Chapter 4: Maps between groups

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 8510, Abstract Algebra

Homomorphisms

Definition

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

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

An **isomorphism** is a bijective homomorphism.

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

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

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

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

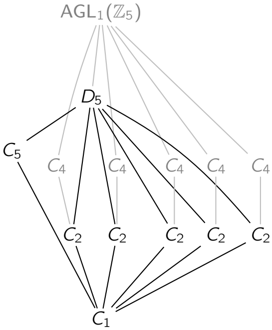
We will use standard function terminology:

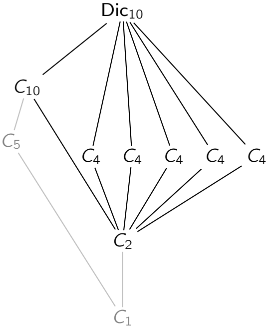
- the group G is the domain
- the group H is the codomain
- the image is what is often called the *range*:

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

Embeddings vs. quotients: A preview

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





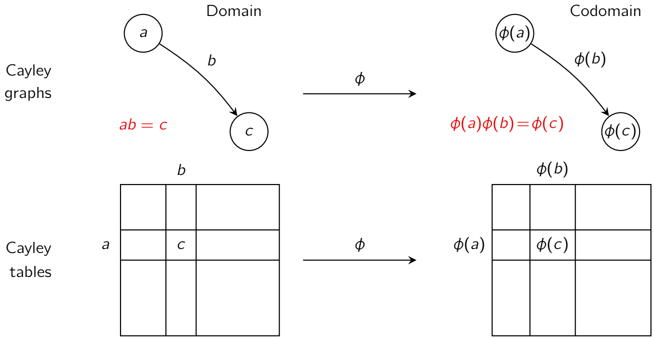
In one of these groups, D_5 is subgroup. In the other, it arises as a quotient.

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

Homomorphisms

The condition $\phi(ab) = \phi(a)\phi(b)$ means that the map ϕ preserves the structure of G.

It 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.

Two basic properties of homomorphisms

Proposition

Let $\phi\colon G \to H$ be a homomorphism. Denote the identity of G and H by 1_G and 1_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, $\phi(1_G) = 1_H$. ✓

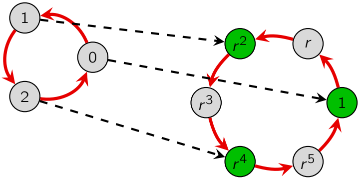
(ii) Take any $g \in G$. Observe that

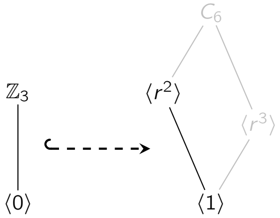
$$\phi(g)\,\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1_G) = 1_H\,.$$

Since $\phi(g)\phi(g^{-1}) = 1_H$, it follows immediately that $\phi(g^{-1}) = \phi(g)^{-1}$. ✓

An embedding and an isomorphisms

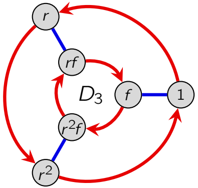
Consider the homomorphism $\theta\colon \mathbb{Z}_3 \to C_6$, defined by $\theta(n) = r^{2n}$:

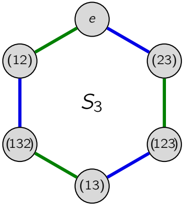


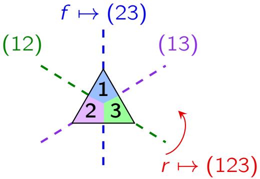


The following is an isomorphism:

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







An example that is neither an embedding nor quotient

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

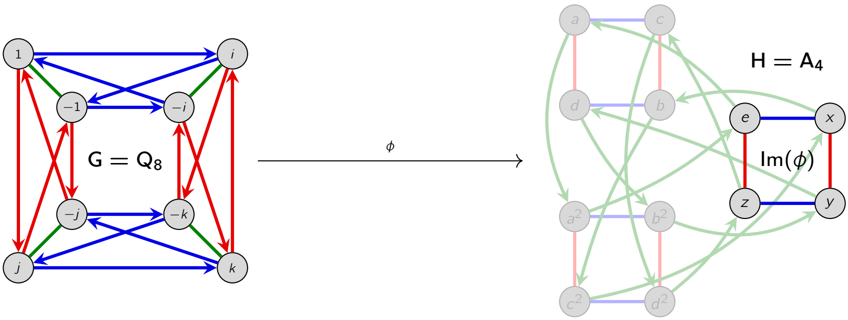
$$\phi(i) = (12)(34), \qquad \phi(j) = (13)(24).$$

Using the property of homomorphisms,

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

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

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



Group representations

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

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

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

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

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

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

Formally, we have an embedding $\phi\colon Q_8 \to \mathrm{GL}_4(\mathbb{R})$ 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

Definition

Let $\phi\colon G \to H$ be a homomorphism. The preimage of $h \in \mathrm{Im}(\phi)$ is

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

Definition

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

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

Exercise

The kernel of any homomorphism $\phi\colon G \to H$ is normal. □

Proposition

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

Proof (sketch)

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

Establish $\phi^{-1}(h) = gN$ by verifying both $\subseteq$ and $\supseteq$. □

The fundamental homomorphism theorem

Theorem (FHT)

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

Let's see this by example:

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

$$\phi(1) = e$$

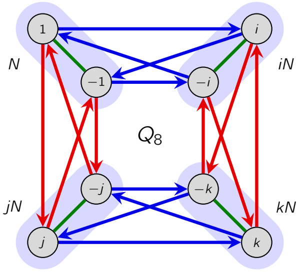
$$\phi(-1) = \phi(i^2) = \phi(i)^2 = v^2 = e$$

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

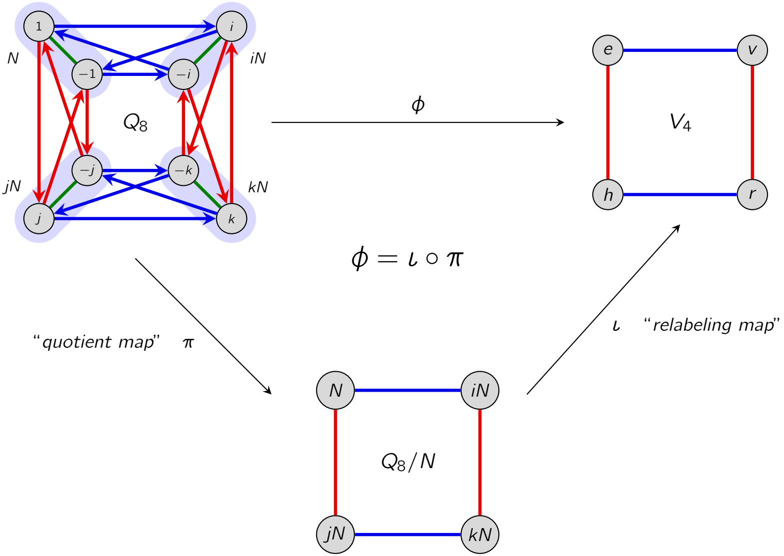
$$\phi(-k) = \phi(ji) = \phi(j)\phi(i) = hv = r$$

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

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



Visualizing the FHT via Cayley graphs



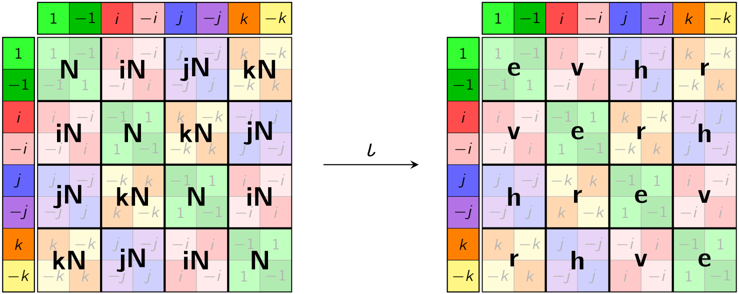
Visualizing the FHT via Cayley tables

Here's another way to think about the homomorphism

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

as the composition of:

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



Proof of the FHT

Fundamental homomorphism theorem

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

Proof

Let $N = \mathrm{Ker}(\phi)$, and define

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

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

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

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

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

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

- *Show ι is a homomorphism*.

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

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

Proof (cont.)

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

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

- *Show ι is surjective (onto)*.

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

Useful technique

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

(i) Define $\phi\colon G/N \to H$ and prove it's a well-defined, bijective, homomorphism.

(ii) Define $\phi\colon G \to H$ and prove that it's a surjective homomorphism, and $\mathrm{Ker}\,\phi = N$.

