

Chapter 4: Maps between groups

Matthew Macauley

Department of Mathematical Sciences
Clemson University

<http://www.math.clemson.edu/~macaule/>

Math 4120 & 4130, Visual Algebra

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 $\phi: G \rightarrow H$ 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 $\phi: G \rightarrow G$.

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

The homomorphism $\phi: G \rightarrow H$ is an

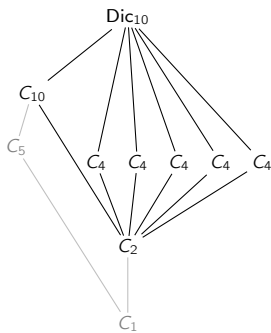
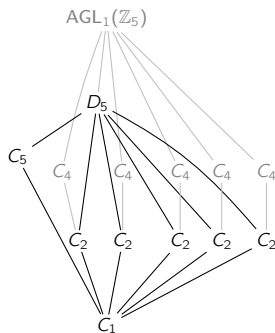
- **embedding** if ϕ is one-to-one: “ G is a **subgroup** of H .”

- **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* $\phi = \pi \circ \iota$ of an embedding with a quotient.

Preview: embeddings vs. quotients

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



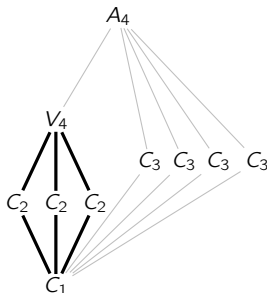
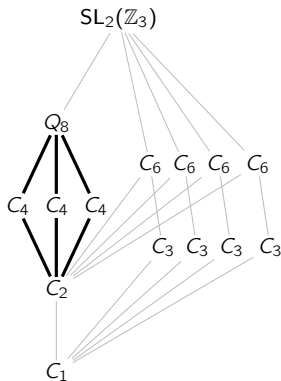
In one of these groups, D_5 is **subgroup**. In the other, it arises as a **quotient**.

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

Preview: subgroups, quotients, and subquotients

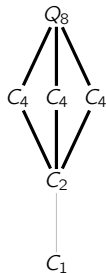
Often, we'll see familiar subgroup lattices in the middle of a larger lattice.

These are called **subquotients**.



subgroup of a quotient

quotient of a subgroup

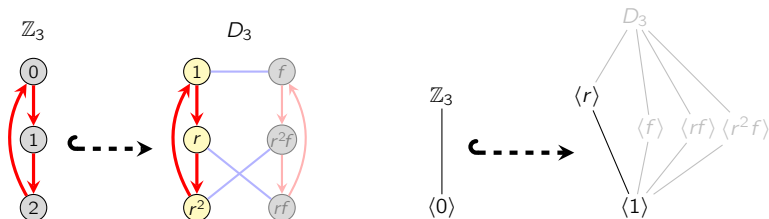


The *isomorphism theorems* relates the structure of a group to that of its quotients and subquotients.

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 $\phi: \mathbb{Z}_3 \rightarrow D_3$, defined by $\phi: n \mapsto r^n$.



In general, a homomorphism is a function $\phi: G \rightarrow H$ 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*:

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

The formal definition

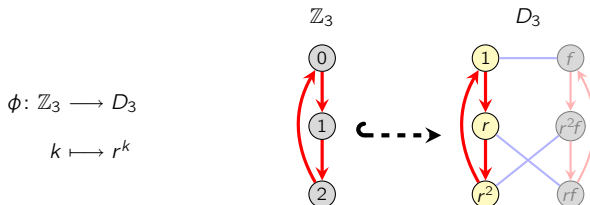
Definition

A **homomorphism** is a function $\phi: G \rightarrow H$ between two groups satisfying

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

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?)



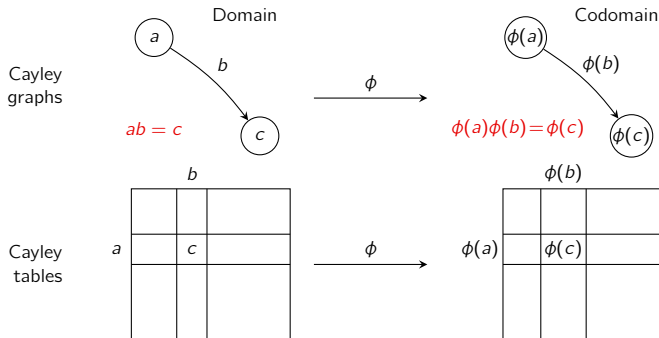
Not only is there a bijective correspondence between the elements in \mathbb{Z}_3 and those in the subgroup $\langle r \rangle$ of D_3 , but the **relationship** between the corresponding nodes is the same.

Homomorphisms

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

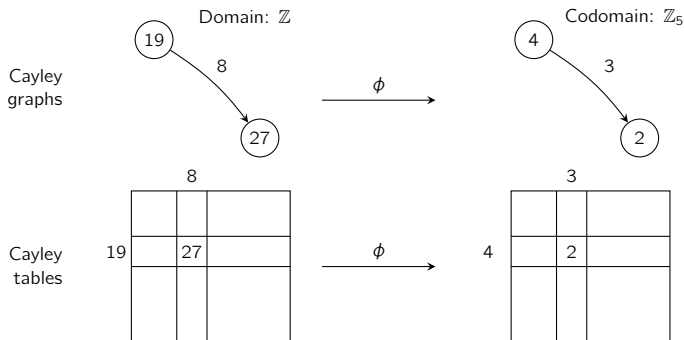
Consider the function ϕ that reduces an integer modulo 5:

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

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 $\phi: \mathbb{Z}_3 \rightarrow \mathbb{Z}_6$ 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 $\phi: G \rightarrow H$, and we know $\phi(a)$ and $\phi(b)$. We can find the image of any $g \in G$. For example, for $g = a^3b^2ab$,

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

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 $\phi: G \rightarrow H$:

- (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 $\phi(g^{-1}) = \phi(g)^{-1}$. ✓

A word of caution

Just because a homomorphism $\phi: G \rightarrow H$ 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 $\phi: \mathbb{Z}_3 \rightarrow \mathbb{Z}_4$ 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 $\phi: \mathbb{Z}_3 \rightarrow \mathbb{Z}_4$; note that there is always the **trivial homomorphism** between two groups:

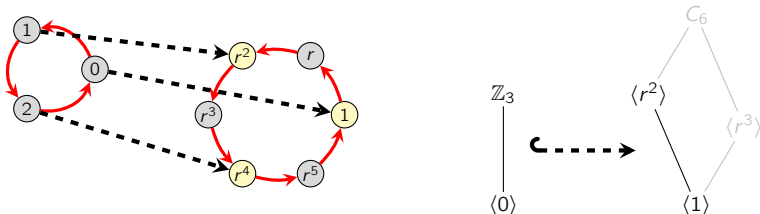
$$\phi: G \longrightarrow H, \quad \phi(g) = 1_H \quad \text{for all } g \in G.$$

Exercise

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

Types of homomorphisms

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

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

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 $\phi: Q_8 \rightarrow A_4$ defined by

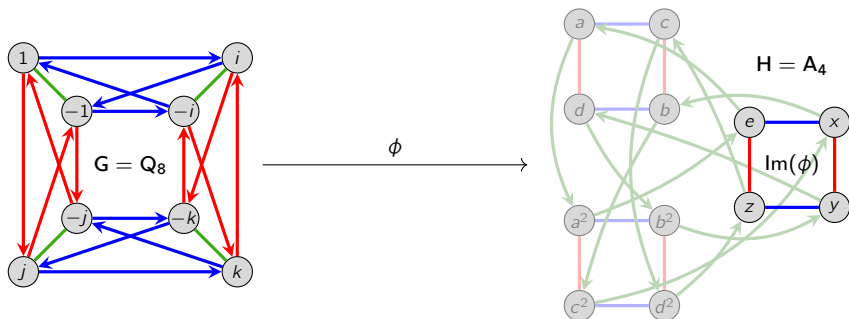
$$\phi(i) = (12)(34), \quad \phi(j) = (13)(24).$$

Using the property of homomorphisms,

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

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

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 .

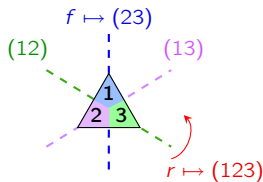
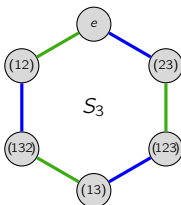
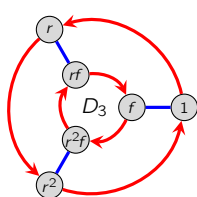
This means that there's a bijective correspondence $f: D_3 \rightarrow S_3$.

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:

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



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

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

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

For example, the following 8 matrices form a 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 $\phi: Q_8 \hookrightarrow \mathrm{GL}_4(\mathbb{R})$ where

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

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

Kernels and quotient maps

If $\phi: G \rightarrow H$ is onto, it is a **quotient map**.

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

Definition

The **kernel** of a homomorphism $\phi: G \rightarrow H$ 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 $\phi: G \rightarrow H$ 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:

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

Note that

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

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

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

$$\text{Ker}(\phi) = \phi^{-1}(1) = \langle r \rangle \quad (\text{"rotations"}),$$

$$\phi^{-1}(-1) = f\langle r \rangle \quad (\text{"reflections"}).$$

An example of a quotient

Define the homomorphism

$$\phi: Q_8 \twoheadrightarrow V_4, \quad \phi(i) = v, \quad \phi(j) = h.$$

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

$$\phi(1) = e$$

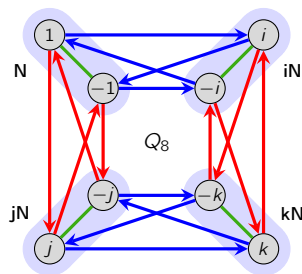
$$\phi(-1) = \phi(i^2) = \phi(i)^2 = v^2 = e$$

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

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

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

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



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

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

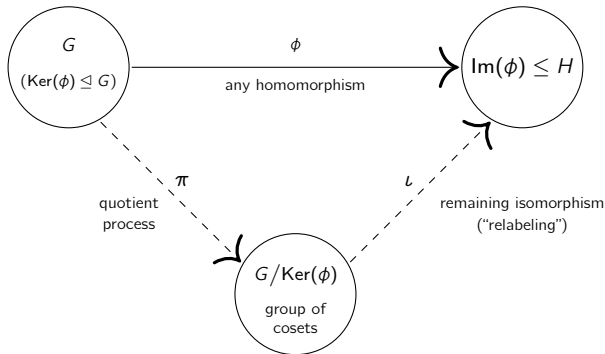
Every homomorphic image is a quotient

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

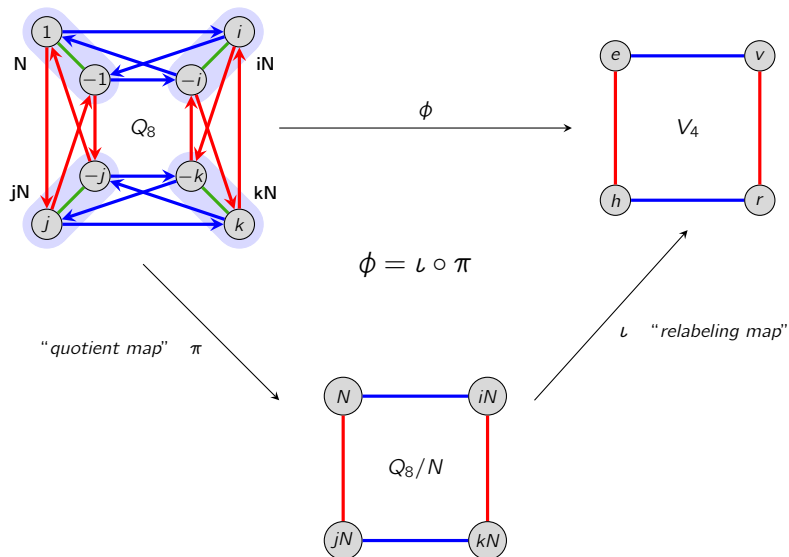
Fundamental homomorphism theorem (FHT)

If $\phi: G \rightarrow H$ is a homomorphism, then $\text{Im}(\phi) \cong G / \text{Ker}(\phi)$.

