

## 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  $\phi: G \rightarrow H$  between two groups satisfying

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

An **isomorphism** is a bijective homomorphism.

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

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

- **embedding** if  $\phi$  is one-to-one: “ $G$  is a *subgroup* of  $H$ .”
- **quotient map** if  $\phi$  is onto: “ $H$  is a *quotient* of  $G$ .”

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

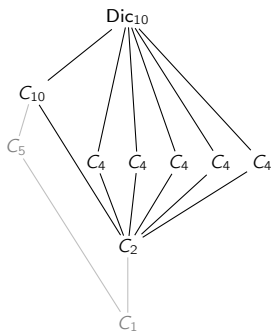
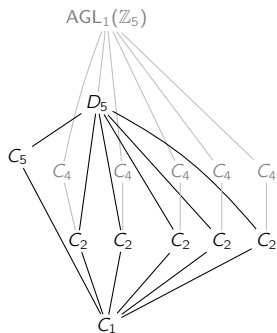
We will use standard function terminology:

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

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

## Embeddings vs. quotients: A preview

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

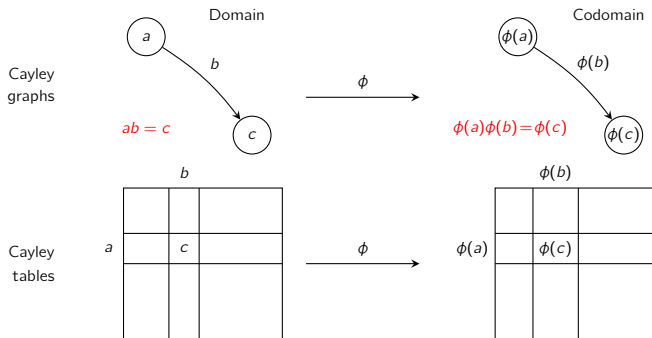


In one of these groups,  $D_5$  is **subgroup**. In the other, it arises as a **quotient**.

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  $\phi$  **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  $\phi: G \rightarrow H$  be a homomorphism. Denote the identity of  $G$  and  $H$  by  $1_G$  and  $1_H$ .

- (i)  $\phi(1_G) = 1_H$       " $\phi$  sends the identity to the identity"
- (ii)  $\phi(g^{-1}) = \phi(g)^{-1}$       " $\phi$  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,  $\phi(1_G) = 1_H$ . ✓

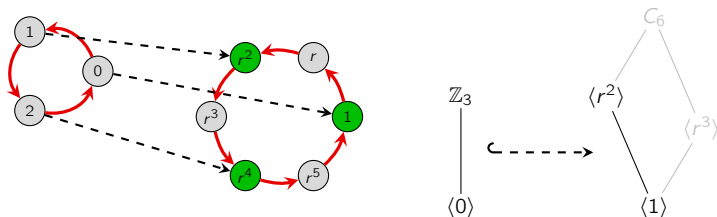
- (ii) Take any  $g \in G$ . Observe that

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

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

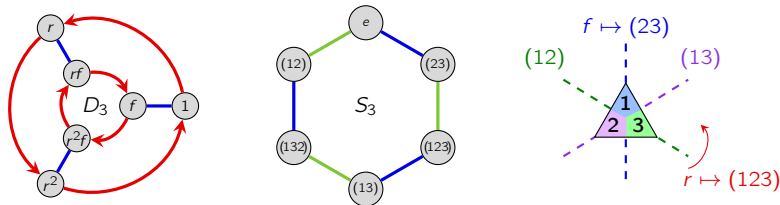
## An embedding and an isomorphisms

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



The following is an isomorphism:

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



## An example that is neither an embedding nor quotient

Consider the homomorphism  $\phi: Q_8 \rightarrow A_4$  defined by

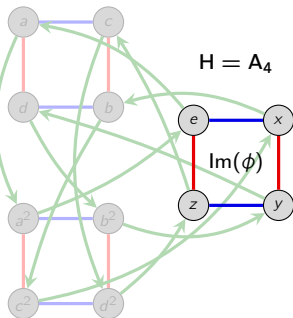
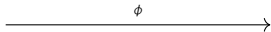
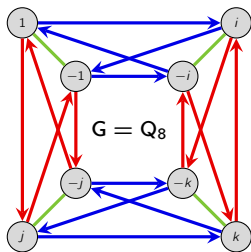
$$\phi(i) = (12)(34), \quad \phi(j) = (13)(24).$$

Using the property of homomorphisms,

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

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

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



## 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 group under multiplication, isomorphic to  $Q_8$ .

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

Formally, we have an embedding  $\phi: Q_8 \rightarrow \mathrm{GL}_4(\mathbb{R})$  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  $\phi: G \rightarrow H$  be a homomorphism. The **preimage** of  $h \in \text{Im}(\phi)$  is

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

### Definition

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

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

### Exercise

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

### Proposition

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

### Proof (sketch)

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

Let's see this by example:

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

$$\phi(1) = e$$

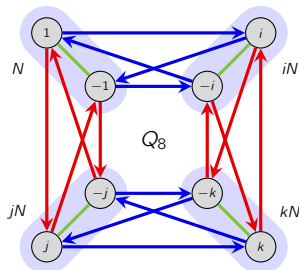
$$\phi(-1) = \phi(i^2) = \phi(i)^2 = v^2 = e$$

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

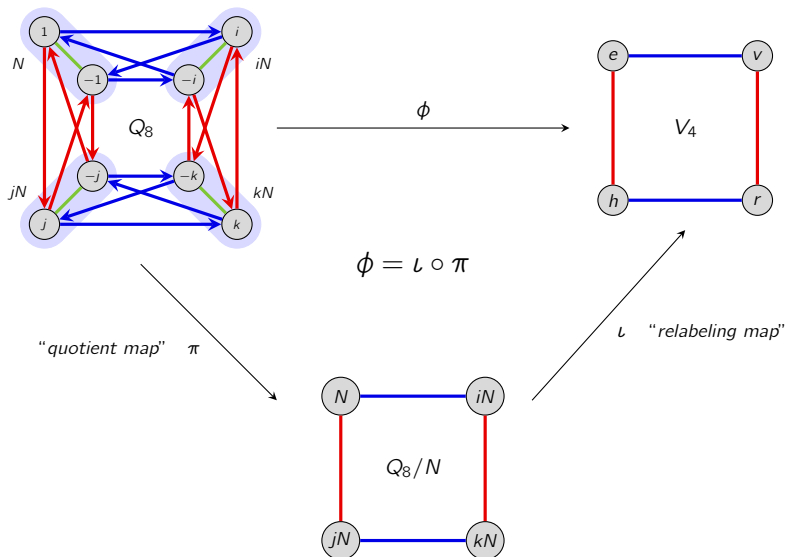
$$\phi(-k) = \phi(ji) = \phi(j)\phi(i) = hv = r$$