Consequences of the FHT

Let's 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

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

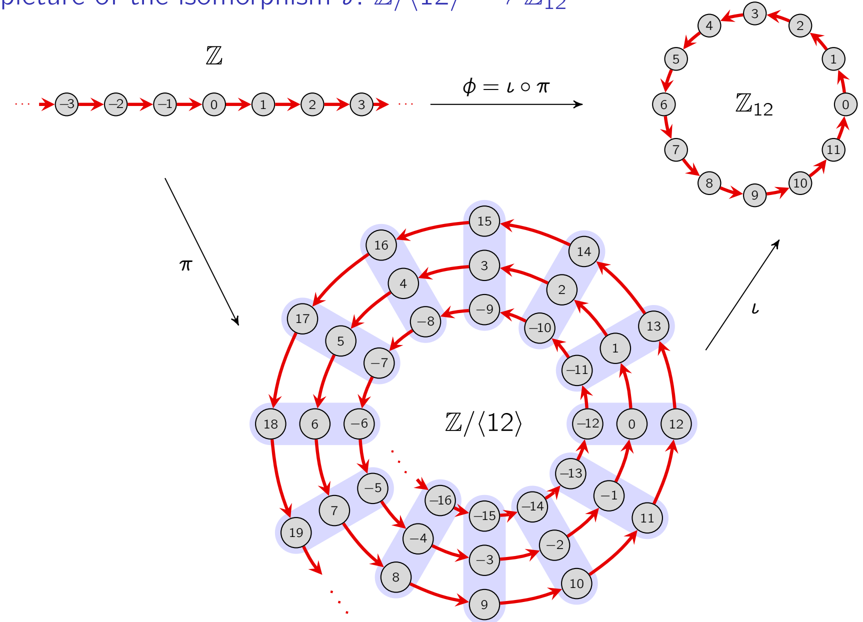
- The map $\iota\colon G/N \to H$, where $\iota(aN) = \phi(a)$, is a well-defined homomorphism, meaning that

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

Remark

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

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



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: Characterizes "*quotients of a products by a factor*"

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 theorem, *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.

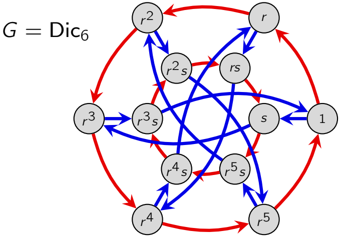
Moreover, "most properties" of $H/N \leq G/N$ are inherited from $H \leq G$.

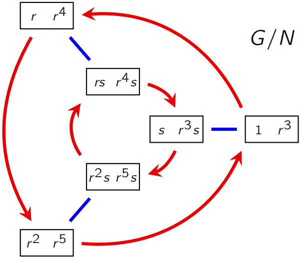
This is best understood by interpreting the subgroup lattices of G and G/N.

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

The correspondence theorem: subgroups of quotients

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





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.*"

"*shoeboxes; lids on*"

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

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

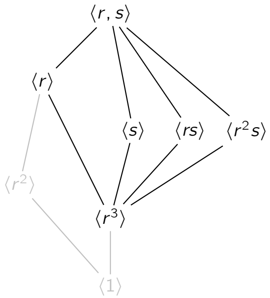
"*shoes out of the box*"

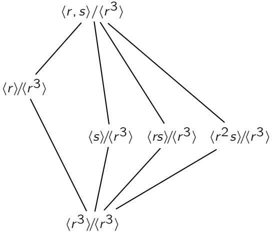
r^2N	r^2sN
rN	rsN
N	sN

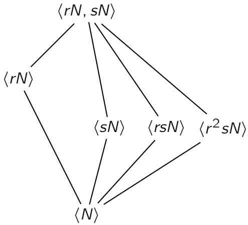
$\langle rN \rangle \leq G/N$

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

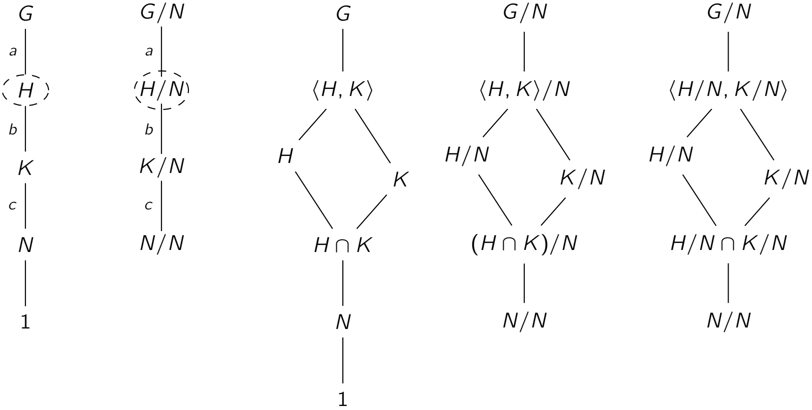
1. Subgroups of the quotient G/N are quotients of the subgroup $H \leq G$ that contain N.
2. $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$
3. $[G/N : H/N] = [G : H]$
4. $H/N \cap K/N = (H \cap K)/N$
5. $\langle H/N, K/N \rangle = \langle H, K \rangle / N$
6. H/N is conjugate to K/N in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

The correspondence theorem: subgroups of quotients

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

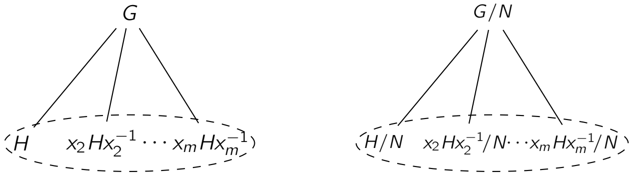
We've already interpreted the the first part.

Here's what the next four parts say.

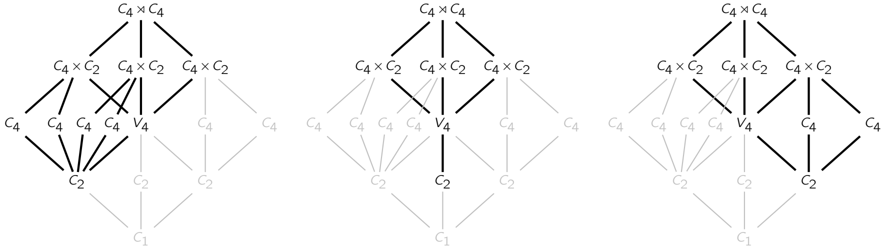


The correspondence theorem: subgroups of quotients

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.



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.

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 $N \leq H \leq G$.

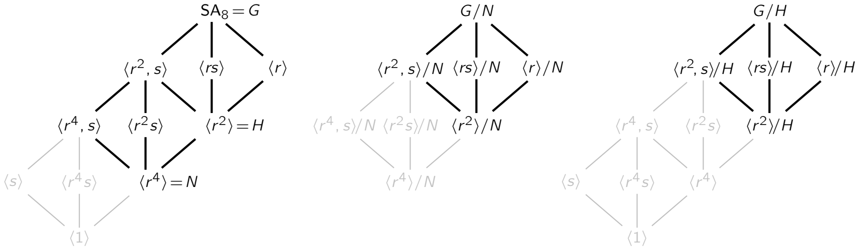
Moreover, if $H \trianglelefteq G$, then $H/N \trianglelefteq G/N$. In this case, we can ask:

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

Fraction theorem

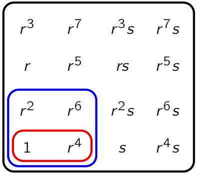
Given a chain $N \leq H \leq G$ of normal subgroups of G,

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

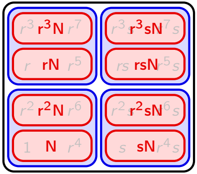


The fraction theorem: quotients of quotients

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

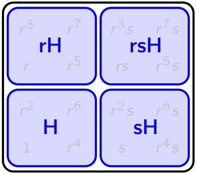


$N \leq H \leq G$



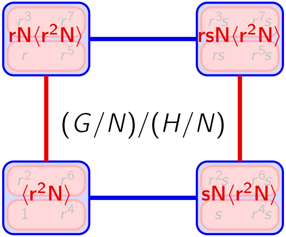
$G/N = \langle rN, sN \rangle \cong C_4 \times C_2$

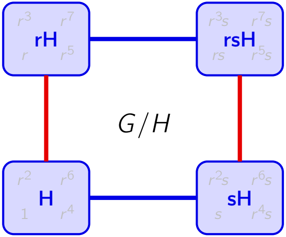
$H/N = \langle r^2N \rangle = \{N, r^2N\} \cong C_2$



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

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





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

$$\phi \colon G/N \longrightarrow G/H, \qquad \phi \colon gN \longmapsto gH.$$

- *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, $(G/N)/\operatorname{Ker}(\phi) = (G/N)/(H/N) \cong \operatorname{Im}(\phi) = G/H$. □

The fraction theorem: quotients of quotients

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

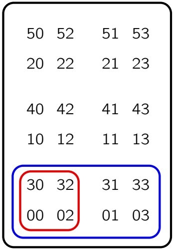
Consider the subgroups $N = \langle 30, 02 \rangle \cong V_4$ and $H = \langle 30, 01 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

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

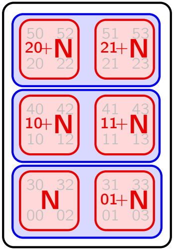
$$G/N = \{N,\ 01{+}N,\ 10{+}N,\ 11{+}N,\ 20{+}N,\ 21{+}N\}, \qquad H/N = \{N,\ 01{+}N\}$$

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

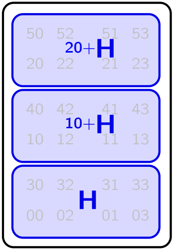
$$(G/N)/(H/N) = \Big\{\{N,\ 01{+}N\},\ \{10{+}N,\ 11{+}N\},\ \{20{+}N,\ 21{+}N\}\Big\}.$$