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



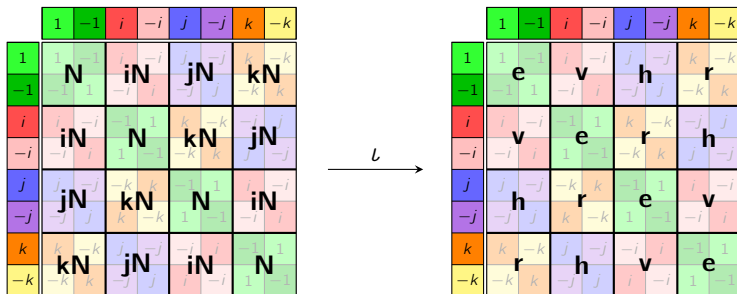
Visualizing the FHT via Cayley tables

Here's another way to think about the homomorphism

$$\phi: Q_8 \twoheadrightarrow V_4, \quad \phi(i) = v, \quad \phi(j) = h$$

as the composition of:

- a quotient by $N = \text{Ker}(\phi) = \langle -1 \rangle = \{\pm 1\}$,
- a relabeling map $\iota: Q_8/N \rightarrow V_4$.



Proposition

The **kernel** of any homomorphism $\phi: G \rightarrow H$, is a **normal subgroup**.

Proof

Let $N := \text{Ker}(\phi)$. 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, $gng^{-1} \in \text{Ker}(\phi)$. □

Key observation

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

Proposition

Let $\phi: G \rightarrow H$ be a homomorphism. Then each **preimage** $\phi^{-1}(h)$ is a **coset** of $\text{Ker}(\phi)$.

Proof

Let $N = \text{Ker}(\phi)$ 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

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

✓

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

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

✓

Proof of the FHT

Fundamental homomorphism theorem

If $\phi: G \rightarrow H$ is a homomorphism, then $\text{Im}(\phi) \cong G / \text{Ker}(\phi)$.

Proof

We'll construct an explicit map $\iota: G / \text{Ker}(\phi) \rightarrow \text{Im}(\phi)$ and prove that it's an isomorphism.

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

$$\iota: G/N \longrightarrow \text{Im}(\phi), \quad \iota: gN \longmapsto \phi(g).$$

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

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

- Show ι is injective (1-1): $[\iota(aN) = \iota(bN) \Rightarrow aN = bN.]$ Replace each \implies with \iff . \checkmark

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

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

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

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

Consequences of the FHT

Corollary

If $\phi: G \rightarrow H$ is a homomorphism, then $\text{Im}(\phi) \leq H$.

The two “extreme cases”

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

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

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

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

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

By the FHT, $C_3/\text{Ker}(\phi) \cong \text{Im}(\phi) \leq C_4$, and so

$$\underbrace{|\text{Im}(\phi)|}_{1, 2, \text{ or } 4} = |C_3/\text{Ker}(\phi)| = \underbrace{3/|\text{Ker}(\phi)|}_{1 \text{ or } 3}.$$

Therefore, $|\text{Im}(\phi)| = 1$, and so the *only* homomorphism $\phi: C_3 \rightarrow C_4$ is trivial.

Consequences of the FHT

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

By the FHT,

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

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

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

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

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** $\iota: G/N \rightarrow H$ 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 $\iota: G/N \rightarrow H$, where $\iota(aN) = \phi(a)$, is a **well-defined homomorphism**, meaning that

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

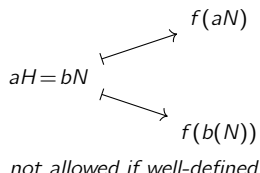
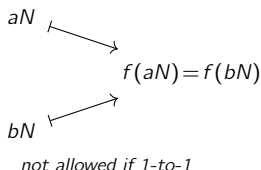
Remark

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.



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

$$\iota: G/N \rightarrow H, \quad \iota(aN) = \phi(a), \quad \text{where } N = \text{Ker}(\phi).$$

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** $\phi: G \rightarrow H$.

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:

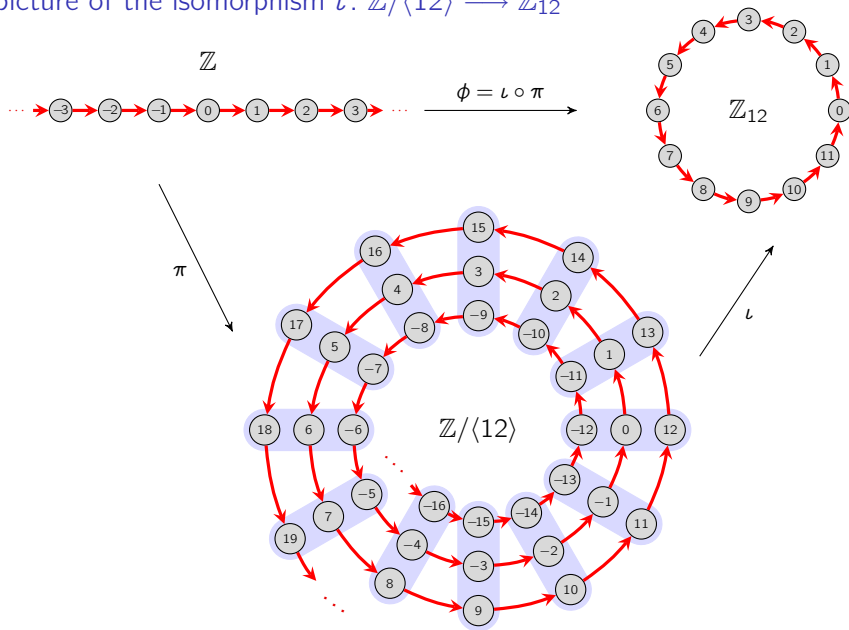
- (i) Define a map $\phi: G/N \rightarrow H$ and prove that it is **well-defined**, a **homomorphism**, and a **bijection**.
- (ii) Define a map $\phi: G \rightarrow H$ and prove that it is a **homomorphism**, a **surjection** (onto), and that **$\text{Ker } \phi = N$** .

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 $\iota: \mathbb{Z}/\langle 12 \rangle \longrightarrow \mathbb{Z}_{12}$



The Isomorphism Theorems

The fundamental homomorphism theorem (FHT) 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:** 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.

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 homomorphic 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 .

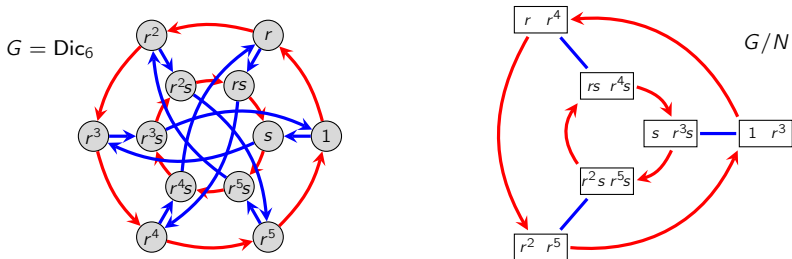
Moreover, “most properties” of $H/N \leq G/N$ are inherited from $H \leq G$.

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 $G = \text{Dic}_6$ with the quotient by $N = \langle r^3 \rangle$.



We know the subgroup 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

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

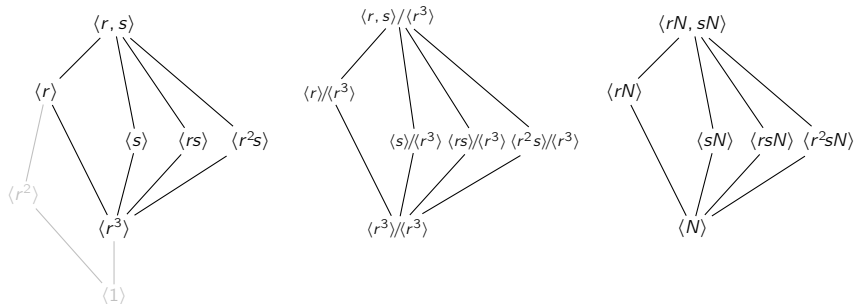
"shoeboxes; lids on"

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 $G = \text{Dic}_6$, 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

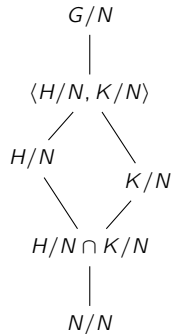
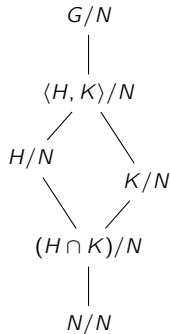
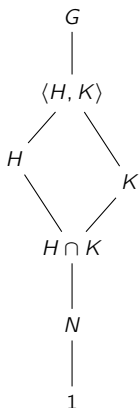
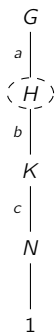
1. Subgroups of the quotient G/N are quotients of subgroups $H \leq G$ that contain N .
2. $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$
3. $[G/N : H/N] = [G : H]$
4. $H/N \cap K/N = (H \cap K)/N$
5. $\langle H/N, K/N \rangle = \langle H, K \rangle / N$
6. H/N is conjugate to K/N in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

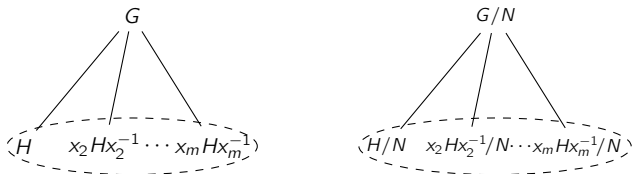
We've already interpreted the first part.

Here's what the next four parts say.

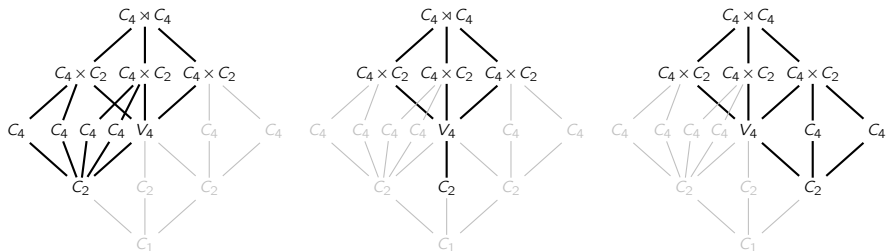


The correspondence theorem: subgroups of quotients

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.