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

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



# Visualizing the FHT via Cayley graphs



## Visualizing the FHT via Cayley tables

Here's another way to think about the homomorphism

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

as the composition of:

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

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	N	1	iN	-iN	jN	-jN	kN	-kN
i	iN	-iN	1	N	kN	-kN	jN	-jN
-i	-iN	iN	-iN	1	-kN	kN	jN	-jN
j	jN	-jN	-kN	kN	1	N	iN	-iN
-j	-jN	jN	kN	-kN	1	-iN	iN	-iN
k	kN	-kN	jN	-jN	-iN	iN	1	N
-k	-kN	kN	-jN	jN	iN	-iN	1	-iN

$\xrightarrow{\nu}$

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	e	1	v	-v	h	-h	r	-r
i	i	-i	1	e	k	-k	j	-j
-i	-i	i	-i	1	-k	k	j	-j
j	j	-j	-k	k	1	e	v	-v
-j	-j	j	k	-k	1	-e	v	-v
k	k	-k	j	-j	-i	i	1	e
-k	-k	k	-j	j	i	-i	1	-e

# 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

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

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

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

$$aN = bN \implies b^{-1}aN = N \implies b^{-1}a \in N.$$

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

$$1_H = \phi(b^{-1}a) = \phi(b^{-1})\phi(a) = \phi(b)^{-1}\phi(a) \implies \phi(a) = \phi(b).$$

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

- Show  $\iota$  is a homomorphism.

$\iota(aN \cdot bN)$	$=$	$\iota(abN)$	$(aN \cdot bN := abN)$
	$=$	$\phi(ab)$	(definition of $\iota$ )
	$=$	$\phi(a)\phi(b)$	( $\phi$ is a homom.)
	$=$	$\iota(aN)\iota(bN)$	(definition of $\iota$ ) ✓

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

### Proof (cont.)

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

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

✓

- Show  $\iota$  is surjective (onto).

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

✓

### Useful technique

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

- Define  $\phi: G/N \rightarrow H$  and prove it's a **well-defined**, **bijective**, **homomorphism**.
- Define  $\phi: G \rightarrow H$  and prove that it's a **surjective homomorphism**, and  **$\text{Ker } \phi = N$** .

## Consequences of the FHT

Let's 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

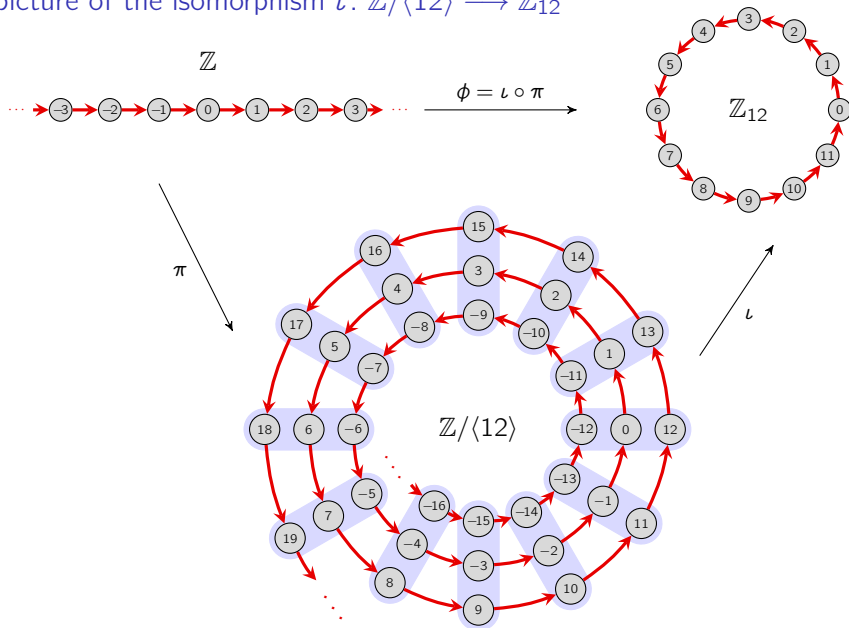
$$\text{if } aN = bN, \text{ then } \iota(aN) = \iota(bN) \text{ (that is, } \phi(a) = \phi(b) \text{) holds.}$$

### Remark

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



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:** 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  $N$ .

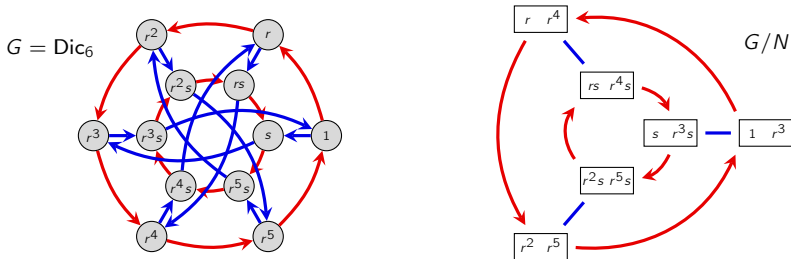
Moreover, “most properties” of  $H/N \leq G/N$  are inherited from  $H \leq G$ .

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  $N$ .”

“shoebboxes; lids on”

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

$$\langle r \rangle \leq G$$

“shoebboxes; lids off”

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

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

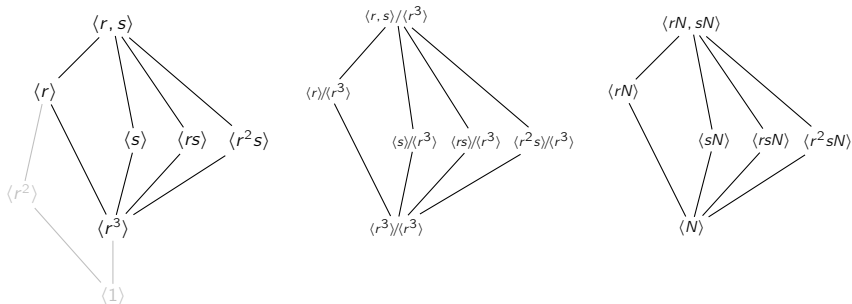
“shoes out of the box”

