{-1} = (h_1N)(h_2^{-1}N) = (h_1h_2^{-1})N. \tag{1}$$

That is, $h_1h_2^{-1} \in H$, which means that H is a subgroup. ✓

Conversely, suppose that $N \leq H \leq G$. The one-step subgroup test shows that $H/N \leq G/N$; see Eq. (1). □

The other parts are straightforward and will be left as exercises.

Another fun group to play with!

Groups of matrices

Definition

Let $\mathrm{Mat}_n(\mathbb{F})$ be the set of $n \times n$ matrices with coefficients from $\mathbb{F}$.

$\mathbb{F}$ is a "field" – you can add, subtract, multiply, and divide, and everything commutes. Examples of fields?

- $\mathbb{Q}$, the rationals
- $\mathbb{R}$, the real numbers
- $\mathbb{C}$, the complex numbers
- Weirdly, $\mathbb{Z}_p$ for p a prime ("finite fields")

Careful:

$\mathrm{Mat}_n(\mathbb{F})$ is not a group under multiplication! Why not?

Definition

Thqe general linear group of degree n over $\mathbb{F}$ is the set of invertible matrices with coefficients from $\mathbb{F}$:

$$\mathrm{GL}_n(\mathbb{F}) = \{A \in \mathrm{Mat}_n(\mathbb{F}) \mid \det A \neq 0\}.$$

The special linear group is the subgroup of matrices with determinant 1:

$$\mathrm{SL}_n(\mathbb{F}) = \{A \in \mathrm{GL}_n(\mathbb{F}) \mid \det A = 1\}.$$

Groups of 2×2 matrices over $\mathbb{Z}_3$

$\mathrm{Mat}_2(\mathbb{Z}_3)$

Give an example of:

- a 2×2 matrix
- whose elements are all in $\mathbb{Z}_3$.

$\mathrm{GL}_2(\mathbb{Z}_3)$ (or you might see $\mathrm{GL}(2, \mathbb{Z}_3)$)

Give an example of:

- a 2×2 matrix
- whose elements are all in $\mathbb{Z}_3$
- and whose determinant is nonzero.

$\mathrm{SL}_2(\mathbb{Z}_3)$ aka $\mathrm{SL}(2, \mathbb{Z}_3)$

Give an example of:

- a 2×2 matrix
- whose elements are all in $\mathbb{Z}_3$
- and whose determinant is nonzero
- and whose determinant is specifically 1.

$\mathsf{SL}(2, \mathbb{Z}_3)$

How many matrices are there in $\mathsf{SL}(2, \mathbb{Z}_3)$?

Here are two good ones to play with:

$$a = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$$

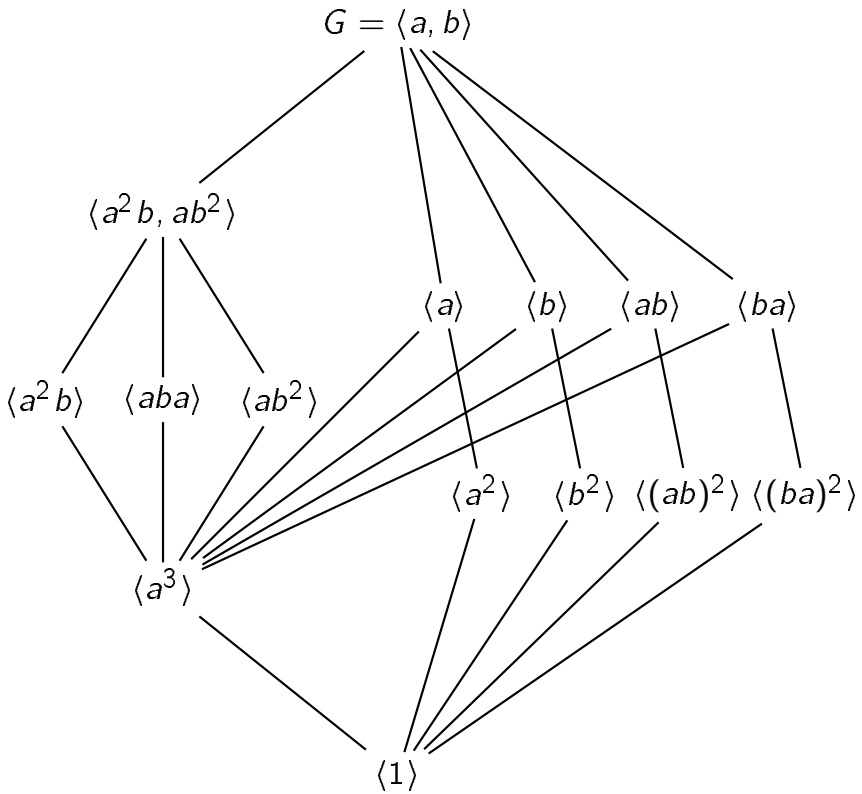
$$b = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$$

The "subgroup" and "quotient" operations commute

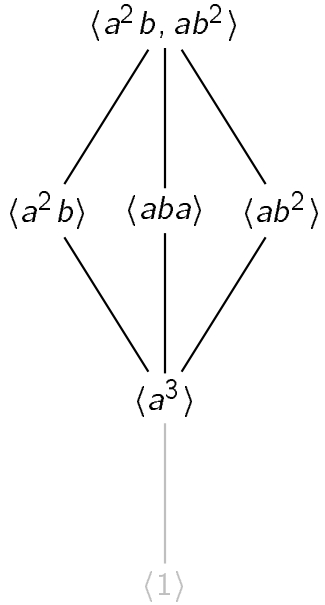
Key idea

The quotient of a subgroup is just the subgroup of the quotient.