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 subgroups $H \leq G$ 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 **1-step subgroup test**: take $h_1, h_2 \in H$. Then S contain h_1N, h_2N , and

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

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.

The quotient $G/Z(G)$ can *never* be a nontrivial cyclic subgroup

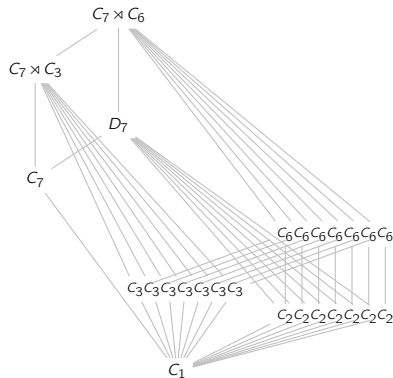
Lemma (exercise; see images below)

If $G/Z(G)$ is cyclic, then G is abelian.

$$G/Z(G) = \langle gZ \rangle, \text{ where } Z = Z(G)$$

$\bullet g^{n-1}$	$\bullet g^{n-1}z_1$	$\bullet g^{n-1}z_2$	$\bullet g^{n-1}z_3$	\dots	$\bullet g^{n-1}Z$
\vdots					
$\bullet g^2$	$\bullet g^2z_1$	$\bullet g^2z_2$	$\bullet g^2z_3$	\dots	$\bullet g^2Z$
$\bullet g$	$\bullet gz_1$	$\bullet gz_2$	$\bullet gz_3$	\dots	$\bullet gZ$
$\bullet e$	$\bullet z_1$	$\bullet z_2$	$\bullet z_3$	\dots	$\bullet Z$

Note that if G is abelian, then $Z(G) = G$.



Corollary

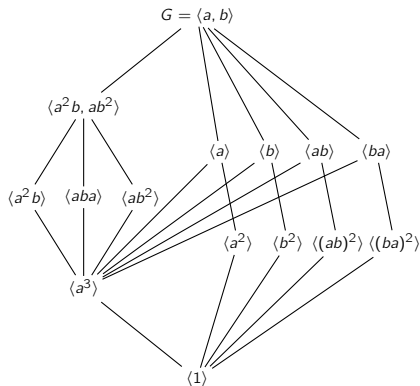
For any group G , finite or infinite, $[G : Z(G)] \geq 4$.

The “subgroup” and “quotient” operations commute

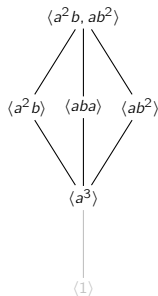
Key idea

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

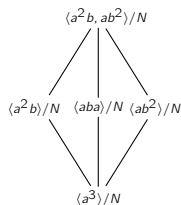
Example: Consider the group $G = \mathrm{SL}_2(\mathbb{Z}_3)$.



subgroup $H \cong Q_8$



$H/N \cong V_4$



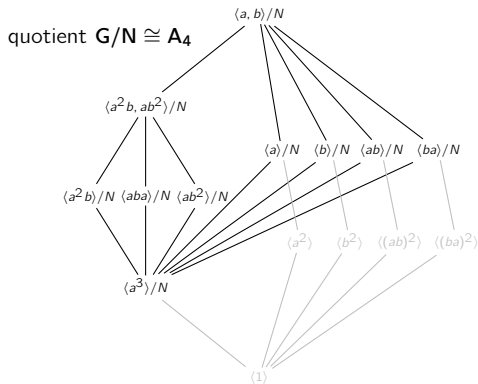
“quotient of the subgroup”

The “subgroup” and “quotient” operations commute

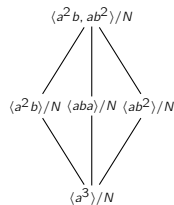
Key idea

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

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



$$V_4 \cong H/N \leq G/N$$



“subgroup of the quotient”

The fraction theorem: quotients of quotients

The correspondence theorem characterizes the **subgroup structure** of the quotient G/N .

Every subgroup of G/N is of the form H/N , where $N \leq H \leq G$.

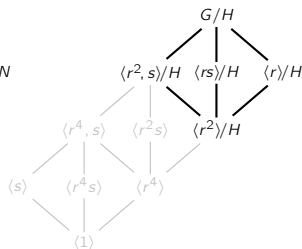
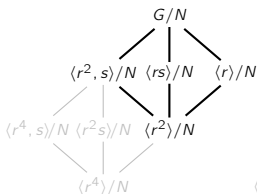
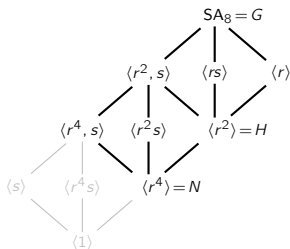
Moreover, if $H \trianglelefteq G$, then $H/N \trianglelefteq G/N$. In this case, we can ask:

What is the quotient group $(G/N)/(H/N)$ isomorphic to?

Fraction theorem

Given a chain $N \leq H \leq G$ of normal subgroups of G ,

$$(G/N)/(H/N) \cong G/H.$$

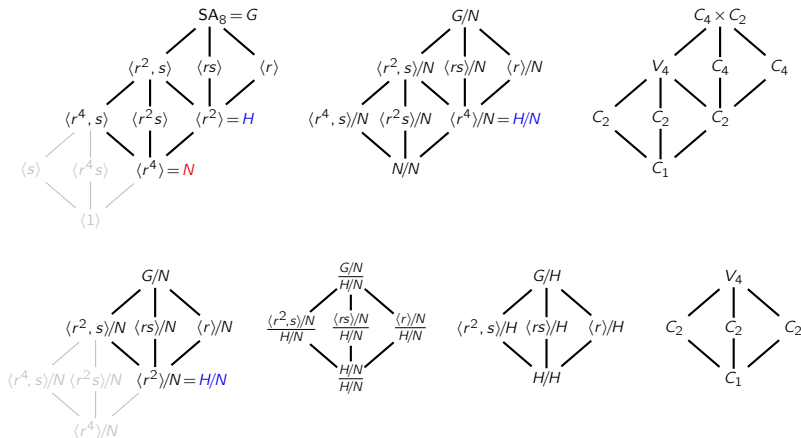


The fraction theorem: quotients of quotients

Fraction theorem

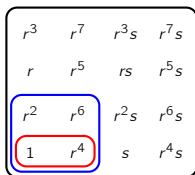
Given a chain $N \leq H \leq G$ of normal subgroups of G ,

$$(G/N)/(H/N) \cong G/H.$$

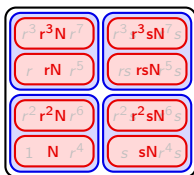


The fraction theorem: quotients of quotients

Let's continue our example of the semiabelian group $G = \text{SA}_8 = \langle r, s \rangle$.

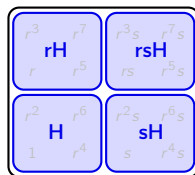


$$N \leq H \leq G$$



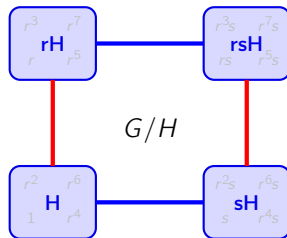
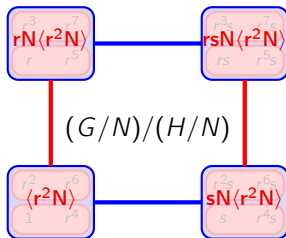
$$G/N = \langle rN, sN \rangle \cong C_4 \times C_2$$

$$H/N = \langle r^2N \rangle = \{N, r^2N\} \cong C_2$$



$$G/H = \langle rH, sH \rangle \cong V_4$$

$$(G/N)/(H/N) \cong G/H$$



The fraction theorem: quotients of quotients

Fraction theorem

Given a chain $N \leq H \leq G$ of normal subgroups of G ,

$$(G/N)/(H/N) \cong G/H.$$

Proof

This is tailor-made for the FHT. Define the map

$$\phi: G/N \longrightarrow G/H, \quad \phi: gN \longmapsto gH.$$

- Show ϕ is well-defined: Suppose $g_1N = g_2N$. Then $g_1 = g_2n$ for some $n \in N$. But $n \in H$ because $N \leq H$. Thus, $g_1H = g_2H$, i.e., $\phi(g_1N) = \phi(g_2N)$. ✓
- ϕ is clearly onto and a homomorphism. ✓
- Apply the FHT:

$$\begin{aligned} \text{Ker}(\phi) &= \{gN \in G/N \mid \phi(gN) = H\} \\ &= \{gN \in G/N \mid gH = H\} \\ &= \{gN \in G/N \mid g \in H\} = H/N \end{aligned}$$

By the FHT, $(G/N)/\text{Ker}(\phi) = (G/N)/(H/N) \cong \text{Im}(\phi) = G/H$. □

The fraction theorem: quotients of quotients

For another visualization, consider $G = \mathbb{Z}_6 \times \mathbb{Z}_4$ and write elements as strings.

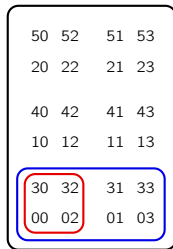
Consider the subgroups $N = \langle 30, 02 \rangle \cong V_4$ and $H = \langle 30, 01 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

Notice that $N \leq H \leq G$, and $H = N \cup (01+N)$, and

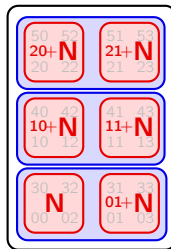
$$G/N = \{N, 01+N, 10+N, 11+N, 20+N, 21+N\}, \quad H/N = \{N, 01+N\}$$

$$G/H = \{N \cup (01+N), (10+N) \cup (11+N), (20+N) \cup (21+N)\}$$

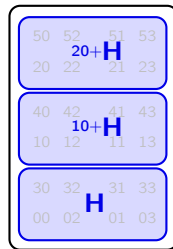
$$(G/N)/(H/N) = \{\{N, 01+N\}, \{10+N, 11+N\}, \{20+N, 21+N\}\}.$$



$N \leq H \leq G$



G/N consists of 6 cosets
 $H/N = \{N, 01+N\}$



G/H consists of 3 cosets
 $(G/N)/(H/N) \cong G/H$

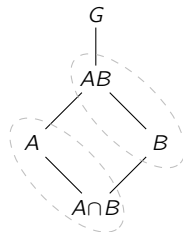
The diamond theorem: duality of subquotients

Diamond theorem

Suppose $A, B \leq G$, and that A normalizes B . Then

- (i) $A \cap B \trianglelefteq A$ and $B \trianglelefteq AB$.
- (ii) The following quotient groups are isomorphic:

$$AB/B \cong A/(A \cap B)$$



Proof (sketch)

Define the following map

If we can show: $\phi: A \longrightarrow AB/B, \quad \phi: a \longmapsto aB.$

- 1. ϕ is a homomorphism,
- 2. ϕ is surjective (onto),
- 3. $\text{Ker}(\phi) = A \cap B$,

then the result will follow *immediately* from the FHT. The details are left as HW.