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

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

## 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"*

$r^2N$	$r^5sN$
$rN$	$rsN$
$N$	$sN$

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

## 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

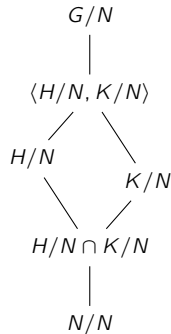
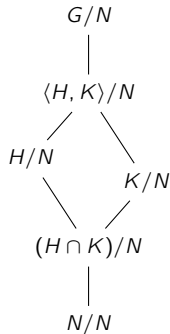
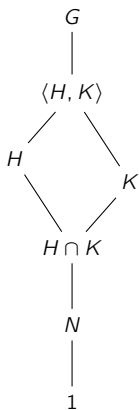
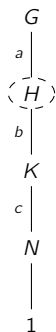
1. Subgroups of the quotient  $G/N$  are quotients of the subgroup  $H \leq G$  that contain  $N$ .
2.  $H/N \trianglelefteq G/N$  if and only if  $H \trianglelefteq G$
3.  $[G/N : H/N] = [G : H]$
4.  $H/N \cap K/N = (H \cap K)/N$
5.  $\langle H/N, K/N \rangle = \langle H, K \rangle/N$
6.  $H/N$  is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

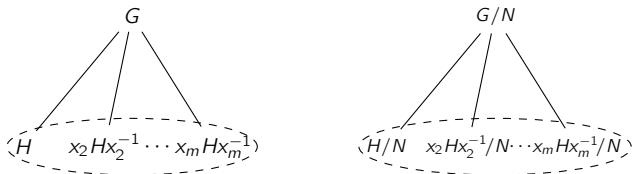
We've already interpreted the the first part.

Here's what the next four parts say.

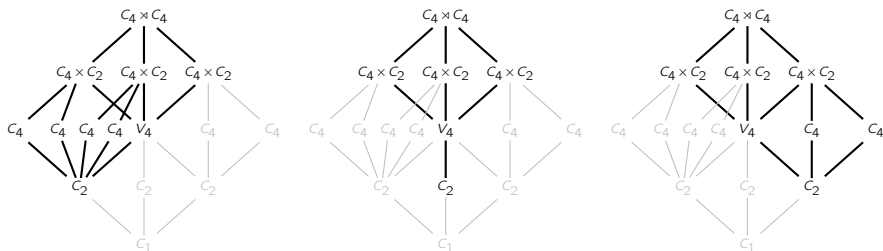


## The correspondence theorem: subgroups of quotients

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  $C_4 \times C_4$  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

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

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 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  $N \leq H \leq G$ .

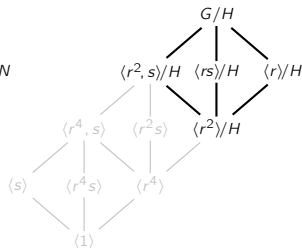
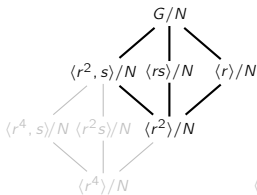
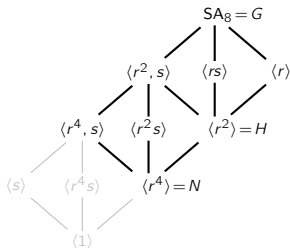
Moreover, if  $H \trianglelefteq G$ , then  $H/N \trianglelefteq G/N$ . In this case, we can ask:

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

### Fraction theorem

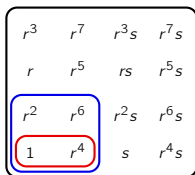
Given a chain  $N \leq H \leq G$  of normal subgroups of  $G$ ,

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

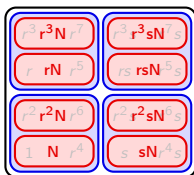


# The fraction theorem: quotients of quotients

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

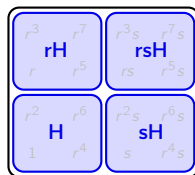


$$N \leq H \leq G$$



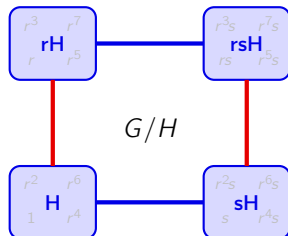
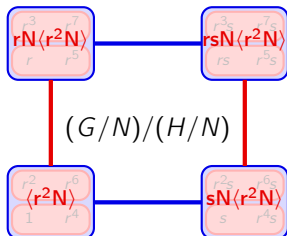
$$G/N = \langle rN, sN \rangle \cong C_4 \times C_2$$

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



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

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



# 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  $\phi$  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.,  $\phi(g_1N) = \phi(g_2N)$ . ✓
- $\phi$  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.

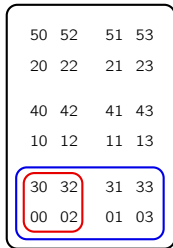
Consider the subgroups  $N = \langle 30, 02 \rangle \cong V_4$  and  $H = \langle 30, 01 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ .

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

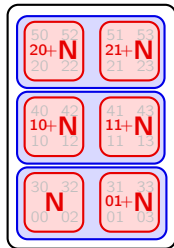
$$G/N = \{N, 01+N, 10+N, 11+N, 20+N, 21+N\}, \quad H/N = \{N, 01+N\}$$

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

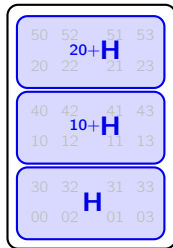
$$(G/N)/(H/N) = \{\{N, 01+N\}, \{10+N, 11+N\}, \{20+N, 21+N\}\}.$$



$$N \leq H \leq G$$



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



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

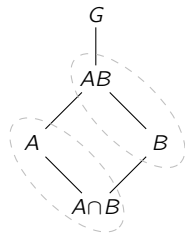
## The diamond theorem: quotients of products by factors

### 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

$$\phi: A \longrightarrow AB/B, \quad \phi: a \longmapsto aB.$$

If we can show:

1.  $\phi$  is a homomorphism,
2.  $\phi$  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

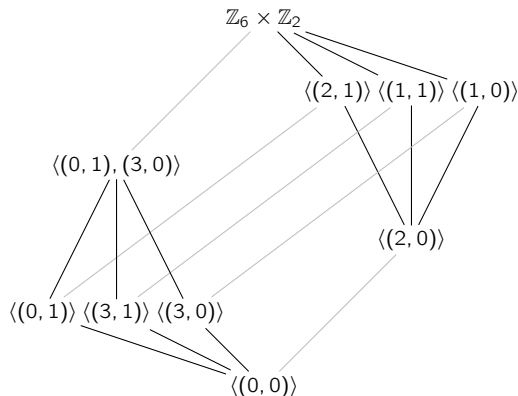
Let  $A, B \leq G$ , with one of them normalizing the other. Then  $|AB| = \frac{|A| \cdot |B|}{|A \cap B|}$ .