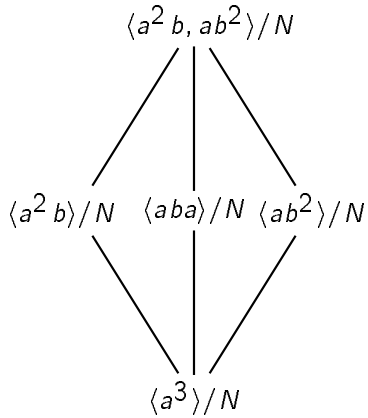
Example: Consider the group $G = \mathsf{SL}_2(\mathbb{Z}_3)$.



subgroup $\mathbf{H \cong Q_8}$



$\mathbf{H/N \cong V_4}$



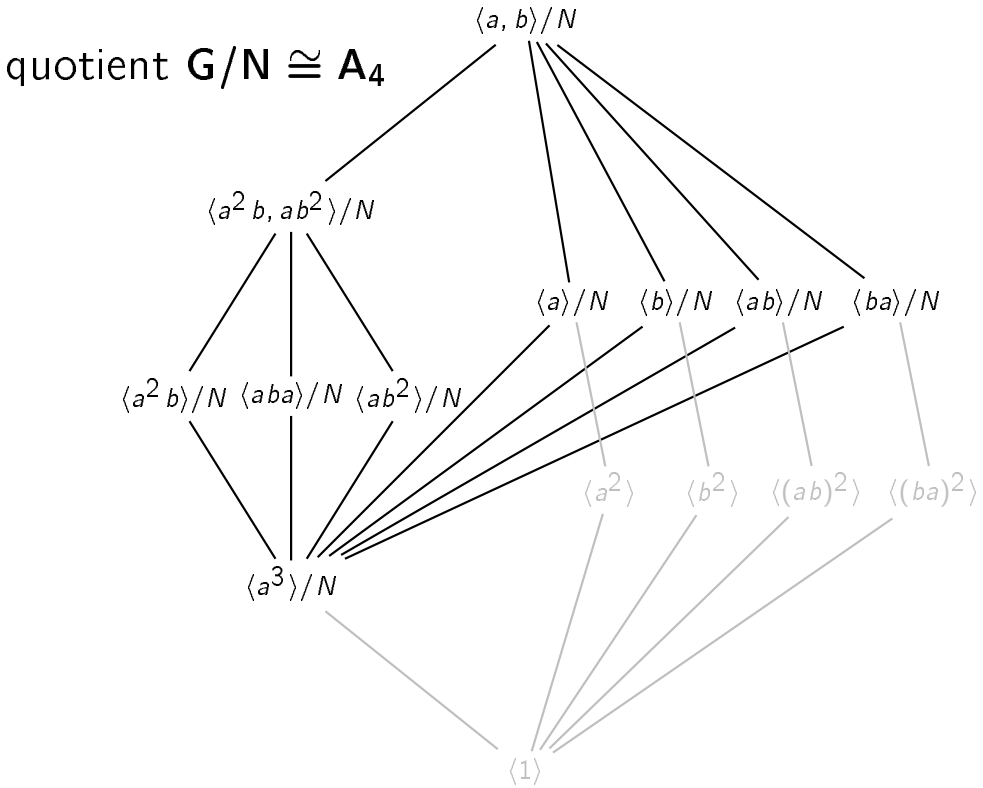
"quotient of the subgroup"

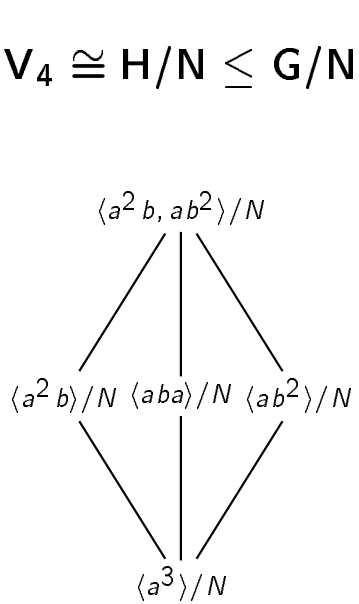
The "subgroup" and "quotient" operations commute

Key idea

The quotient of a subgroup is just the subgroup of the quotient.

Example: Consider the group $G = \mathrm{SL}_2(\mathbb{Z}_3)$.





"subgroup of the quotient"