Corollary

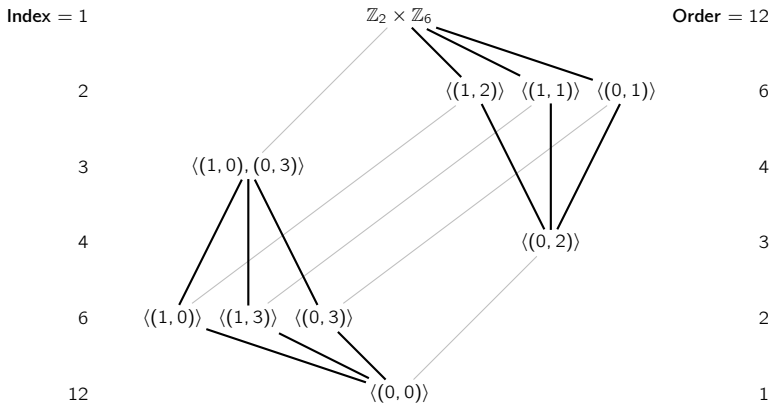
Let $A, B \leq G$, with one of them normalizing the other. Then $|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$

The diamond theorem: duality of subquotients

Let $G = \mathbb{Z}_2 \times \mathbb{Z}_6$, and consider subgroups $A = \langle (1, 0), (0, 3) \rangle$, and $B = \langle (0, 2) \rangle$.

Then $G = AB$, and $A \cap B = \langle (0, 0) \rangle$.

Let's interpret the diamond theorem $AB/B \cong A/A \cap B$ in terms of the subgroup lattice.

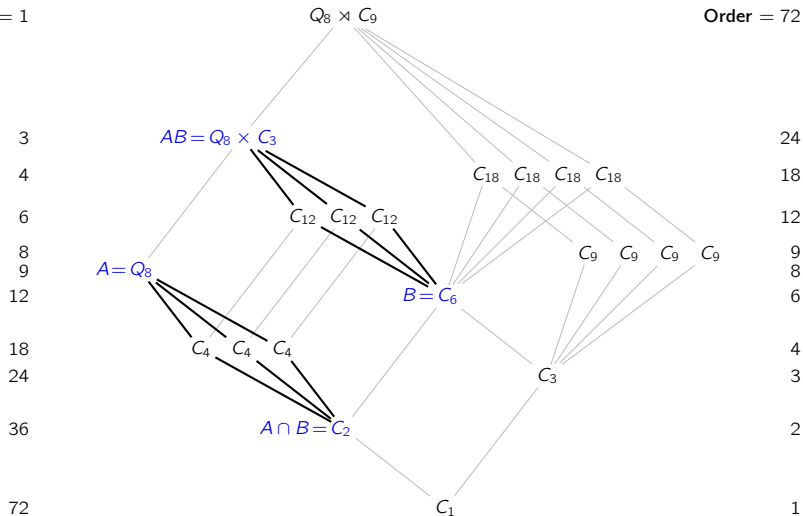


The fact that the subgroup lattice of V_4 is diamond shaped is coincidental.

The diamond theorem: duality of subquotients

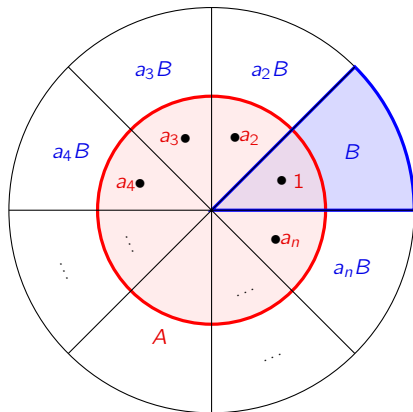
Index = 1

Order = 72



The diamond theorem illustrated by a “pizza diagram”

The following analogy is due to Douglas Hofstadter:



AB = large pizza

A = small pizza

B = large pizza slice

$A \cap B$ = small pizza slice

$AB/B = \{\text{large pizza slices}\}$

$A/(A \cap B) = \{\text{small pizza slices}\}$

Diamond theorem: $AB/B \cong A/(A \cap B)$

The diamond theorem: duality of subquotients

Proposition

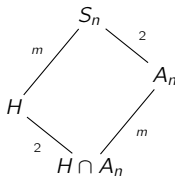
Suppose H is a subgroup of S_n that is not contained in A_n . Then exactly half of the permutations in H are even.

Index = 1

2

m

$2m$



Order = $n!$

$n!/2$

$n!/m$

$n!/2m$

Proof

It suffices to show that $[H : H \cap A_n] = 2$, or equivalently, that $H/(H \cap A_n) \cong C_2$.

Since $H \not\subseteq A_n$, the product HA_n must be strictly larger, and so $HA_n = S_n$.

By the diamond theorem,

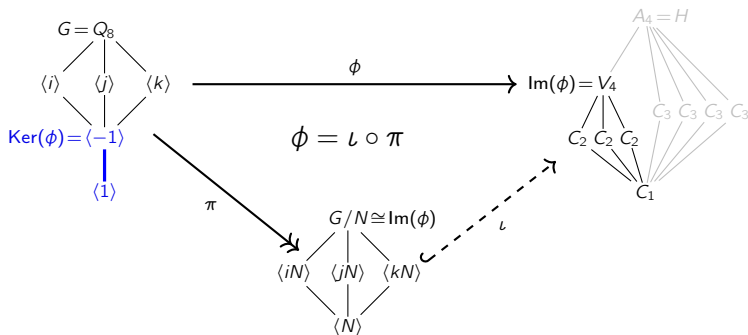
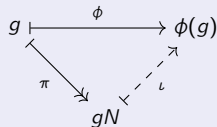
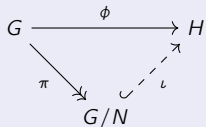
$$H/(H \cap A_n) = HA_n/A_n = S_n/A_n \cong C_2.$$

□

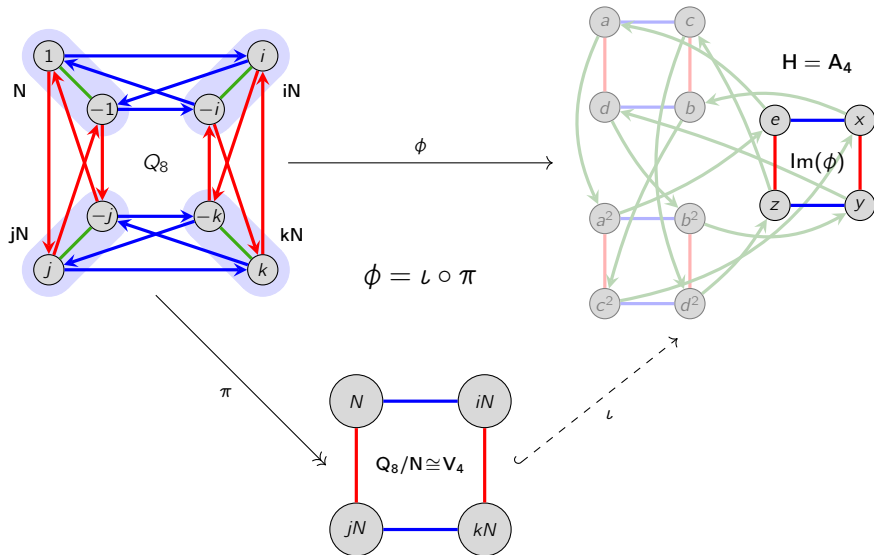
A generalization of the FHT

Theorem (exercise)

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



A generalization of the FHT



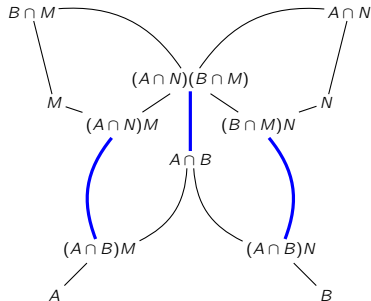
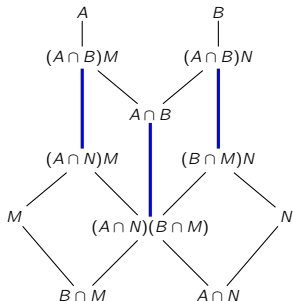
A theorem of Hans Zassenhaus

Butterfly lemma (see book for proof)

Let A, B be subgroups of a group, that contain $M \trianglelefteq A$ and $N \trianglelefteq B$. Then

1. $(A \cap N)M \trianglelefteq (A \cap B)M$,
2. $(B \cap M)N \trianglelefteq (A \cap B)N$,
3. The following quotient groups are isomorphic:

$$\frac{(A \cap B)M}{(A \cap N)M} \cong \frac{(A \cap B)N}{(B \cap M)N}.$$

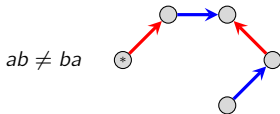
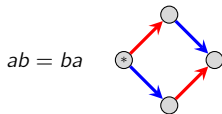


Commutators

We've seen how to divide \mathbb{Z} by $\langle 12 \rangle$, thereby “forcing” all multiples of 12 to be zero. This is one way to construct the integers modulo 12: $\mathbb{Z}_{12} \cong \mathbb{Z}/\langle 12 \rangle$.

Now, suppose G is nonabelian. We'd like to divide G by its “non-abelian parts,” making them zero and leaving only “abelian parts” in the resulting quotient.

A **commutator** is an element of the form $aba^{-1}b^{-1}$. Since G is nonabelian, *there are non-identity commutators*: $aba^{-1}b^{-1} \neq e$ in G .



In this case, the set $C := \{aba^{-1}b^{-1} \mid a, b \in G\}$ contains *more* than the identity.

Definition

The **commutator subgroup** G' of G is

$$G' := \langle aba^{-1}b^{-1} \mid a, b \in G \rangle.$$

The commutator subgroup is normal in G , and G/G' is abelian (homework).

The abelianization of a group

Definition

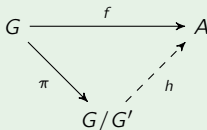
The **abelianization** of G is the quotient group G/G' .

The commutator subgroup G' is the **smallest normal subgroup** N of G such that G/N is abelian. [Note that G would be the “largest” such subgroup.]

Equivalently, the quotient G/G' is the **largest abelian quotient** of G . [Note that $G/G \cong \langle e \rangle$ would be the “smallest” such quotient.]

Universal property of commutator subgroups

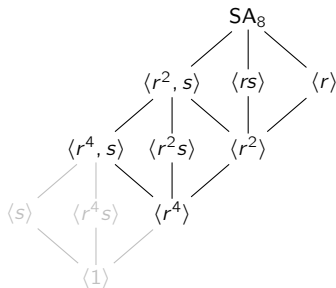
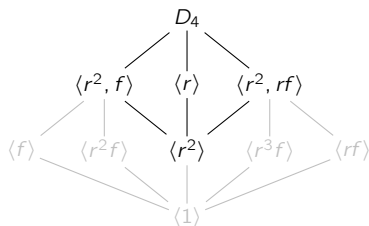
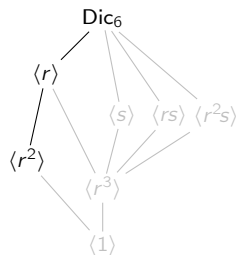
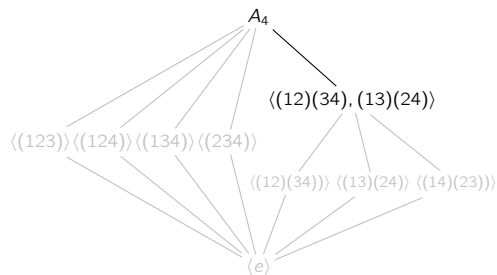
Suppose $f: G \rightarrow A$ is a homomorphism to an abelian group A . Then there is a unique homomorphism $h: G/G' \rightarrow A$ such that $f = h \circ \pi$:



We say that f “factors through” the abelianization, G/G' .