## The diamond theorem: 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  $A \cap B = \langle (0, 0) \rangle$ .

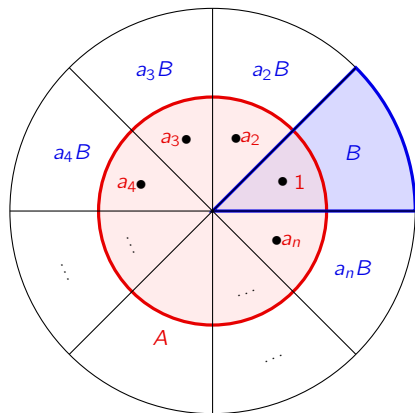
Let's interpret the diamond theorem  $AB/B \cong A/A \cap B$  in terms of the subgroup lattice.



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

$AB/B$  = {large pizza slices}

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

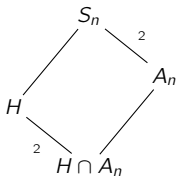
**Diamond theorem:**  $AB/B \cong A/(A \cap B)$



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

By the diamond theorem,

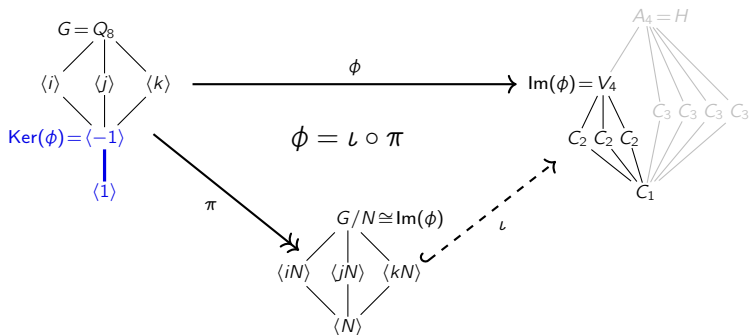
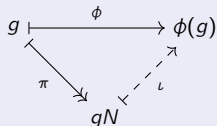
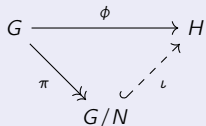
$$H/(H \cap A_n) = HA_n/A_n = S_n/A_n \cong C_2.$$

□

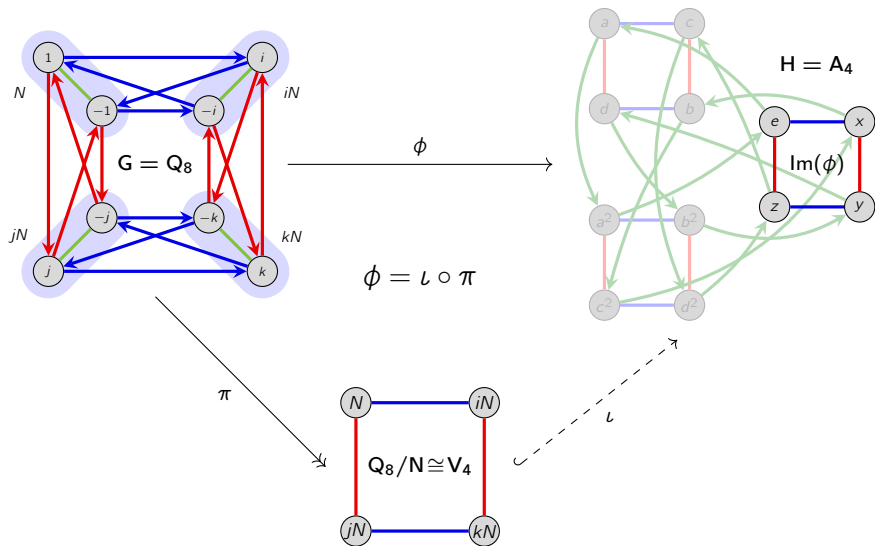
# A generalization of the FHT

## Theorem (exercise)

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



# A generalization of the FHT

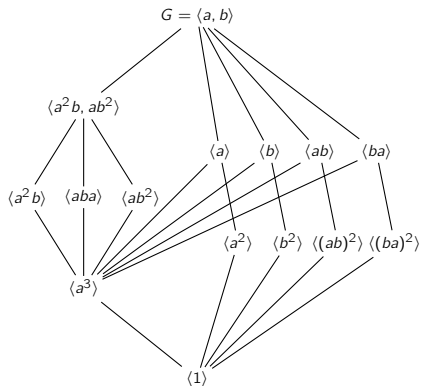


# The “subgroup” and “quotient” operations commute

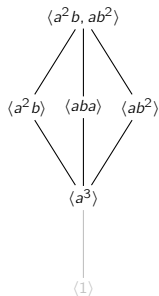
## Key idea

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

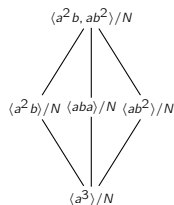
**Example:** Consider the group  $G = \text{SL}_2(\mathbb{Z}_3)$ .



subgroup  $H \cong Q_8$



$H/N \cong V_4$



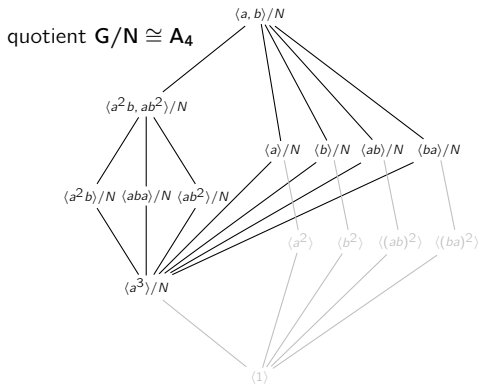
“quotient of the subgroup”

# The “subgroup” and “quotient” operations commute

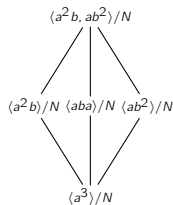
## Key idea

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

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



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

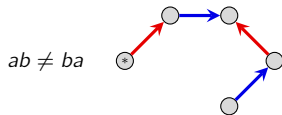
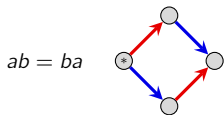


“subgroup of the quotient”