$N \leq H \leq G$

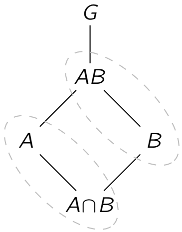


G/N consists of 6 cosets
$H/N = \{N,\ 01{+}N\}$



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

The diamond theorem: quotients of products by factors



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

$$\phi\colon A \longrightarrow AB/B\,, \qquad \phi\colon a \longmapsto aB\,.$$

If we can show:

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

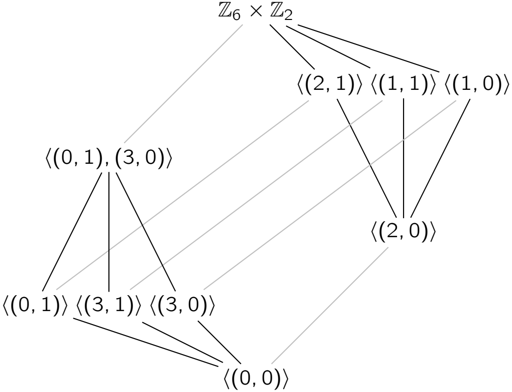
Let $A, B \leq G$, with one of them normalizing the other. Then $|AB| = \dfrac{|A| \cdot |B|}{|A \cap B|}$.

The diamond theorem: quotients of products by factors

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

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

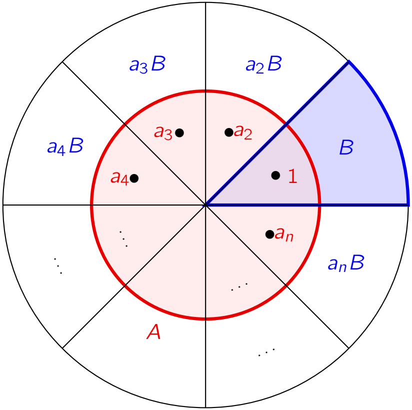
Let's interpret the diamond theorem $AB/B \cong A/A \cap B$ in terms of the subgroup lattice.



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

The diamond theorem 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

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

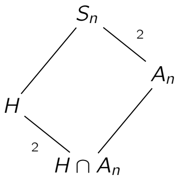
$A/(A \cap B) = \{\text{small pizza slices}\}$

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

The diamond theorem: quotients of products by factors

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.



Proof

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

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

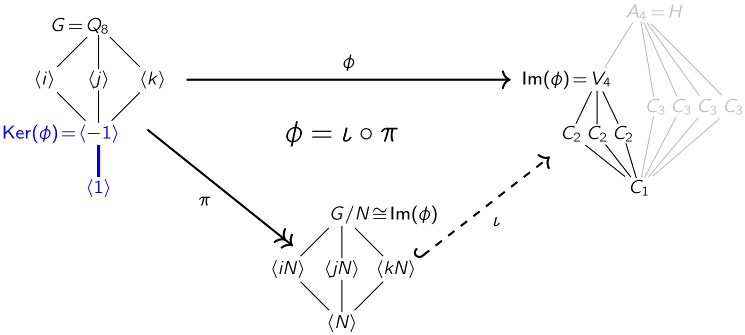
By the diamond theorem,

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

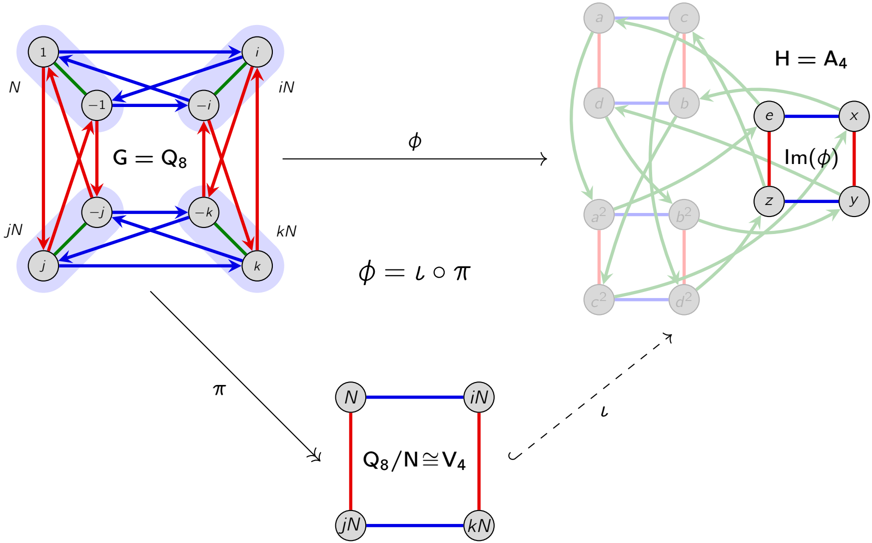
A generalization of the FHT

Theorem (exercise)

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



A generalization of the FHT

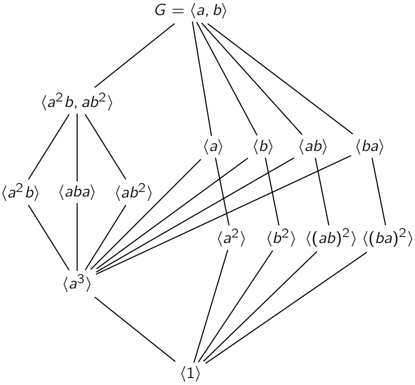


The "subgroup" and "quotient" operations commute

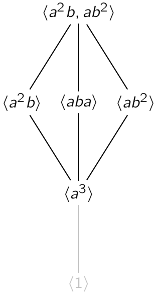
Key idea

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

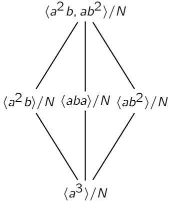
Example: Consider the group $G = \mathrm{SL}_2(\mathbb{Z}_3)$.



subgroup $\mathbf{H} \cong \mathbf{Q_8}$



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



"*quotient of the subgroup*"

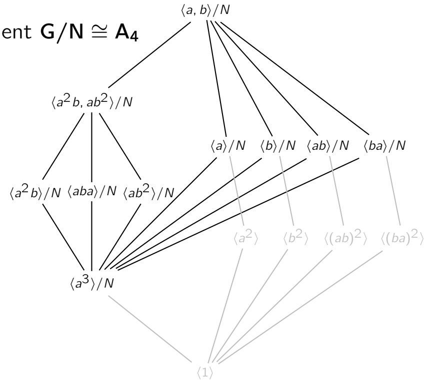
The "subgroup" and "quotient" operations commute

Key idea

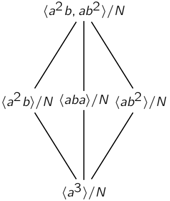
The quotient of a subgroup is just the subgroup of the quotient.

Example: Consider the group $G = SL_2(\mathbb{Z}_3)$.

quotient $\mathbf{G/N \cong A_4}$



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



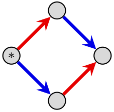
"*subgroup of the quotient*"

Commutators

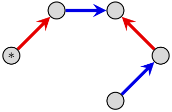
We contructed $\mathbb{Z}_{12} \cong \mathbb{Z}/\langle 12 \rangle$ by "forcing" multiples of 12 to be zero (kernel of a quotient).

A commutator is an element of the form $aba^{-1}b^{-1}$.

$ab = ba$



$ab \neq ba$



Definition

The commutator subgroup of G is

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

Do you see why $G' \trianglelefteq G$? [*Hint*: Consider the product gcg^{-1} and c^{-1}.]

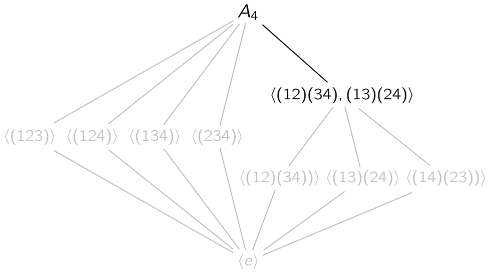
Definition

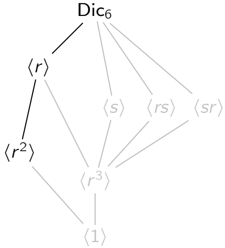
The abelianization of G is the quotient group G/G'.

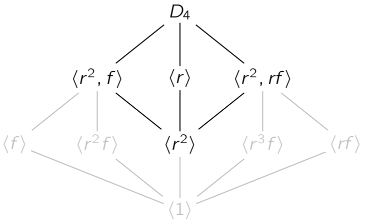
- G' is the smallest normal subgroup N of G such that G/N is abelian.
- G/G' is the largest abelian quotient of G.

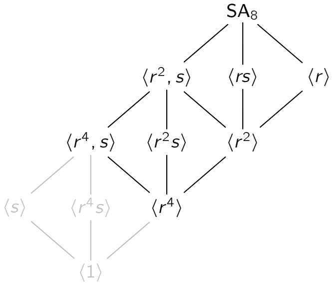
Some examples of abelianizations

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









Automorphisms

An automorphism of G is a homomorphism $\phi\colon G \to G$.