Some examples of abelianizations

By the isomorphism theorems, we can usually identify the commutator subgroup G and abelianation by inspection, from the subgroup lattice.



Automorphisms

We have already seen automorphisms of cyclic groups: “*structure-preserving rewirings*.”

For a general group G , an **automorphism** is an isomorphism $\phi: G \rightarrow G$.

The set of automorphisms of G defines the **automorphism group** of G , denoted $\text{Aut}(G)$.

Proposition

The automorphism group of \mathbb{Z}_n is $\text{Aut}(\mathbb{Z}_n) = \{\sigma_a \mid a \in U_n\} \cong U_n$, where

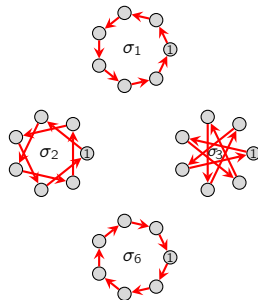
$$\sigma_a: \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad \sigma_a(1) = a.$$

$$U_7 = \langle 3 \rangle \cong C_6$$

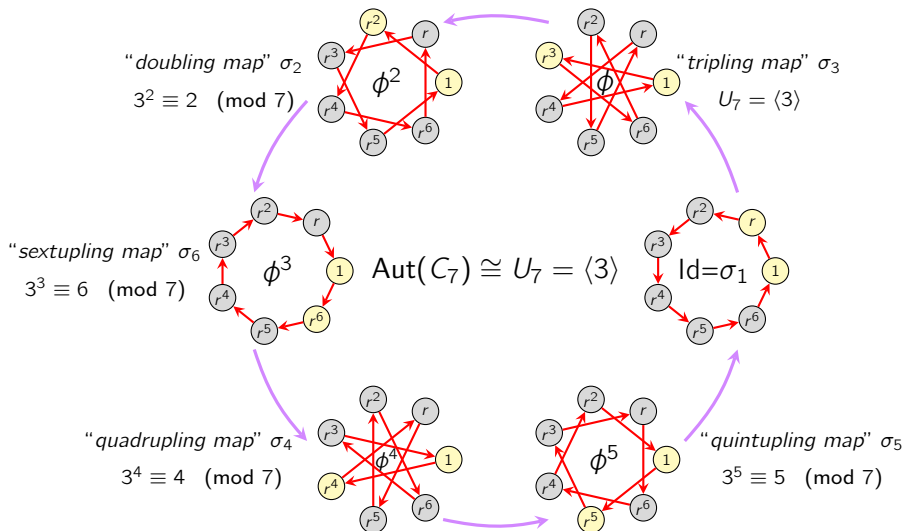
	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	2	4	6	1	3
3	3	3	6	2	5	1
4	4	4	1	5	2	6
5	5	5	3	1	6	4
6	6	6	5	4	3	2

$$\text{Aut}(C_7) = \langle \sigma_3 \rangle \cong U_7$$

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_2	σ_4	σ_6	σ_1	σ_3
σ_3	σ_3	σ_3	σ_6	σ_2	σ_5	σ_1
σ_4	σ_4	σ_4	σ_1	σ_5	σ_2	σ_6
σ_5	σ_5	σ_5	σ_3	σ_1	σ_6	σ_4
σ_6	σ_6	σ_6	σ_5	σ_4	σ_3	σ_2



An example: the automorphism group of C_7



Automorphisms of noncyclic groups

An automorphism is determined by where it sends the generators.

Examples

1. An automorphism ϕ of $V_4 = \langle h, v \rangle$ is determined by the image of h and v .

There are 3 choices for $\phi(h)$, then 2 choices for $\phi(v)$, thus $|\text{Aut}(V_4)| = 6$.

Every permutation of $\{h, v, r\}$ is an automorphism, and so $\text{Aut}(V_4) \cong S_3$.

2. Every $\phi \in \text{Aut}(D_3)$ is determined by $\phi(r)$ and $\phi(f)$.

Since automorphisms preserve order, if $\phi \in \text{Aut}(D_3)$, then

$$\phi(1) = 1, \quad \phi(r) = \underbrace{r \text{ or } r^2}_{2 \text{ choices}}, \quad \phi(f) = \underbrace{f, rf, \text{ or } r^2f}_{3 \text{ choices}}.$$

Thus, $|\text{Aut}(D_3)| \leq 6$. Both of the following define automorphisms of D_3 :

$$\left\{ \begin{array}{l} \alpha(r) = r \\ \alpha(f) = rf \end{array} \right. \quad \left\{ \begin{array}{l} \beta(r) = r^2 \\ \beta(f) = f \end{array} \right.$$

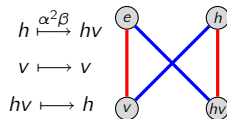
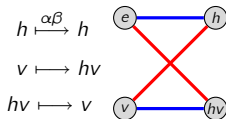
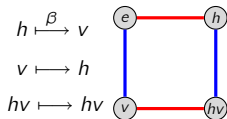
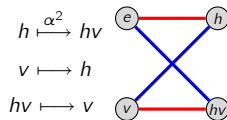
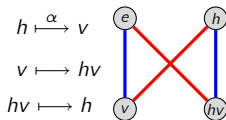
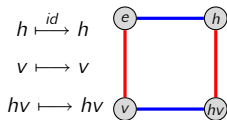
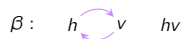
It is elementary to check that $\alpha\beta = \beta\alpha^2$, and so $\text{Aut}(D_3) \cong D_3 \cong S_3$.

Automorphisms of $V_4 = \langle h, v \rangle$

The following **permutations** are both automorphisms:



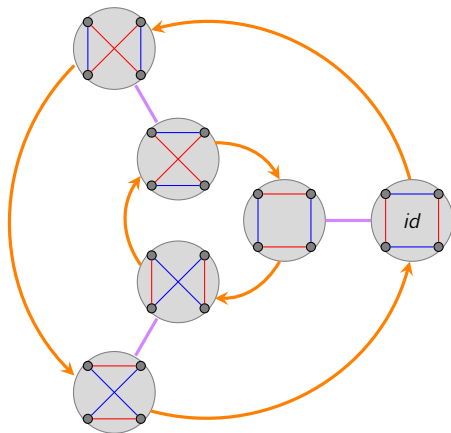
and



Automorphisms of $V_4 = \langle h, v \rangle$

Here is the Cayley table and Cayley graph of $\text{Aut}(V_4) = \langle \alpha, \beta \rangle \cong S_3 \cong D_3$.

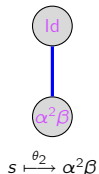
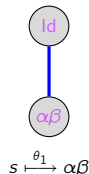
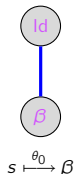
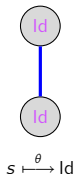
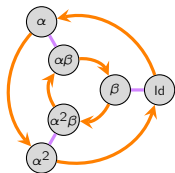
	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
id	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	id	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	id	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	id	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	id	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	id



Recall that α and β can be thought of as the permutations $h \xrightarrow{\alpha} v \xrightarrow{\alpha} hv$ and $h \xrightarrow{\beta} v \xrightarrow{\beta} hv$ and so $\text{Aut}(G) \hookrightarrow \text{Perm}(G) \cong S_n$ always holds.

The construction of $V_4 \rtimes C_2$

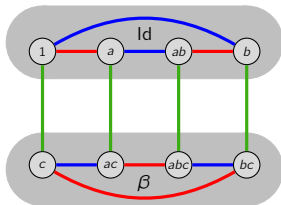
A labeling map $\theta_i: C_2 \longrightarrow \text{Aut}(V_4) \cong D_3$ is just a homomorphism. There are four:



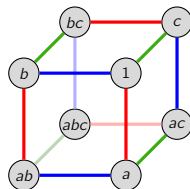
Let's now carry out our "inflation method" to construct $V_4 \rtimes C_2$.



Start with a copy of $B = C_2$



Inflate each node, insert **rewired versions** of $A = V_4$, and connect corresponding nodes



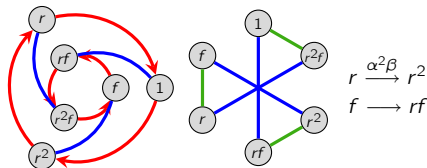
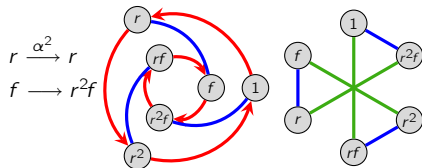
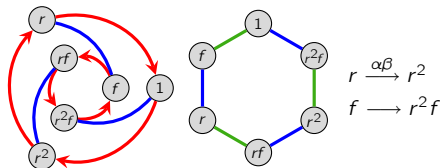
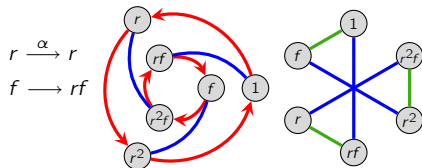
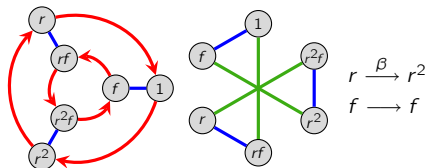
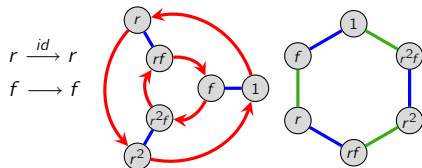
rearrange the Cayley graph
What familiar group is $V_4 \rtimes C_2$?

Automorphisms of D_3

$$\alpha: \quad r \quad r^2 \quad f \quad rf \quad r^2f$$

and

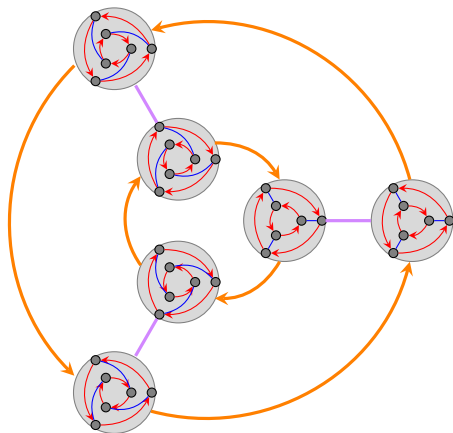
$$\beta: \quad r \quad r^2 \quad f \quad rf \quad r^2f$$



Automorphisms of D_3

Here is the Cayley table and Cayley graph of $\text{Aut}(D_3) = \langle \alpha, \beta \rangle$.

	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
id	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	id	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	id	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	id	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	id	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	id



$$\alpha: \quad r \quad r^2 \quad f \quad rf \quad r^2f$$

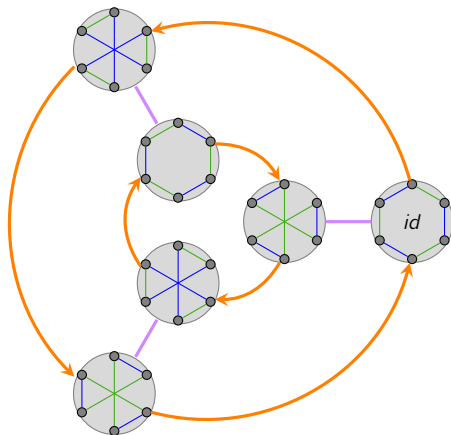
and

$$\beta: \quad r \quad r^2 \quad f \quad rf \quad r^2f$$

Automorphisms of D_3

Here is the Cayley table and Cayley graph of $\text{Aut}(D_3) = \langle \alpha, \beta \rangle$.