## Commutators

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

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



### Definition

The **commutator subgroup** of  $G$  is

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

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

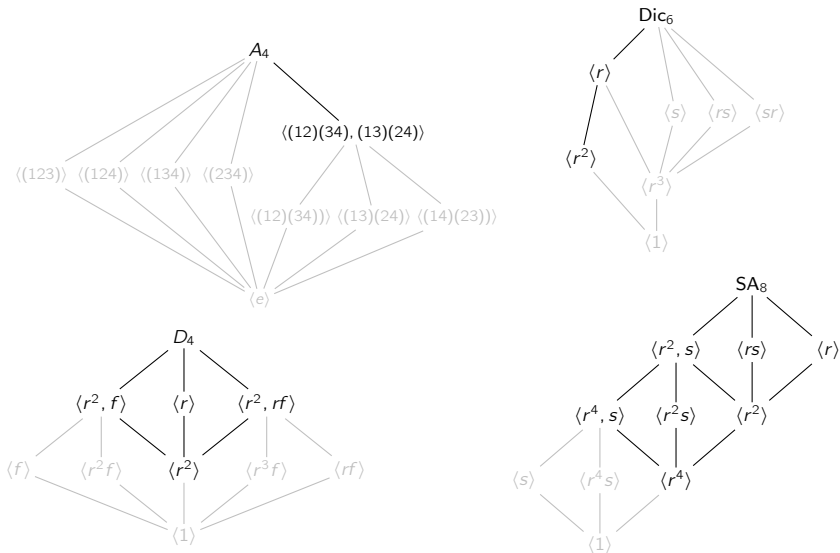
### Definition

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 identify the commutator subgroup  $G$  and abelianization by inspection, from the subgroup lattice.



# Automorphisms

An **automorphism** of  $G$  is a 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

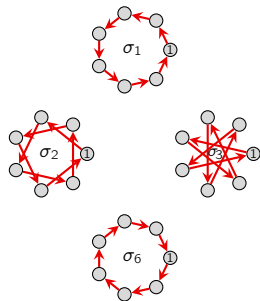
$$\sigma_a: \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad \sigma_a(1) = a.$$

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

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

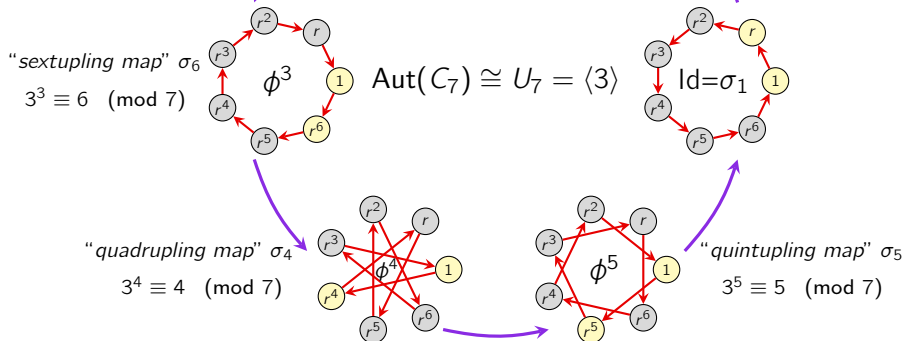
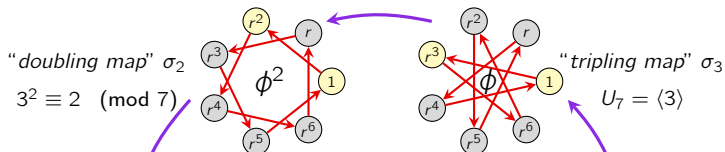
$$\text{Aut}(C_7) = \langle \sigma_3 \rangle \cong U_7$$

	$\sigma_1$	$\sigma_2$	$\sigma_3$	$\sigma_4$	$\sigma_5$	$\sigma_6$
$\sigma_1$	$\sigma_1$	$\sigma_2$	$\sigma_3$	$\sigma_4$	$\sigma_5$	$\sigma_6$
$\sigma_2$	$\sigma_2$	$\sigma_4$	$\sigma_6$	$\sigma_1$	$\sigma_3$	$\sigma_5$
$\sigma_3$	$\sigma_3$	$\sigma_6$	$\sigma_2$	$\sigma_5$	$\sigma_1$	$\sigma_4$
$\sigma_4$	$\sigma_4$	$\sigma_1$	$\sigma_5$	$\sigma_2$	$\sigma_6$	$\sigma_3$
$\sigma_5$	$\sigma_5$	$\sigma_3$	$\sigma_1$	$\sigma_6$	$\sigma_4$	$\sigma_2$
$\sigma_6$	$\sigma_6$	$\sigma_5$	$\sigma_4$	$\sigma_3$	$\sigma_2$	$\sigma_1$





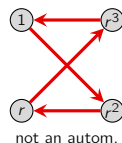
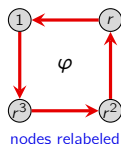
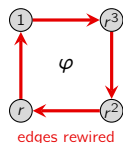
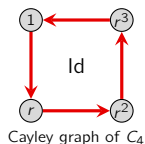
# An example: the automorphism group of $C_7$



# 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  $\text{Aut}(V_4) \cong S_3$ .
2. Every  $\phi \in \text{Aut}(D_3)$  is determined by  $\phi(r)$  and  $\phi(f)$ . Since they preserve order

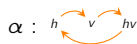
$$\phi(1) = 1, \quad \phi(r) = \underbrace{r \text{ or } r^2}_{2 \text{ choices}}, \quad \phi(f) = \underbrace{f, rf, \text{ or } r^2f}_{3 \text{ choices}}.$$

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

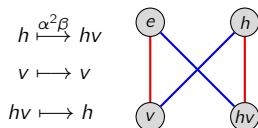
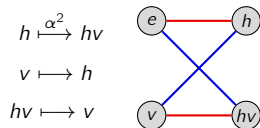
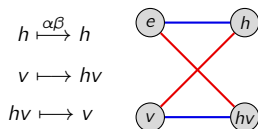
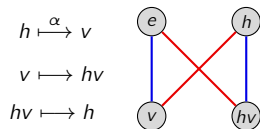
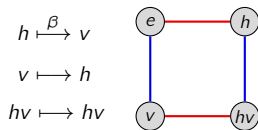
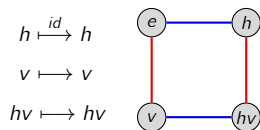
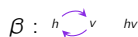
$$\begin{cases} \alpha(r) = r \\ \alpha(f) = rf \end{cases} \quad \begin{cases} \beta(r) = r^2 \\ \beta(f) = f \end{cases}$$

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

The following **permutations** are both automorphisms:



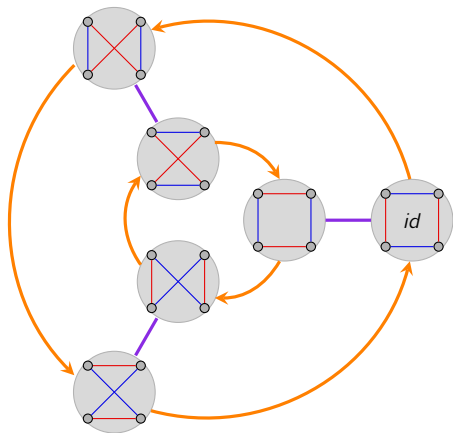
and



# 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	$\alpha$	$\alpha^2$	$\beta$	$\alpha\beta$	$\alpha^2\beta$
id	id	$\alpha$	$\alpha^2$	$\beta$	$\alpha\beta$	$\alpha^2\beta$
$\alpha$	$\alpha$	$\alpha^2$	id	$\alpha\beta$	$\alpha^2\beta$	$\beta$
$\alpha^2$	$\alpha^2$	id	$\alpha$	$\alpha^2\beta$	$\beta$	$\alpha\beta$
$\beta$	$\beta$	$\alpha^2\beta$	$\alpha\beta$	id	$\alpha^2$	$\alpha$
$\alpha\beta$	$\alpha\beta$	$\beta$	$\alpha^2\beta$	$\alpha$	id	$\alpha^2$
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	$\beta$	$\alpha^2$	$\alpha$	id



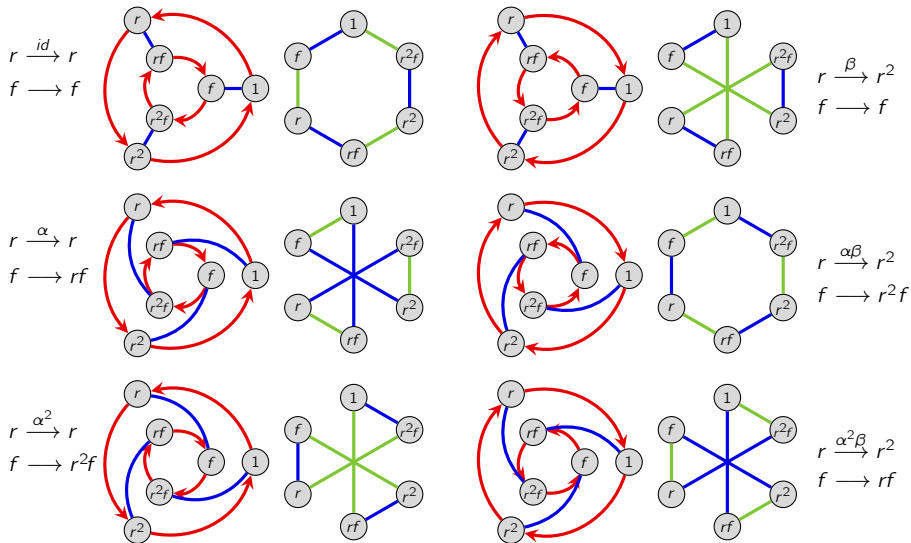
Recall that  $\alpha$  and  $\beta$  can be thought of as the permutations  $h \xrightarrow{\alpha} v \xrightarrow{\alpha} hv$  and  $h \xrightarrow{\beta} v \xrightarrow{\beta} hv$

# Automorphisms of $D_3$

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

and

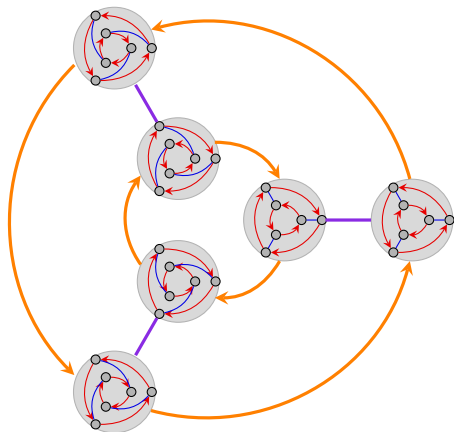
$$\beta : r \mapsto r^2 \quad f \mapsto rf \quad r^2 \mapsto r^2f$$



# Automorphisms of $D_3$

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

	$id$	$\alpha$	$\alpha^2$	$\beta$	$\alpha\beta$	$\alpha^2\beta$
$id$	$id$	$\alpha$	$\alpha^2$	$\beta$	$\alpha\beta$	$\alpha^2\beta$
$\alpha$	$\alpha$	$\alpha^2$	$id$	$\alpha\beta$	$\alpha^2\beta$	$\beta$
$\alpha^2$	$\alpha^2$	$id$	$\alpha$	$\alpha^2\beta$	$\beta$	$\alpha\beta$
$\beta$	$\beta$	$\alpha^2\beta$	$\alpha\beta$	$id$	$\alpha^2$	$\alpha$
$\alpha\beta$	$\alpha\beta$	$\beta$	$\alpha^2\beta$	$\alpha$	$id$	$\alpha^2$
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	$\beta$	$\alpha^2$	$\alpha$	$id$



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

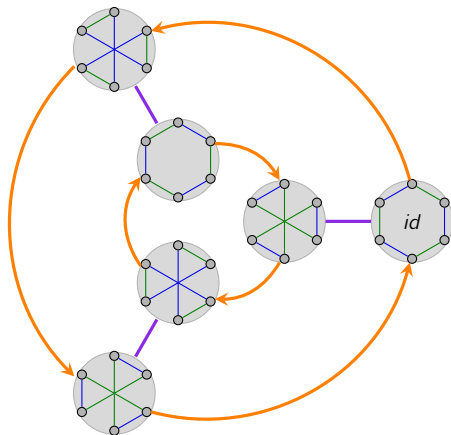
and

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

# Automorphisms of $D_3$

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

	id	$\alpha$	$\alpha^2$	$\beta$	$\alpha\beta$	$\alpha^2\beta$
id	id	$\alpha$	$\alpha^2$	$\beta$	$\alpha\beta$	$\alpha^2\beta$
$\alpha$	$\alpha$	$\alpha^2$	id	$\alpha\beta$	$\alpha^2\beta$	$\beta$
$\alpha^2$	$\alpha^2$	id	$\alpha$	$\alpha^2\beta$	$\beta$	$\alpha\beta$
$\beta$	$\beta$	$\alpha^2\beta$	$\alpha\beta$	id	$\alpha^2$	$\alpha$
$\alpha\beta$	$\alpha\beta$	$\beta$	$\alpha^2\beta$	$\alpha$	id	$\alpha^2$
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	$\beta$	$\alpha^2$	$\alpha$	id



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

and

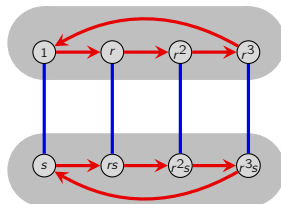
$$\beta : r \quad r^2 \quad f \quad rf \quad r^2f$$

# Semidirect products

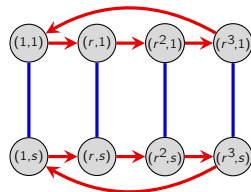
Consider the following “inflation” construction of the Cayley graph of a direct product:



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

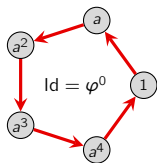
$$\theta: B \longrightarrow \text{Aut}(A),$$

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

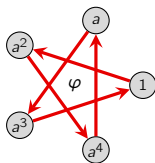


# Semidirect products

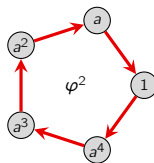
Let's construct all semidirect products of  $A = C_5 = \langle a \rangle$  with  $B = C_4 = \langle b \rangle$ .