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

Proposition

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

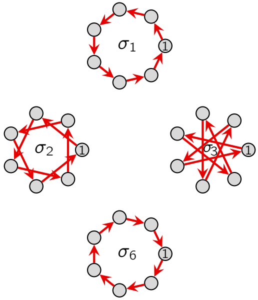
$$\sigma_a\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_n\,, \qquad \sigma_a(1) = a\,.$$

$\mathbf{U_7} = \langle \mathbf{3} \rangle \cong \mathbf{C_6}$

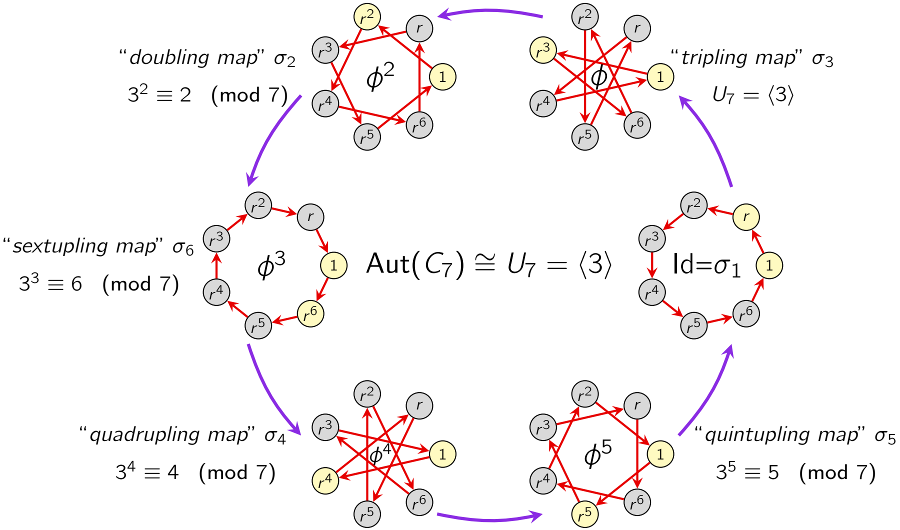
	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

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

	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_4	σ_6	σ_1	σ_3	σ_5
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_3
σ_5	σ_5	σ_3	σ_1	σ_6	σ_4	σ_2
σ_6	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1



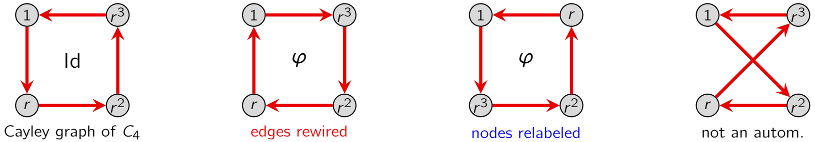
An example: the automorphism group of C_7



Automorphisms of noncyclic groups

Key idea

Think of an automorphism as a "*structure-preserving*" *rewiring* of the Cayley graph.



Examples

1. Every permutation of $\{h, v, r\}$ defines an automorphism, so $\mathrm{Aut}(V_4) \cong S_3$.

2. Every $\phi \in \mathrm{Aut}(D_3)$ is determined by $\phi(r)$ and $\phi(f)$. Since they preserve order

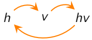
$$\phi(1) = 1\,, \qquad \phi(r) = \underbrace{r \text{ or } r^2}_{\text{2 choices}}, \qquad \phi(f) = \underbrace{f,\ rf,\ \text{or } r^2 f}_{\text{3 choices}}\,.$$

Thus, $|\mathrm{Aut}(D_3)| \leq 6$. The following are noncommuting automorphisms:

$$\begin{cases} \alpha(r) = r \\ \alpha(f) = rf \end{cases} \qquad \begin{cases} \beta(r) = r^2 \\ \beta(f) = f \end{cases}$$

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

The following permutations are both automorphisms:

α : 

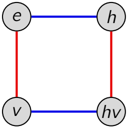
and

β : 

$h \stackrel{id}{\longmapsto} h$

$v \longmapsto v$

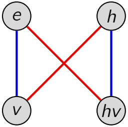
$hv \longmapsto hv$



$h \stackrel{\alpha}{\longmapsto} v$

$v \longmapsto hv$

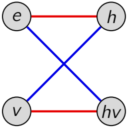
$hv \longmapsto h$



$h \stackrel{\alpha^2}{\longmapsto} hv$

$v \longmapsto h$

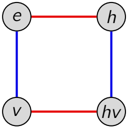
$hv \longmapsto v$



$h \stackrel{\beta}{\longmapsto} v$

$v \longmapsto h$

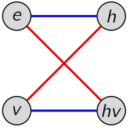
$hv \longmapsto hv$



$h \stackrel{\alpha\beta}{\longmapsto} h$

$v \longmapsto hv$

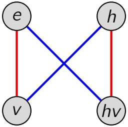
$hv \longmapsto v$



$h \stackrel{\alpha^2\beta}{\longmapsto} hv$

$v \longmapsto v$

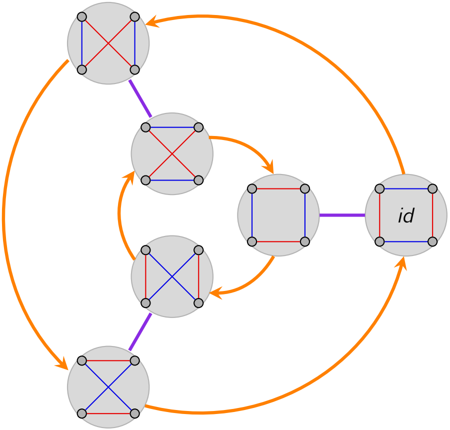
$hv \longmapsto h$



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

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

	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 

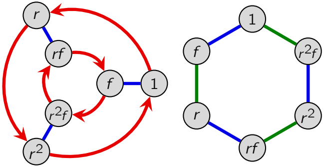
and 

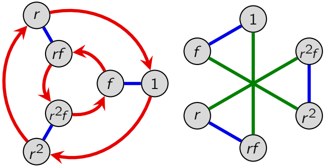
Automorphisms of D_3

α : r r^2 f rf r^2f and β : r r^2 f rf r^2f

$r \xrightarrow{id} r$

$f \longrightarrow f$



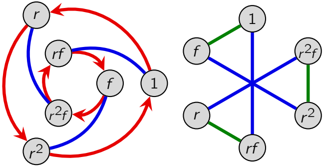


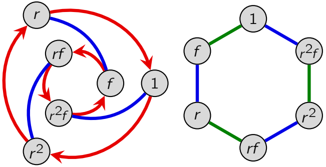
$r \xrightarrow{\beta} r^2$

$f \longrightarrow f$

$r \xrightarrow{\alpha} r$

$f \longrightarrow rf$



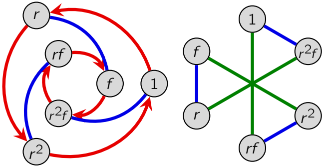


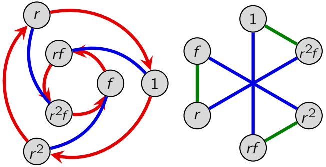
$r \xrightarrow{\alpha\beta} r^2$

$f \longrightarrow r^2f$

$r \xrightarrow{\alpha^2} r$

$f \longrightarrow r^2f$





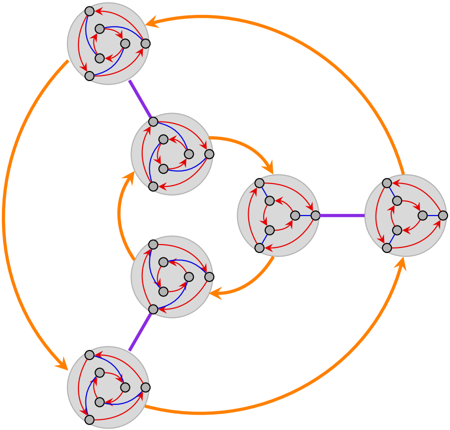
$r \xrightarrow{\alpha^2\beta} r^2$

$f \longrightarrow rf$

Automorphisms of D_3

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

	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

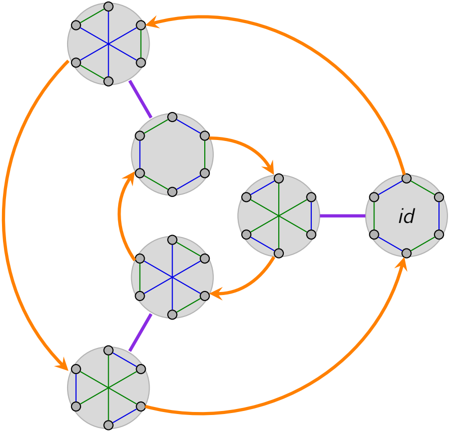


α : r r^2 f rf r^2f and β : r r^2 f rf r^2f

Automorphisms of D_3

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

	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

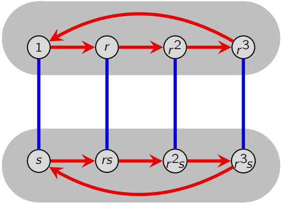


α : r r^2 f rf $r^2 f$ and β : r r^2 f rf $r^2 f$

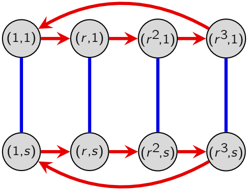
Semidirect products

Consider the following "inflation" construction of the Cayley graph of a direct product:

Start with a copy of $B = C_2$



Inflate each node, insert $A = C_4$ in each and connect corresponding nodes with edges



"pop" each inflated node to get the direct product $C_4 \times C_2$

Reversing the red arrows in the bottom "balloon" would result in a Cayley graph for D_4.