	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
id	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	id	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	id	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	id	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	id	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	id



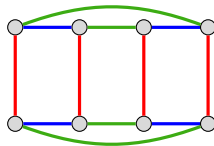
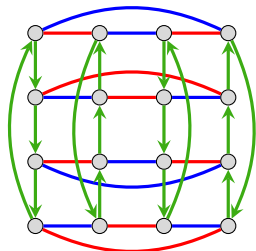
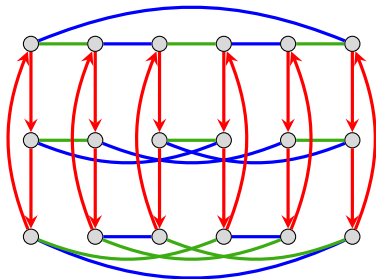
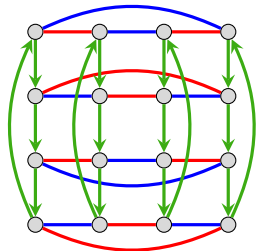
$$\alpha: \quad r \quad r^2 \quad f \quad rf \quad r^2f$$

and

$$\beta: \quad r \quad r^2 \quad f \quad rf \quad r^2f$$

A few more examples of semidirect products

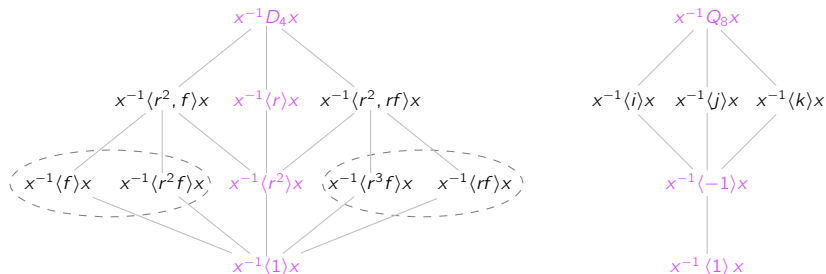
What groups are these?



Inner and outer automorphisms

Earlier in this class, we conjugated an entire group G by a fixed element $x \in G$.

This is an example of an **inner automorphism**. Here are two examples:



This permutes subgroups *within a conjugacy class*: $r^{-1}\langle f \rangle r = \langle r^2 f \rangle$.

Every subgroup of Q_8 is normal, thus any inner automorphism fixes every subgroup.

However, there is an automorphism of Q_8 that permutes subgroups, defined by

$$\phi: Q_8 \longrightarrow Q_8, \quad \phi(i) = j, \quad \phi(j) = k \quad \Rightarrow \quad \phi(k) = \phi(ij) = \phi(i)\phi(j) = jk = i.$$

This is called an **outer automorphism**.

The inner automorphism group

Definition

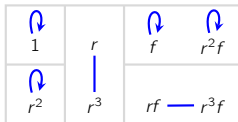
An **inner automorphism** of G is an automorphism $\varphi_x \in \text{Aut}(G)$ defined by

$$\varphi_x(g) := x^{-1}gx, \quad \text{for some } x \in G.$$

The inner automorphisms of G form a group, denoted **$\text{Inn}(G)$** . (Exercise)

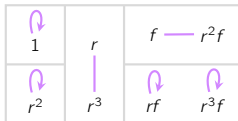
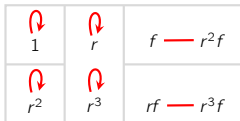
There are four inner automorphisms of D_4 :

$$\text{Id} = \varphi_1 = \varphi_{r^2}$$



$$\varphi_f = \varphi_{r^2f}$$

$$\varphi_r = \varphi_{r^3}$$



$$\varphi_{rf} = \varphi_{r^3f}$$

Since $\varphi_x^2 = \text{Id}$ for all of these, $\text{Inn}(D_4) = \langle \varphi_r, \varphi_f \rangle \cong V_4$.

Are there any other automorphisms of D_4 ?

The inner automorphism group

Proposition (exercise)

$\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$.

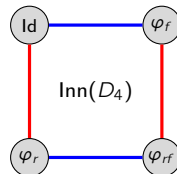
Remarks

- Many books define $\varphi_x(g) = xgx^{-1}$. Our choice is so $\varphi_{xy} = \varphi_x\varphi_y$ (reading L-to-R).
- If $z \in Z(G)$, then $\varphi_z \in \text{Inn}(G)$ is trivial.
- If $x = yz$ for some $z \in Z(G)$, then $\varphi_x = \varphi_y$ in $\text{Inn}(G)$:

$$\varphi_x(g) = x^{-1}gx = (yz)^{-1}g(yz) = z^{-1}(y^{-1}gy)z = y^{-1}gy = \varphi_y(g).$$

That is, if x and y are in **the same coset of $Z(G)$** , then $\varphi_x = \varphi_y$. (And conversely.)

	Z	rZ	fZ	rfZ	
	1	r	f	rf	cosets of $Z(D_4)$ are in bijection with inner automorphisms of D_4
	r^2	r^3	r^2f	r^3f	
$\text{cl}(1)$	1	r	f	rf	inner automorphisms of D_4 permute elements within conjugacy classes
$\text{cl}(r^2)$	r^2	r^3	r^2f	r^3f	
	$\text{cl}(r)$	$\text{cl}(f)$	$\text{cl}(rf)$		



The inner automorphism group

Key point

Two elements $x, y \in G$ are in the same coset of $Z(G)$ if and only if $\varphi_x = \varphi_y$ in $\text{Inn}(G)$.

Proposition

In any group G , we have $G/Z(G) \cong \text{Inn}(G)$.

Proof

Consider the map

$$f: G \longrightarrow \text{Inn}(G), \quad x \longmapsto \varphi_x,$$

It is straightforward to check this is (i) a homomorphism, (ii) onto, and (iii) that $\text{Ker}(f) = Z(G)$.

The result is now immediate from the FHT. □

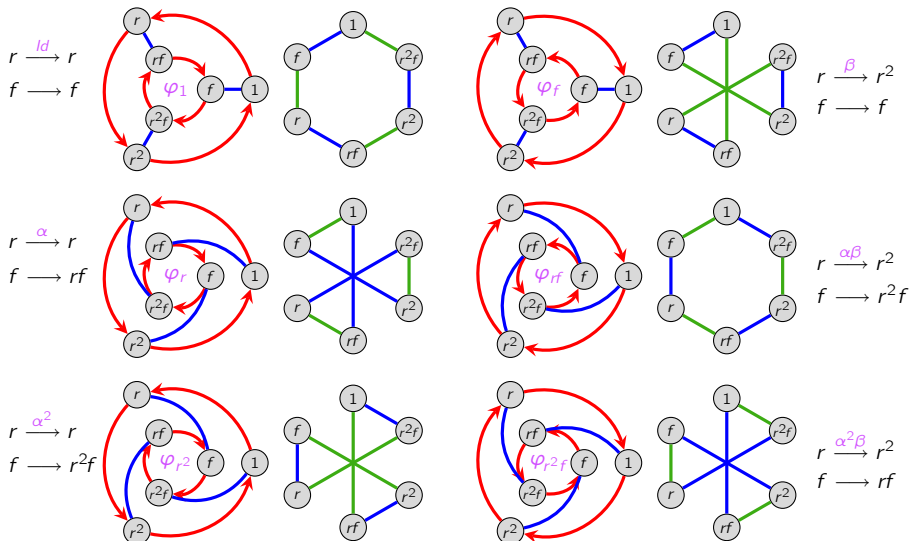
We just saw that $\text{Aut}(D_3) \cong D_3$, and we know that $Z(D_3) = \langle 1 \rangle$. Therefore,

$$\text{Inn}(D_3) \cong D_3/Z(D_3) \cong D_3 \cong \text{Aut}(D_3),$$

i.e., every automorphism is inner.

Inner automorphisms of D_3

Let's label each $\phi \in \text{Aut}(D_3)$ with the corresponding inner automorphism.



Automorphisms of D_4

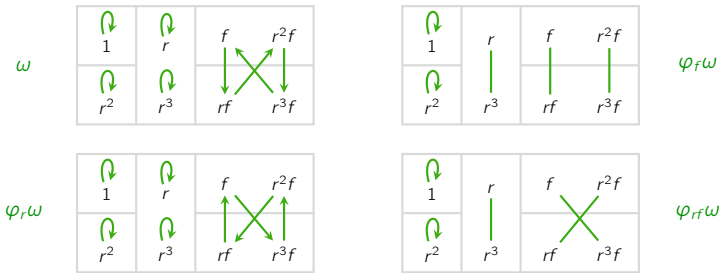
Every automorphism of $D_4 = \langle r, f \rangle$ is determined by where it sends the generators:

$$\phi(r) = \underbrace{r \text{ or } r^3}_{2 \text{ choices}}, \quad \phi(f) = \underbrace{f, rf, r^2f, r^3f, \text{ or } r^2}_{5 \text{ choices}}.$$

Thus $|\text{Aut}(D_4)| \leq 10$. But $\text{Inn}(D_4) \leq \text{Aut}(D_4)$, forces $|\text{Aut}(D_4)| = 4$ or 8 . Moreover,

$$\omega: D_4 \longrightarrow D_4, \quad \omega(r) = r, \quad \omega(f) = rf$$

is an (outer) automorphism, which swaps the “two types” of reflections of the square.



$$\text{Aut}(D_4) = \{Id, \varphi_r, \varphi_f, \varphi_{rf}, \omega, \varphi_r\omega, \varphi_f\omega, \varphi_{rf}\omega\} = \text{Inn}(D_4) \cup \text{Inn}(D_4)\omega \cong D_4.$$

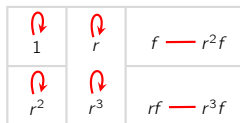
The full automorphism group of D_4

$$\text{Inn}(D_4) = \langle \varphi_r, \varphi_f \rangle$$

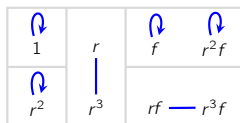
$$Id = \varphi_1$$



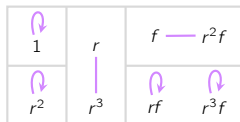
$$\varphi_r$$



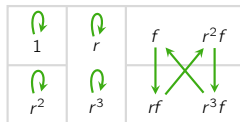
$$\varphi_f$$



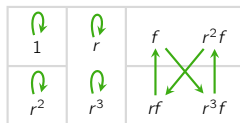
$$\varphi_{rf}$$



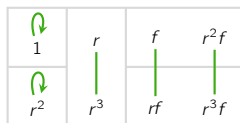
$$\text{Inn}(D_4)\omega$$



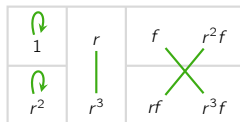
$$\omega$$



$$\varphi_r \omega$$



$$\varphi_f \omega$$



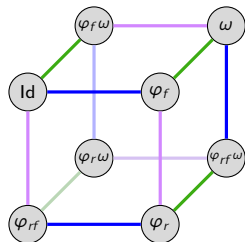
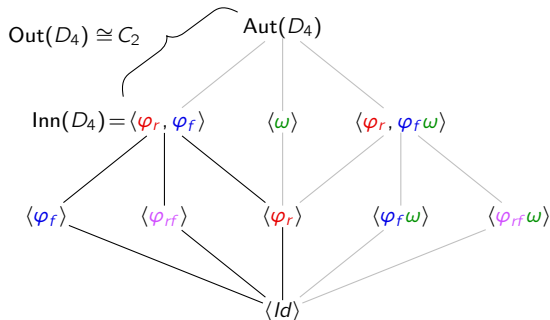
$$\varphi_{rf} \omega$$

The outer automorphism group

Definition

An **outer automorphism** of G is any automorphism that is not inner.