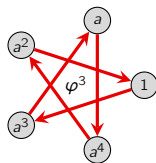
starting graph



$$a^1 \mapsto (a^1)^2 = a^2$$



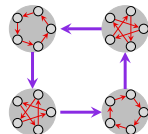
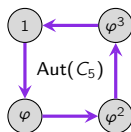
$$a^2 \mapsto (a^2)^2 = a^4$$



$$a^4 \mapsto (a^4)^2 = a^3$$

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

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



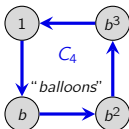
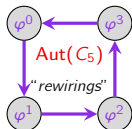
Each “labeling map”

$$\theta_i: C_4 \longrightarrow \text{Aut}(C_5)$$

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

# An example: the direct product of $C_5$ and $C_4$

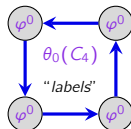
Let's construct the "trivial" semidirect product,  $C_5 \rtimes_{\theta_0} C_4 = C_5 \times C_4$ :



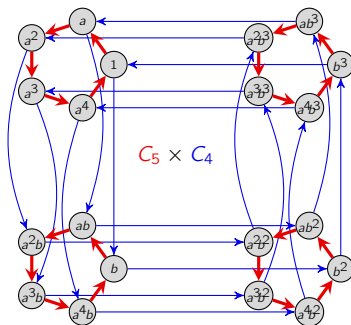
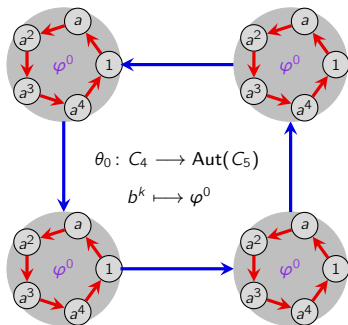
"labeling map"

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

$$b^k \mapsto \varphi^0$$

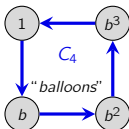
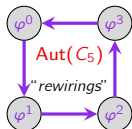


Stick in **non-rewired copies of A**, and then reconnect the **B-arrows**.



# An example: the 1<sup>st</sup> semidirect product of $C_5$ and $C_4$

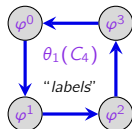
Let's construct the semidirect product  $C_5 \rtimes_{\theta_1} C_4$ :



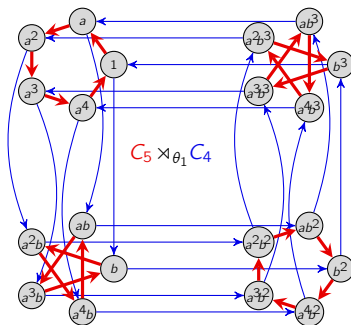
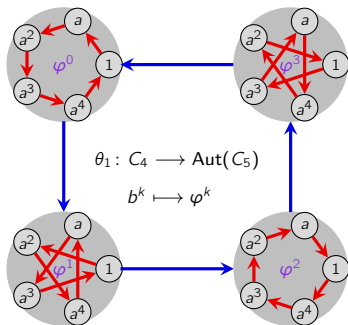
"labeling map"

$$C_4 \xrightarrow{\theta_1} \text{Aut}(C_5)$$

$$b^k \mapsto \varphi^k$$

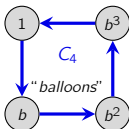
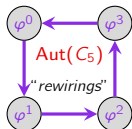


Stick in  $\theta_1$ -rewired copies of  $A$ , and then reconnect the  $B$ -arrows.



# An example: the 2<sup>nd</sup> semidirect product of $C_5$ and $C_4$

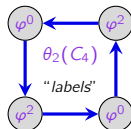
Let's now construct a different semidirect product,  $C_5 \rtimes_{\theta_2} C_4$ :



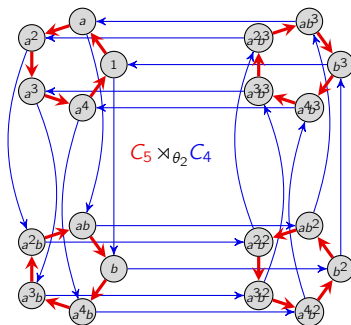
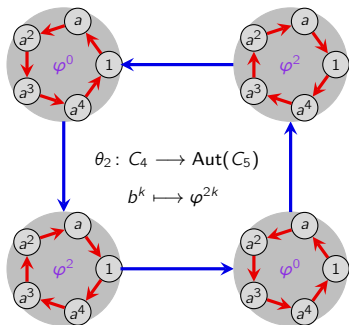
"labeling map"

$$C_4 \xrightarrow{\theta_2} \text{Aut}(C_5)$$

$$b^k \mapsto \varphi^{2^k}$$

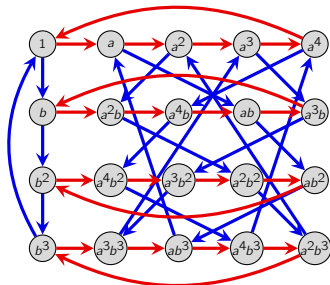
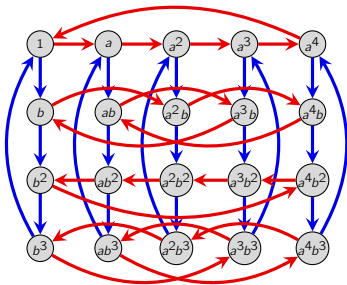


Stick in  $\theta_2$ -rewired copies of  $A$ , and then reconnect the  $B$ -arrows.