We say that D_4 is the semidirect product of C_4 and C_2, written $D_4 \cong C_4 \rtimes C_2$.

Key point

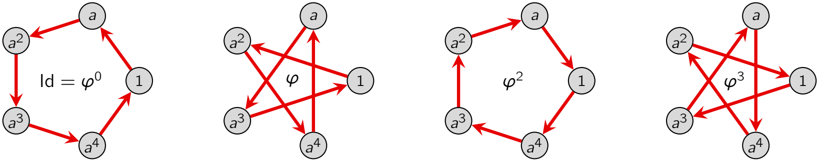
For groups A, B we need a "labeling map" homomorphism

$$\theta \colon B \longrightarrow \mathrm{Aut}(A),$$

where $\theta(b)$ describes: "*which rewiring of A we stick into balloon $b \in B$*".

Semidirect products

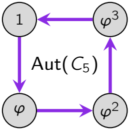
Let's construct all semidirect products of $A = C_5 = \langle a \rangle$ with $B = C_4 = \langle b \rangle$.

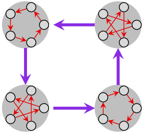


starting graph $\quad a^1 \mapsto (a^1)^2 = a^2 \quad a^2 \mapsto (a^2)^2 = a^4 \quad a^4 \mapsto (a^4)^2 = a^3$

$\mathrm{Aut}(C_5) \cong U(4) \cong C_4 = \langle \varphi \rangle$ is generated by the "doubling map".

$$\mathrm{Aut}(C_5) = \{1, \varphi, \varphi^2, \varphi^3\} \cong C_4$$





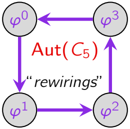
Each "labeling map"

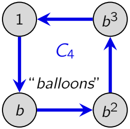
$$\theta_i \colon C_4 \longrightarrow \mathrm{Aut}(C_5)$$

each is determined by $\theta_i(b) = \varphi^i$, for $i = 0, 1, 2, 3$.

An example: the direct product of C_5 and C_4

Let's construct the "trivial" semidirect product, $C_5 \rtimes_{\theta_0} C_4 = C_5 \times C_4$:

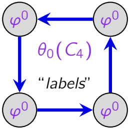




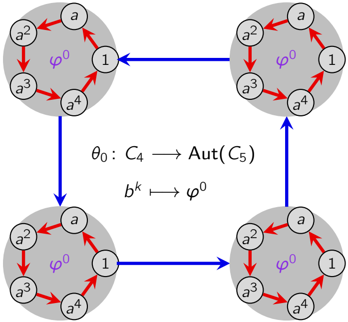
"*labeling map*"

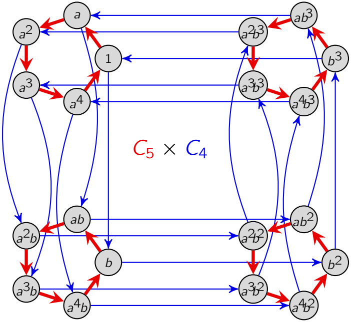
$C_4 \xrightarrow{\theta_0} \mathrm{Aut}(C_5)$

$b^k \longmapsto \varphi^0$



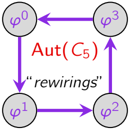
Stick in non-rewired copies of A, and then reconnect the B-arrows.

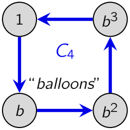




An example: the 1st semidirect product of C_5 and C_4

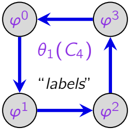
Let's construct the semidirect product $C_5 \rtimes_{\theta_1} C_4$:



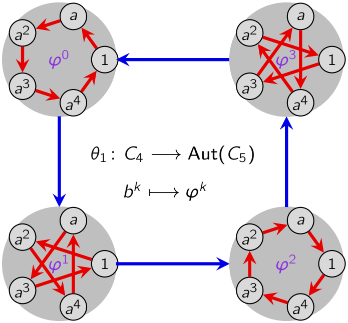


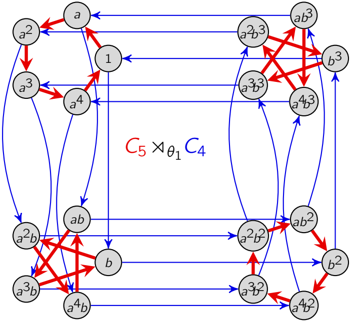
"*labeling map*"

$$C_4 \xrightarrow{\theta_1} \mathrm{Aut}(C_5)$$
$$b^k \longmapsto \varphi^k$$



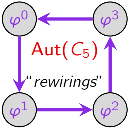
Stick in θ_1-rewired copies of A, and then reconnect the B-arrows.

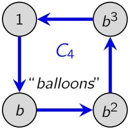




An example: the 2^{nd} semidirect product of C_5 and C_4

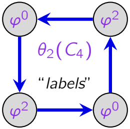
Let's now construct a different semidirect product, $C_5 \rtimes_{\theta_2} C_4$:



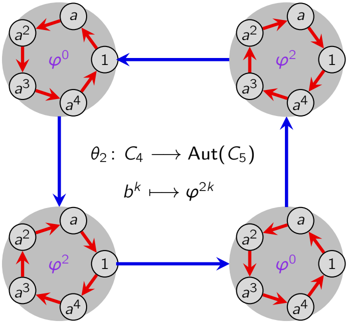


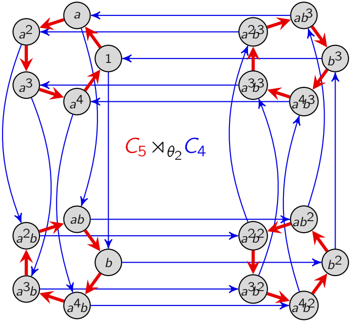
"*labeling map*"

$$C_4 \xrightarrow{\theta_2} \mathrm{Aut}(C_5)$$
$$b^k \longmapsto \varphi^{2k}$$



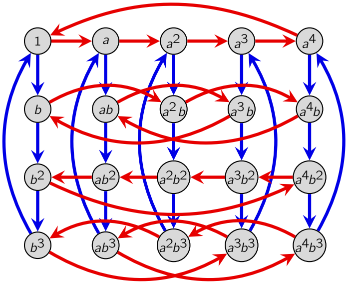
Stick in θ_2-rewired copies of A, and then reconnect the B-arrows.

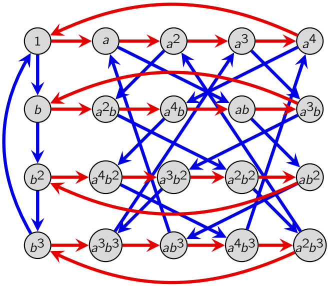




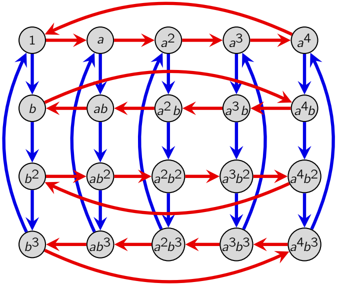
Rewiring edges vs. re-labeling nodes

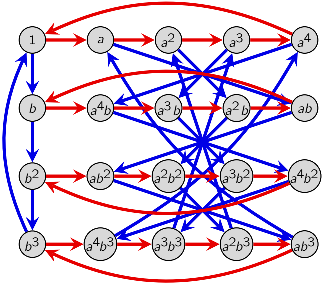
$C_5 \rtimes_{\theta_1} C_4$





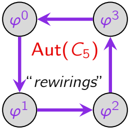
$C_5 \rtimes_{\theta_2} C_4$

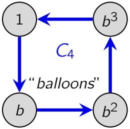




An example: the 3rd semidirect product of C_5 and C_4

Let's construct the last semidirect product $C_5 \rtimes_{\theta_3} C_4$:

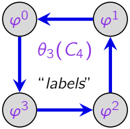




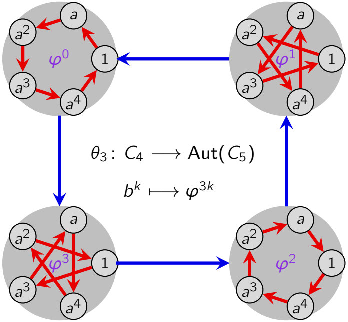
"*labeling map*"

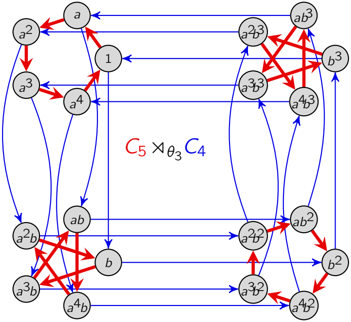
$C_4 \xrightarrow{\theta_3} \mathrm{Aut}(C_5)$