The **outer automorphism group** of G is the quotient $\text{Out}(G) := \text{Aut}(G)/\text{Inn}(G)$.



$$\text{Aut}(D_4) \cong \text{Inn}(D_4) \rtimes \text{Out}(D_4)$$

Note that there are four outer automorphisms, but $|\text{Out}(D_4)| = 2$.

We have seen: $\text{Out}(V_4) \cong D_3$, $\text{Out}(D_3) \cong \{\text{Id}\}$, $\text{Out}(D_4) \cong C_2$, $\text{Out}(Q_8) \cong S_3$.

Class automorphisms

Proposition (exercise)

Automorphisms permute conjugacy classes. That is, $g, h \in G$ are conjugate if and only if $\phi(g)$ and $\phi(h)$ are conjugate.

It is natural to ask if an automorphism being inner is equivalent to being the identity permutation on conjugacy classes.

In other words:

“if $\phi \in \text{Aut}(G)$ sends every element to a conjugate, must $\phi \in \text{Inn}(G)$?”

The answer is “no”. Burnside found examples of groups of order at least 729 that admit such an automorphism.

Definition

A **class automorphism** is an automorphism that sends every element to another in its conjugacy class.

In 1947, G.E. Wall found a group of order 32 with a class automorphism that is outer.

“A wrinkle in the mathematical universe” –John Baez

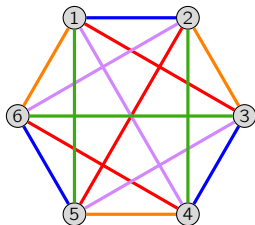
Theorem

The outer automorphism group of S_n is $\text{Out}(S_n) \cong \begin{cases} C_2 & \text{if } n = 6 \\ C_1 & \text{otherwise} \end{cases}$

S_6 has an automorphism that permutes the following conjugacy classes:

$$\text{cl}_{S_6}((12)) \longleftrightarrow \text{cl}_{S_6}((12)(34)(56)), \quad \text{cl}_{S_6}((123)) \longleftrightarrow \text{cl}_{S_6}((145)(256))$$

$$\text{cl}_{S_6}((12)(345)) \longleftrightarrow \text{cl}_{S_6}((123456))$$



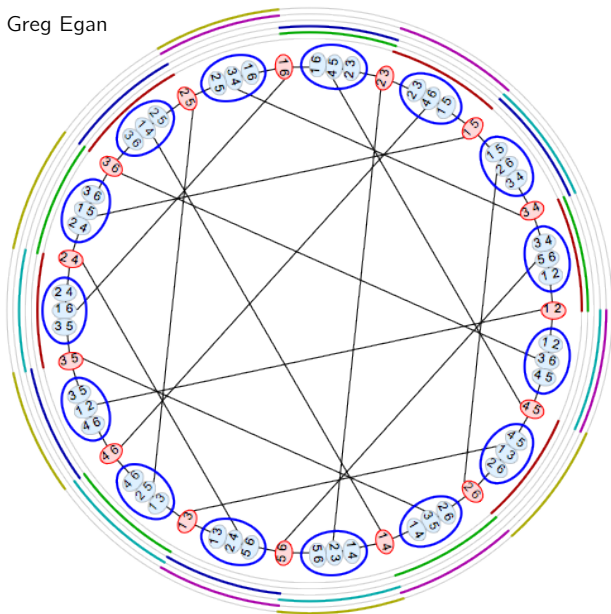
$(12)(36)(45)$: swaps purple and red

(13654) : cycles blue \rightarrow orange \rightarrow purple \rightarrow red \rightarrow green

$$S_5 \cong \langle (12)(36)(45), (13654) \rangle$$

An outer automorphism of S_6

Image credit: Greg Egan



Semidirect products, algebraically

Thus far, we've seen how to construct $A \rtimes_{\theta} B$ with our "inflation method."

Given A (for "*automorphism*") and B (for "*balloon*"), we label each inflated node $b \in B$ with $\phi \in \text{Aut}(A)$ via some **labeling map**

$$\theta: B \longrightarrow \text{Aut}(A).$$

Naturally, this can be defined algebraically. Denote multiplication in $A \times B$ by

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Definition

The (external) **semidirect product** $A \rtimes_{\theta} B$ of A and B , with respect to the homomorphism

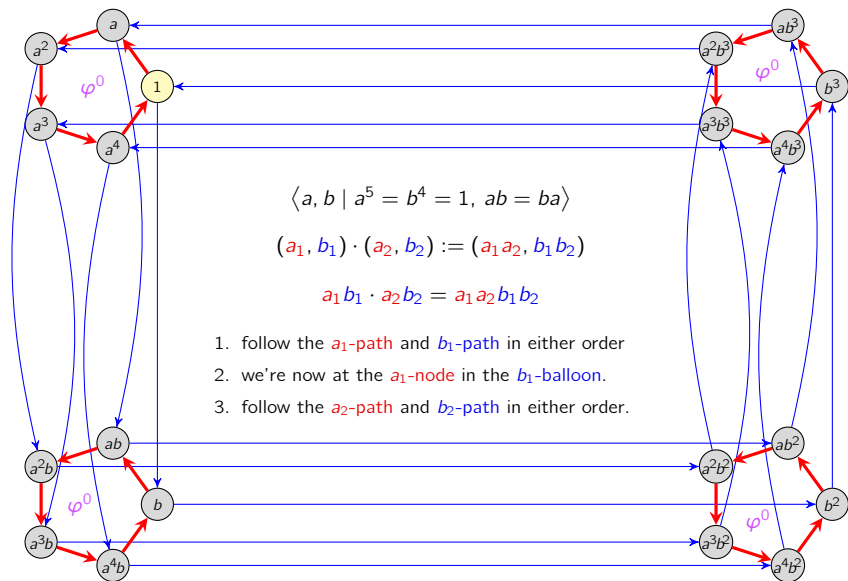
$$\theta: B \longrightarrow \text{Aut}(A),$$

is on the underlying set $A \times B$, where the binary operation $*$ is defined as

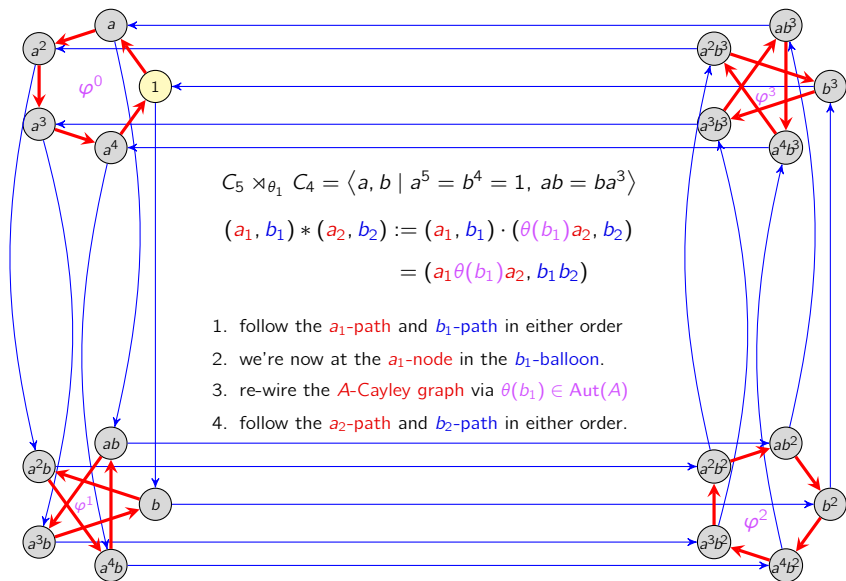
$$(a_1, b_1) * (a_2, b_2) := (a_1, b_1) \cdot (\theta(b_1)a_2, b_2) = (a_1\theta(b_1)a_2, b_1 b_2).$$

The isomorphic group on $B \times A$ by swapping the coordinates above is written $B \ltimes_{\theta} A$.

An example: the direct product $C_5 \times C_4$



An example: the semidirect product $C_5 \rtimes_{\theta} C_4$



Revisiting semidirect products

Recall how to multiply in $A \rtimes_{\theta} B$:

$$(a_1, b_1) * (a_2, b_2) := (a_1, b_1) \cdot (\theta(b_1)a_2, b_2) = (a_1\theta(b_1)a_2, b_1b_2).$$

Lemma

The subgroup $A \times \{1\}$ is normal in $A \rtimes_{\theta} B$.

Proof

Let's conjugate an arbitrary element $(x, 1) \in A \times \{1\}$ by an element $(a, b) \in A \rtimes_{\theta} B$.

$$(a, b)(x, 1)(a, b)^{-1} = (a\theta(b)x, b)(a^{-1}, b^{-1}) = (\underbrace{a\theta(b)x a^{-1}}_{\in A}, 1) \in A \times \{1\}.$$

Not all books use the same notation for semidirect products. Ours is motivated by:

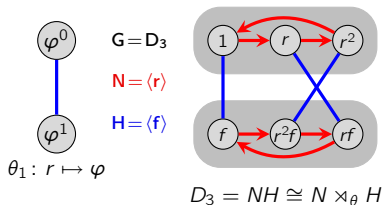
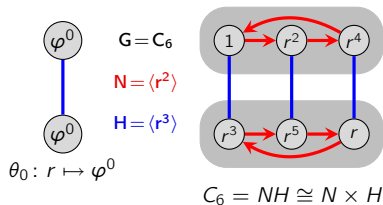
- In $A \times B$, both factors are normal (technically, $A \times \{1\}$ and $\{1\} \times B$).
- In $A \rtimes B$, the group on the “open” side of \rtimes is normal.

Internal products

Previously, we've looked at **outer products**: taking two unrelated groups and constructing a direct or semidirect product.

Now, we'll explore when a group $G = NH$ is isomorphic to a direct or semidirect product.

These are called **internal products**. Let's see two examples:



Questions

- Can we characterize when $NH \cong N \times H$ and/or $NH \cong N \rtimes_{\theta} H$?
- If $NH \cong N \rtimes_{\theta} H$, then what is the map $\theta: H \rightarrow \text{Aut}(N)$?

Internal direct products

When $G = NH$ is isomorphic to $N \times H$, we have an isomorphism

$$i: N \times H \longrightarrow NH, \quad i: (n, h) \longmapsto nh.$$

Since $N \times \{1\}$ and $\{1\} \times H$ are normal in $N \times H$, the subgroups N and H are normal in NH .

Recall that earlier, we showed that

$$|NH| = \frac{|N| \cdot |H|}{|N \cap H|},$$

and so it follows that if $NH \cong N \times H$, then $N \cap H = \{e\}$.

Theorem

Let $N, H \leq G$. Then $G \cong N \times H$ iff the following conditions hold:

- (i) N and H are normal in G
- (ii) $N \cap H = \{e\}$
- (iii) $G = NH$.

Remark

This has a very nice interpretation in terms of subgroup lattices! Groups for which (ii) and (iii) hold are called **lattice complements**.

Internal semidirect products

When $G = NH$ is isomorphic to $N \rtimes_{\theta} H$, we have an isomorphism

$$i: N \rtimes_{\theta} H \longrightarrow NH, \quad i: (n, h) \longmapsto nh.$$

This time, only $N \times \{1\}$ needs to be normal in $N \times H$, and so $N \trianglelefteq NH$.

As before, from

$$|NH| = \frac{|N| \cdot |H|}{|N \cap H|},$$

we conclude that if $NH \cong N \rtimes_{\theta} H$, then $N \cap H = \{e\}$.

Theorem

Let $N, H \leq G$. Then $G \cong N \rtimes H$ iff the following conditions hold:

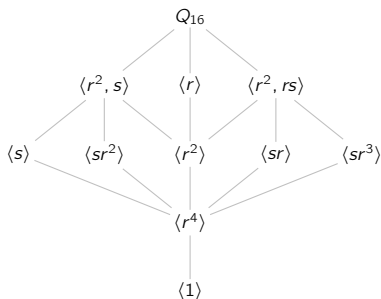
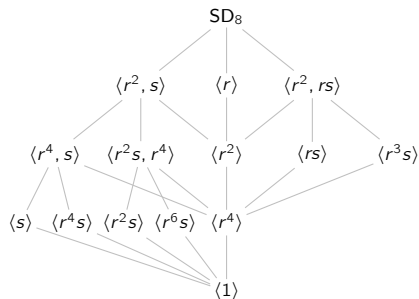
- (i) N is normal in G
- (ii) $N \cap H = \{e\}$
- (iii) $G = NH$,

and the homomorphism θ sends h to the **inner automorphism** $\varphi_{h^{-1}}$:

$$\theta: H \longrightarrow \text{Aut}(N), \quad \theta: h \longmapsto (n \xrightarrow{\varphi_{h^{-1}}} h^{-1}nh).$$

Let's do several examples for intuition, before proving this.

Examples of internal semidirect products



Observations

- The group SD_8 decomposes as a semidirect product several ways:

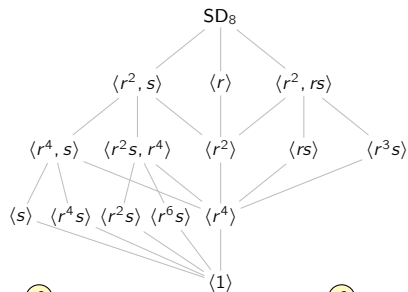
$$N = \langle r \rangle \cong C_8, \quad H = \langle s \rangle \cong C_2, \quad SD_8 = NH \cong C_8 \rtimes_{\theta_3} C_2.$$

or alternatively,

$$N = \langle r^2, rs \rangle \cong Q_8, \quad H = \langle s \rangle \cong C_2, \quad SD_8 = NH \cong Q_8 \rtimes_{\theta'} C_2.$$

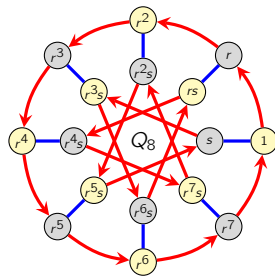
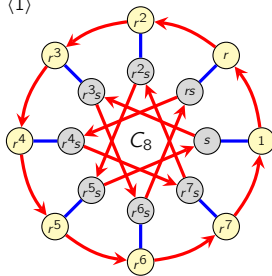
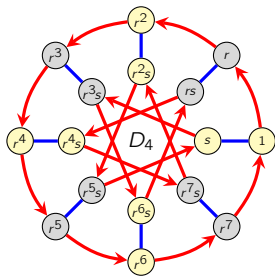
- The group Q_{16} does *not* decompose as a semidirect product!

Semidihedral groups as semidirect products



$$SD_8 \cong \langle r \rangle \rtimes \langle s \rangle \cong C_8 \rtimes C_2$$

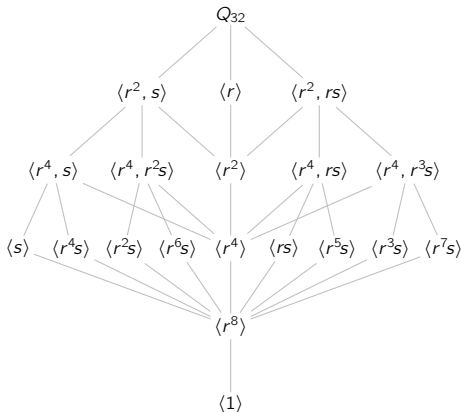
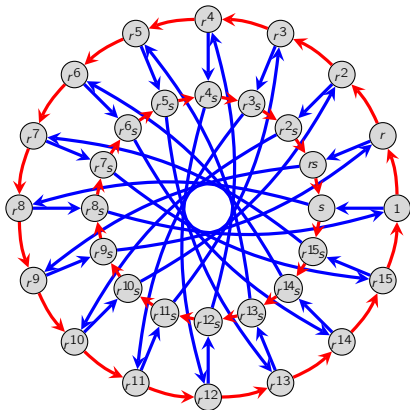
$$SD_8 \cong \langle r^2, rs \rangle \rtimes \langle s \rangle \cong Q_8 \rtimes C_2$$



Generalized quaternion groups

Recall that a **generalized quaternion group** is a dicyclic group whose order is a power of 2.

It's not hard to see that $r^8 = s^2 = -1$ is contained in every cyclic subgroup.



Therefore, $Q_{2^n} \not\cong N \rtimes H$ for any of its nontrivial subgroups.

Internal semidirect products and inner automorphisms

Theorem

Let $N, H \leq G$. Then $G \cong N \rtimes H$ iff the following conditions hold:

- (i) N is normal in G
- (ii) $N \cap H = \{e\}$
- (iii) $G = NH$,

and the homomorphism θ sends h to the inner automorphism φ_h :

$$\theta: H \longrightarrow \text{Aut}(N), \quad \theta: h \longmapsto \left(n \xrightarrow{\varphi_{h^{-1}}} h^{-1}nh \right).$$

Proof

We only need to establish that θ sends $h \mapsto \varphi_{h^{-1}}$.

Take n_1h_1 and n_2h_2 in NH . Their product is

$$(n_1h_1) * (n_2h_2) = n_1\theta(h_1)n_2h_1h_2$$

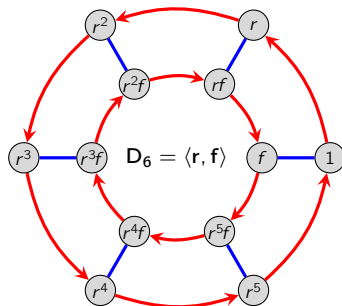
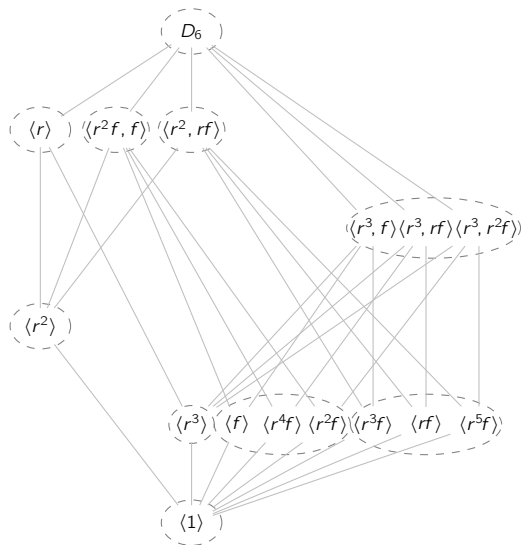
for some $\theta(h_1) \in \text{Aut}(N)$.

To see why $\theta(h_1)$ is the inner automorphism φ_{h_1} , note that

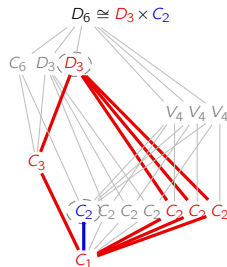
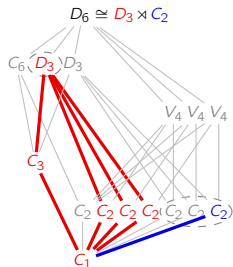
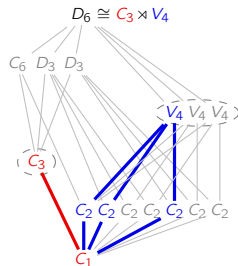
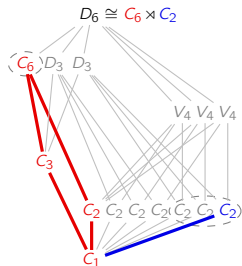
$$n_1\varphi_{h_1^{-1}}(n_2)h_1h_2 = n_1(h_1^{-1}n_2h_1)h_1h_2 = (n_1h_1) * (n_2h_2). \quad \square$$

Internal direct and semidirect products

In how many ways does D_6 decompose as an direct or semidirect product of its subgroups?

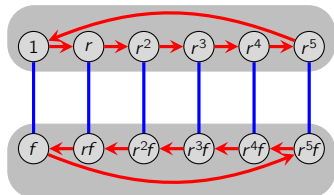


Decompositions of D_6 into direct and semidirect products

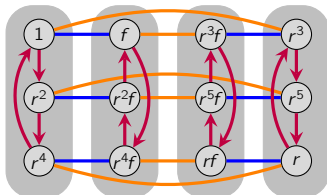


Decompositions of D_6 into direct and semidirect products

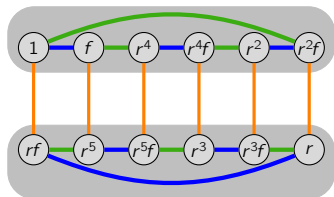
$C_6 \rtimes C_2$



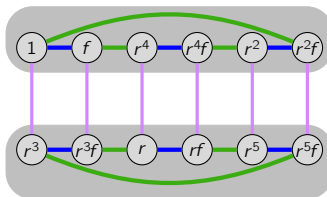
$C_3 \rtimes V_4$



$D_3 \rtimes C_2$



$D_3 \times C_2$



Central products

The following 3 conditions characterize when $G = NH \cong N \times H$.

1. H and N are normal,
2. $G = \langle H, N \rangle$,
3. $H \cap N = \langle 1 \rangle$.

If we weaken the first to only N being normal, we get $G = NH \cong N \rtimes H$.

Alternatively, we can keep the first two but weaken the third.

Definition

Suppose H and N are subgroups of G satisfying:

1. H and N are normal,
2. $G = \langle H, N \rangle$,
3. $H \cap N \leq Z(G)$.

The G is an **internal central product** of H and K , denoted $G \cong H \circ K$.

We can also define an *external central product* of A and B , but we won't do that here.

Central products

The dicyclic group DQ_8 is a central product two nontrivial ways:

- $DQ_8 \cong C_4 \circ Q_8$
- $DQ_8 \cong C_4 \circ D_4$.

Recall that $Z(DQ_8) = N \cong C_4$.

Index = 1

Order = 16