$b^k \longmapsto \varphi^{3k}$



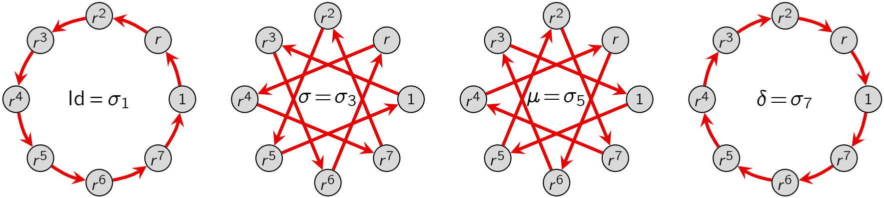
Sticking in θ_3-rewired copies yields the same Cayley diagram as $C_5 \rtimes_{\theta_1} C_4$:





Semidirect products of C_8 and C_2

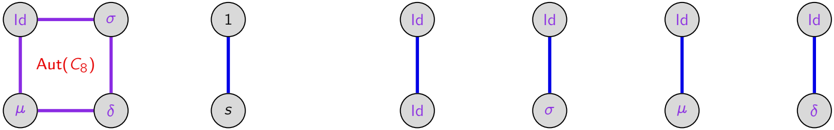
There are four automorphisms of $C_8 = \langle r \rangle$:



All three non-trivial rewirings have order 2, so $\text{Aut}(C_8) = U(8) \cong V_4$:

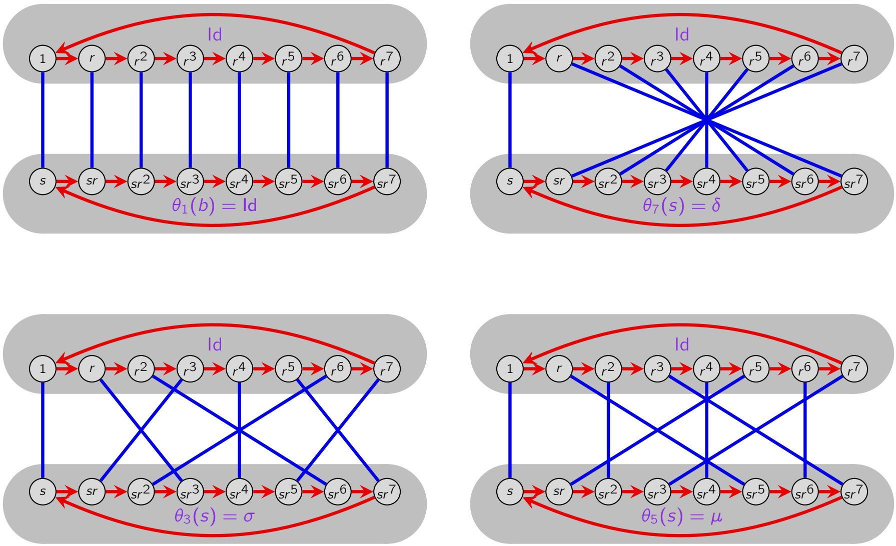
$$r \xrightarrow{\sigma} r^3 \xrightarrow{\sigma} (r^3)^3 = r^9 = r, \qquad r \xrightarrow{\mu} r^5 \xrightarrow{\mu} (r^5)^5 = r^{25} = r, \qquad r \xrightarrow{\delta} r^7 \xrightarrow{\delta} (r^7)^7 = r^{49} = r.$$

There are four labeling maps $\theta_k \colon C_2 \longrightarrow \text{Aut}(C_8) \cong V_4$:



$s \xmapsto{\theta_1} \text{Id}$ $\qquad s \xmapsto{\theta_3} \sigma$ $\qquad s \xmapsto{\theta_5} \mu$ $\qquad s \xmapsto{\theta_7} \delta$

The four semidirect products $C_8 \rtimes_i C_2$



Semidirect products of C_{2^m} and C_2

Lemma

For any $n \geq 3$, the equation $x^2 \equiv 1 \pmod{2^n}$ has four solutions: ± 1 and $2^{n-1} \pm 1$.

There are four "labeling maps"

$$\theta_i \colon C_2 \longrightarrow \mathrm{Aut}(C_{2^m}) \cong U(2^m) = \langle \varphi \rangle, \qquad \theta_i(b) = \varphi^i$$

one for each i of order 1 or 2 in $U(2^m)$.

Corollary

For each $n = 2^m$, there are four distinct semidirect products of C_n with C_2:

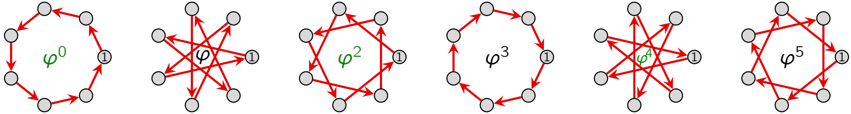
1. $C_n \rtimes_{\theta_1} C_2 \cong C_n \times C_2$,
2. $C_n \rtimes_{\theta_\sigma} C_2 \cong \mathrm{SD}_n$,
3. $C_n \rtimes_{\theta_\mu} C_2 \cong \mathrm{SA}_n$,
4. $C_n \rtimes_{\theta_\delta} C_2 \cong D_n$,

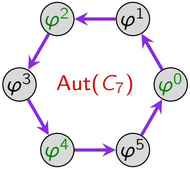
The labeling maps define the automorphisms:

$$r \xmapsto{\theta_1} r, \qquad r \xmapsto{\theta_\sigma} r^{2^{m-1}-1}, \qquad r \xmapsto{\theta_\mu} r^{2^{m-1}+1}, \qquad r \xmapsto{\theta_\delta} r^{-1}.$$

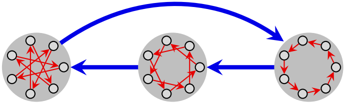
The smallest nonabelian group of odd order: $C_7 \rtimes_\theta C_3$

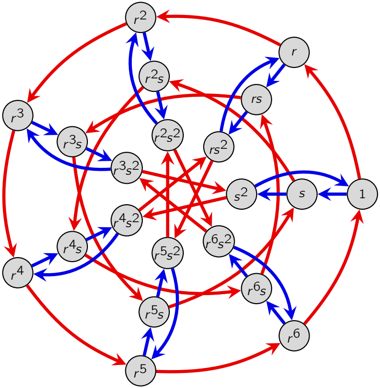
Recall that $\mathrm{Aut}(C_7) = U(7) \cong C_6 = \langle \varphi \rangle$.





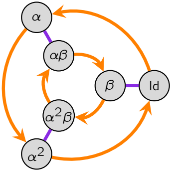
$$\begin{aligned} C_3 &\xrightarrow{\ \theta\ } \mathrm{Aut}(C_7) \\ s^k &\longmapsto \varphi^{2k} \end{aligned}$$

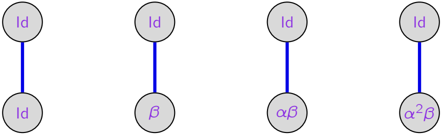




The construction of $V_4 \rtimes C_2$

There are four labeling maps: $\theta_i \colon C_2 \longrightarrow \mathrm{Aut}(V_4) \cong D_3$:

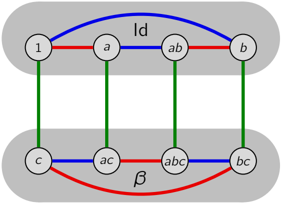




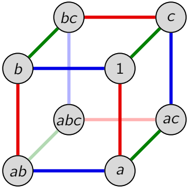
$s \stackrel{\theta}{\longmapsto} \mathrm{Id}$ $\quad s \stackrel{\theta_0}{\longmapsto} \beta$ $\quad s \stackrel{\theta_1}{\longmapsto} \alpha\beta$ $\quad s \stackrel{\theta_2}{\longmapsto} \alpha^2\beta$

The nontrivial ones define isomorphic semidirect products, $V_4 \rtimes C_2$:

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 $V_4 \rtimes C_2$?

The inner automorphism group

Definition

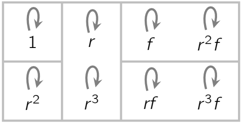
An inner automorphism of G is an automorphism $\varphi_x \in \mathrm{Aut}(G)$ defined by

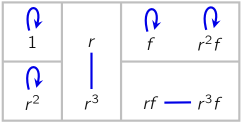
$$\varphi_x(g) := x^{-1}gx, \qquad \text{for some } x \in G.$$

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

There are four inner automorphisms of D_4:

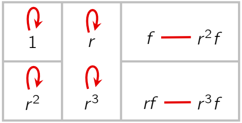
$\mathrm{Id} = \varphi_1 = \varphi_{r^2}$

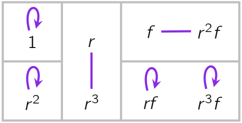




$\varphi_f = \varphi_{r^2f}$

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





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

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

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 $Z(G)$, then $\varphi_x = \varphi_y$ in $\text{Inn}(G)$:

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

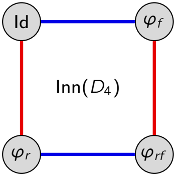
That is, if x and y are in the same coset of $Z(G)$, then $\varphi_x = \varphi_y$. (And conversely.)

Z	rZ	fZ	rfZ
1	r	f	rf
r^2	r^3	r^2f	r^3f

cosets of $Z(D_4)$ are in bijection with inner automorphisms of D_4

	$\text{cl}(r)$	$\text{cl}(f)$	$\text{cl}(rf)$
$\text{cl}(1)$: 1	r	f	rf
$\text{cl}(r^2)$: r^2	r^3	r^2f	r^3f

inner automorphisms of D_4 permute elements within conjugacy classes



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 $\mathrm{Inn}(G)$.

Proposition

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

Proof

Consider the map

$$f\colon G \longrightarrow \mathrm{Inn}(G), \qquad x \longmapsto \varphi_x,$$

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

The result is now immediate from the FHT. □

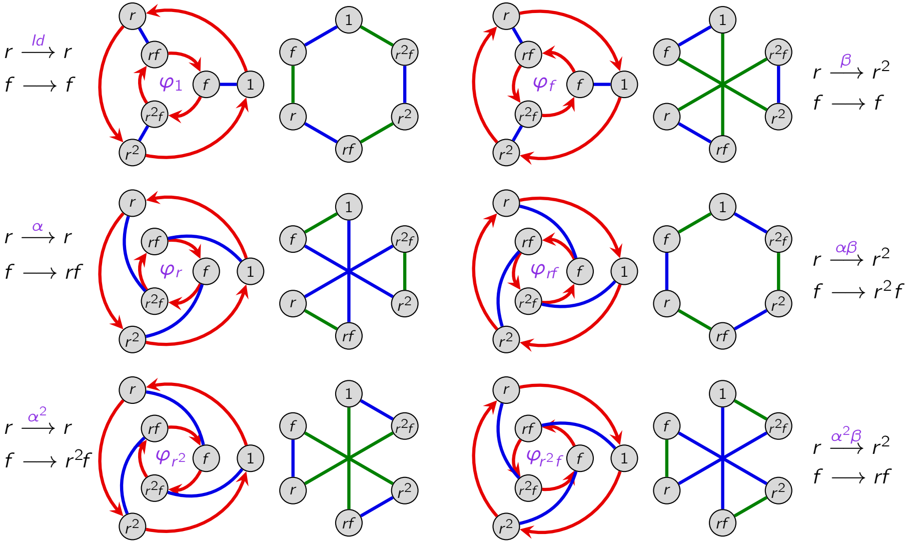
We just saw that $\mathrm{Aut}(D_3) \cong D_3$, and we know that $Z(D_3) = \langle 1 \rangle$. Therefore,

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

i.e., every automorphism is inner.

Inner automorphisms of D_3

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



Automorphisms of D_4

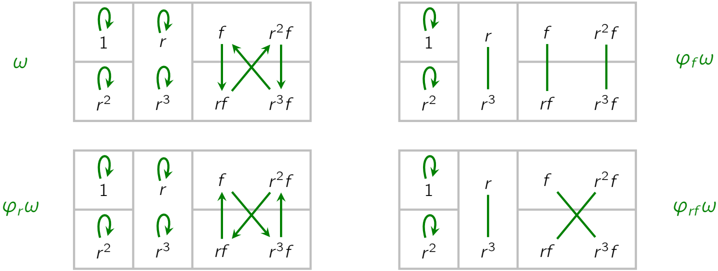
Every automorphism of $D_4 = \langle r, f \rangle$ is determined by where it sends the generators:

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

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

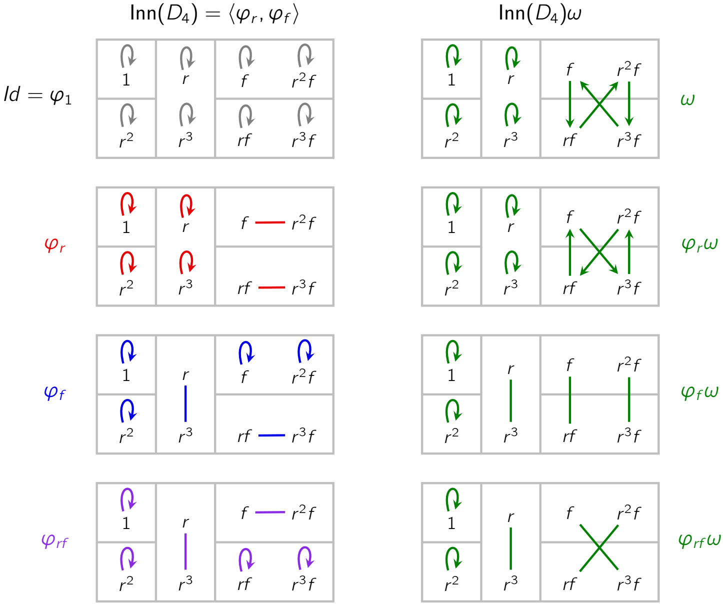
$$\omega\colon D_4 \longrightarrow D_4, \qquad \omega(r) = r, \quad \omega(f) = rf$$

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



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

The full automorphism group of D_4

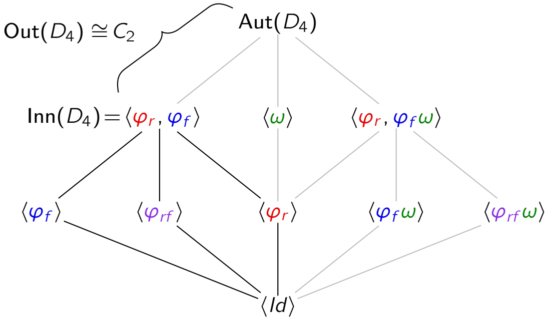


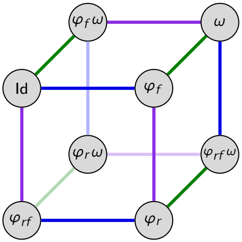
The outer automorphism group

Definition

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

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





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

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

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

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* $\phi \in \mathrm{Aut}(G)$ *sends every element to a conjugate, must* $\phi \in \mathrm{Inn}(G)$*?*"

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.

Semidirect products, algebraically

Thus far, we've see 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 $\phi \in \mathrm{Aut}(A)$ via some labeling map

$$\theta \colon B \longrightarrow \mathrm{Aut}(A).$$

Of course can all 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

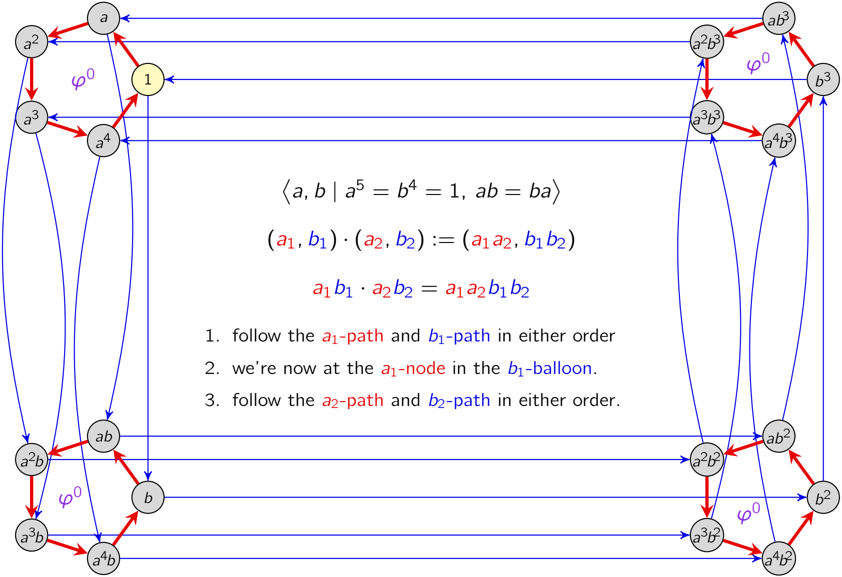
$$\theta \colon B \longrightarrow \mathrm{Aut}(A),$$

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 $C_5 \times C_4$



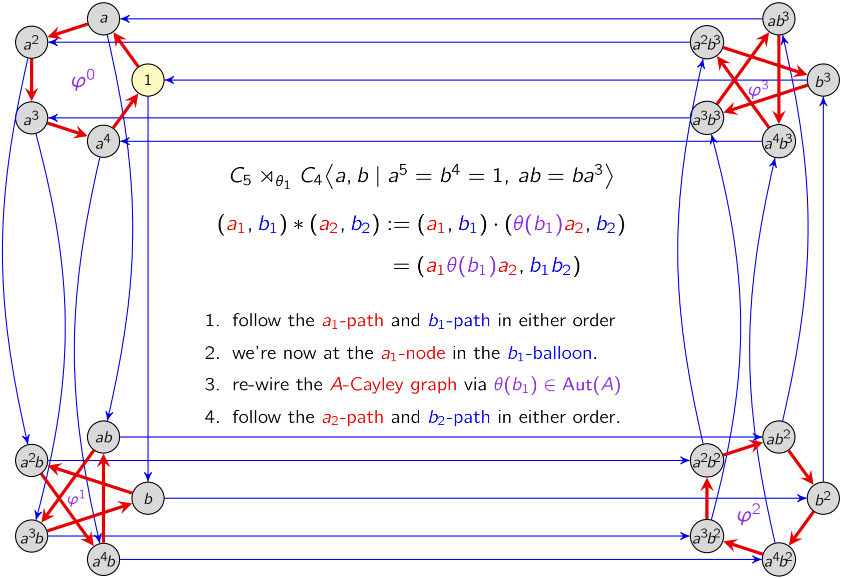
$$\langle a, b \mid a^5 = b^4 = 1,\ ab = ba \rangle$$

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

$$a_1 b_1 \cdot a_2 b_2 = a_1 a_2 b_1 b_2$$

1. follow the a_1-path and b_1-path in either order
2. we're now at the a_1-node in the b_1-balloon.
3. follow the a_2-path and b_2-path in either order.

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



$$C_5 \rtimes_{\theta_1} C_4 \langle a, b \mid a^5 = b^4 = 1,\ ab = ba^3 \rangle$$

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

$$= (a_1 \theta(b_1) a_2, b_1 b_2)$$

1. follow the a_1-path and b_1-path in either order
2. we're now at the a_1-node in the b_1-balloon.
3. re-wire the A-Cayley graph via $\theta(b_1) \in \mathrm{Aut}(A)$
4. follow the a_2-path and b_2-path in either order.

Semidirect products, algebraically

Recall how to multipy in $A \rtimes_\theta B$:

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

Lemma

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

Proof

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

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

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

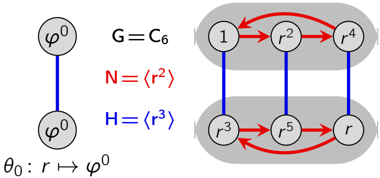
- In $A \times B$, both factors are normal (technically, $A \times \{1\}$ and $\{1\} \times B$).
- In $A \rtimes B$, the group on the "open" side of $\rtimes$ is normal.

Internal products

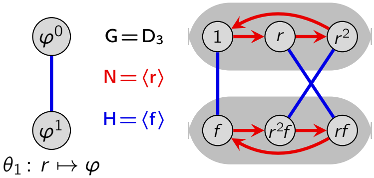
Previously, we've looked at outer products: taking two unrelated groups and constructing a direct or semidirect product.

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:



$C_6 = NH \cong N \times H$



$D_3 = NH \cong N \rtimes_\theta H$

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 $\theta \colon H \to \mathrm{Aut}(N)$?

Internal direct products

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

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

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

$$i\colon N \rtimes_\theta H \longrightarrow NH, \qquad i\colon (n,h) \longmapsto nh.$$

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) $N \cap H = \{e\}$

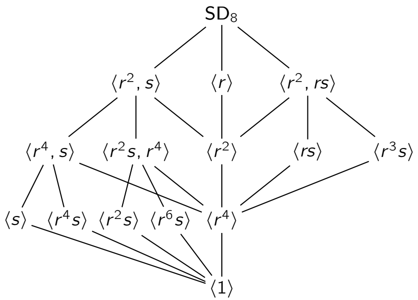
(iii) $G = NH$,

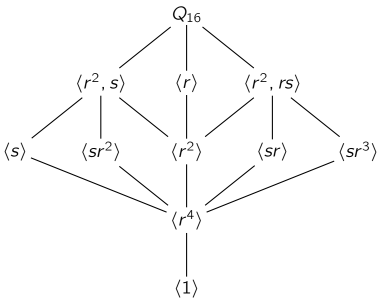
and the homomorphism θ sends h to the inner automorphism $\varphi_{h^{-1}}$:

$$\theta\colon H \longrightarrow \mathrm{Aut}(N), \qquad \theta\colon h \longmapsto \big(n \overset{\varphi_{h^{-1}}}{\longmapsto} h^{-1}nh\big).$$

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

Examples of internal semidirect products





Observations

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

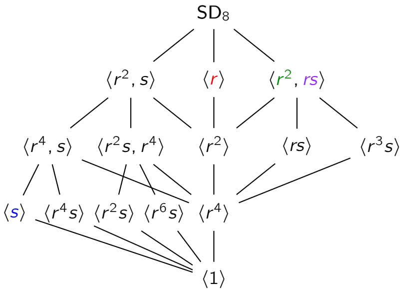
$$N = \langle r \rangle \cong C_8, \quad H = \langle s \rangle \cong C_2, \qquad \text{SD}_8 = NH \cong C_8 \rtimes_{\theta_3} C_2.$$

  or alternatively,

$$N = \langle r^2, rs \rangle \cong Q_8, \quad H = \langle s \rangle \cong C_2, \qquad \text{SD}_8 = NH \cong Q_8 \rtimes_{\theta'} C_2.$$

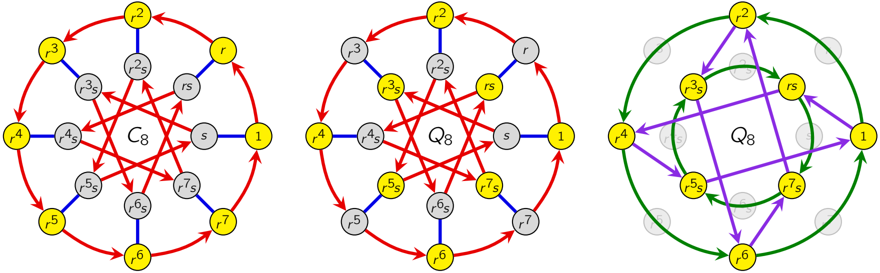
- The group Q_{16} does *not* decompose as a semidirect product!

Semidihedral groups as semidirect products



$\mathrm{SD}_8 \cong \langle r \rangle \rtimes \langle s \rangle \cong C_8 \rtimes C_2$

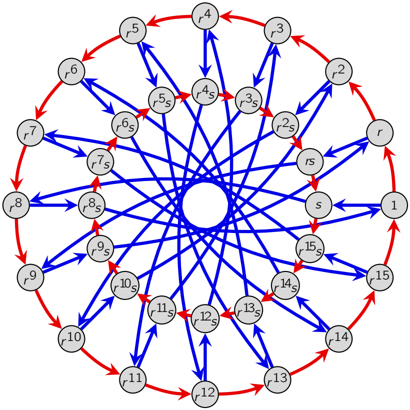
$\mathrm{SD}_8 \cong \langle r^2, rs \rangle \rtimes \langle s \rangle \cong Q_8 \rtimes C_2$

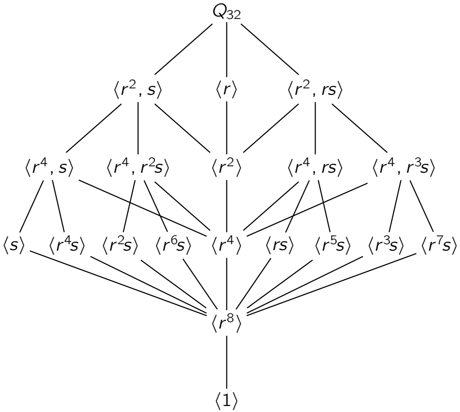


Generalized quaternion groups

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:

$$\theta\colon H \longrightarrow \mathrm{Aut}(N), \qquad \theta\colon h \longmapsto \big(n \overset{\varphi_{h^{-1}}}{\longmapsto} h^{-1}nh\big).$$

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

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

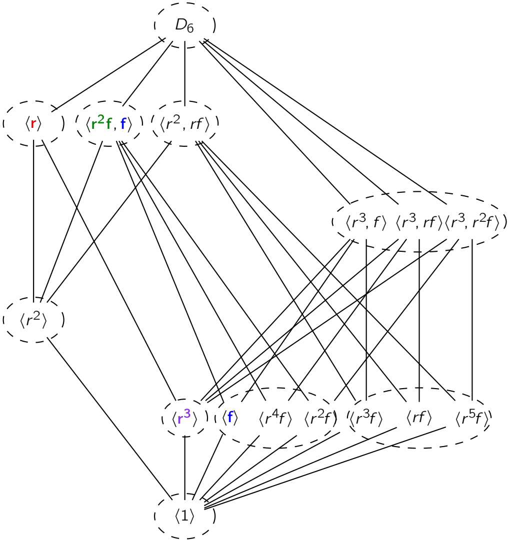
for some $\theta(h_1) \in \mathrm{Aut}(N)$.

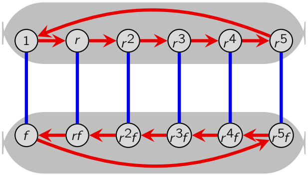
To see why $\theta(h_1)$ is the inner automorphism φ_{h_1}, note that

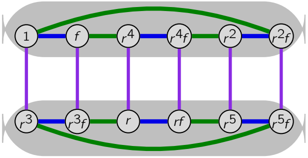
$$n_1\varphi_{h_1^{-1}}(n_2)h_1h_2 = n_1(h_1^{-1}n_2h_1)h_1h_2 = (n_1h_1) * (n_2h_2). \qquad \square$$

Internal direct and semidirect products

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







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

Alernatively, 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 diquaternion group DQ_8 is a central product two nontrivial ways:

- $\mathrm{DQ}_8 \cong C_4 \circ Q_8$
- $\mathrm{DQ}_8 \cong C_4 \circ D_4$.

Recall that $Z(\mathrm{DQ}_8) = N \cong C_4$.