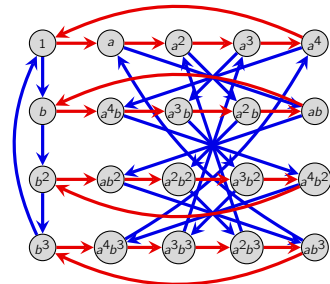
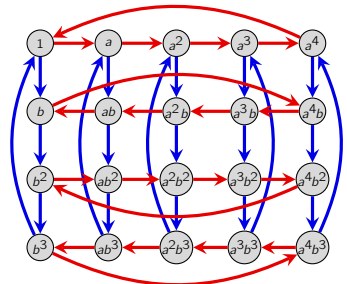


# Rewiring edges vs. re-labeling nodes

$C_5 \rtimes_{\theta_1} C_4$

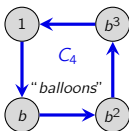
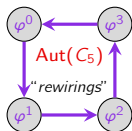


$C_5 \rtimes_{\theta_2} C_4$



# An example: the 3<sup>rd</sup> semidirect product of $C_5$ and $C_4$

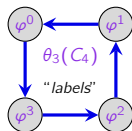
Let's construct the last semidirect product  $C_5 \rtimes_{\theta_3} C_4$ :



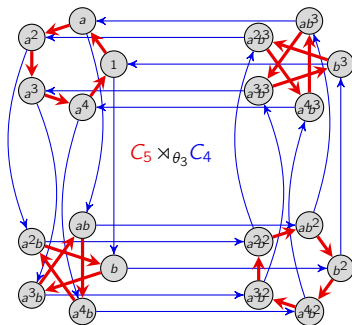
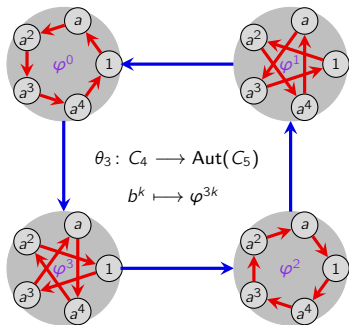
"labeling map"

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

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

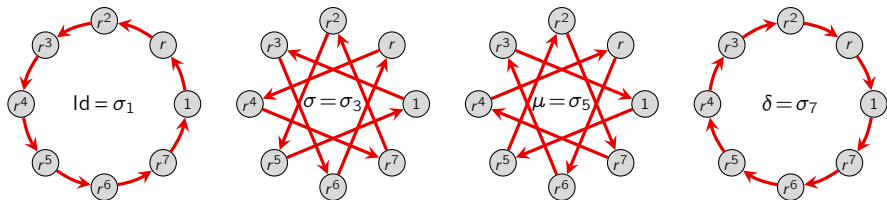


Sticking in  $\theta_3$ -rewired copies yields the same Cayley diagram as  $C_5 \rtimes_{\theta_1} C_4$ :



## Semidirect products of $C_8$ and $C_2$

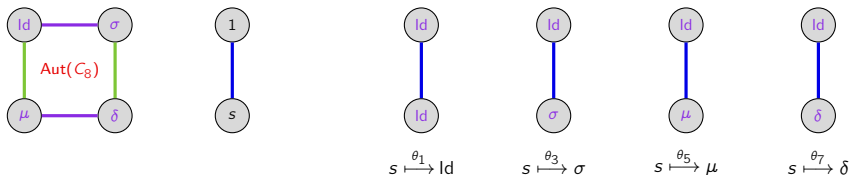
There are four automorphisms of  $C_8 = \langle r \rangle$ :



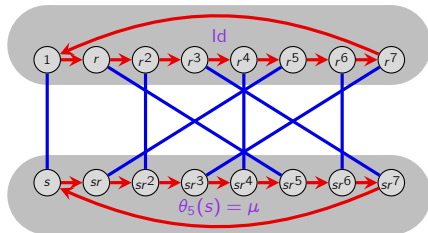
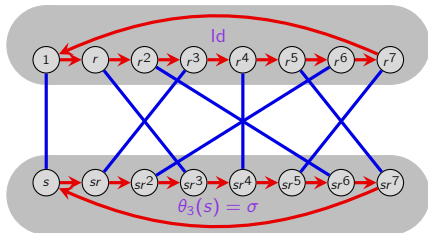
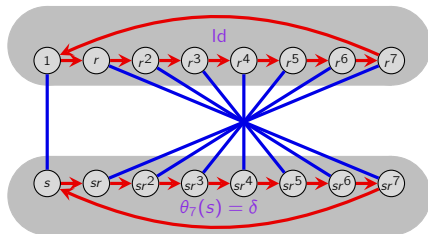
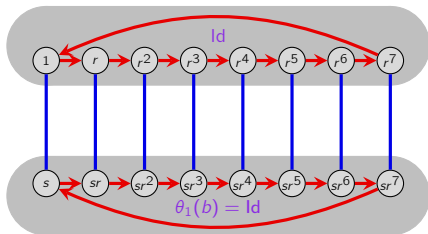
All three non-trivial rewirings have order 2, so  $\text{Aut}(C_8) = U(8) \cong V_4$ :

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

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



# 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:  $\pm 1$  and  $2^{n-1} \pm 1$ .

There are four “labeling maps”

$$\theta_i: C_2 \longrightarrow \text{Aut}(C_{2^m}) \cong U(2^m) = \langle \varphi \rangle, \quad \theta_i(b) = \varphi^i$$

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  $C_2$ :

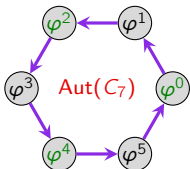
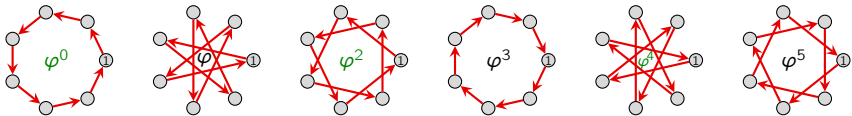
1.  $C_n \rtimes_{\theta_1} C_2 \cong C_n \times C_2$ ,
2.  $C_n \rtimes_{\theta_\sigma} C_2 \cong \text{SD}_n$ ,
3.  $C_n \rtimes_{\theta_\mu} C_2 \cong \text{SA}_n$ ,
4.  $C_n \rtimes_{\theta_\delta} C_2 \cong D_n$ ,

The labeling maps define the automorphisms:

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

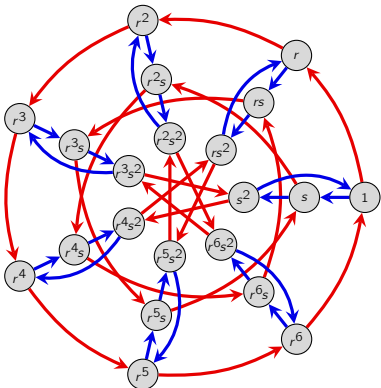
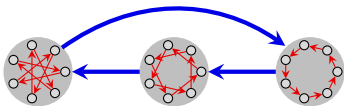
# The smallest nonabelian group of odd order: $C_7 \rtimes_{\theta} C_3$

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



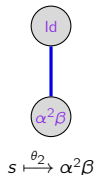
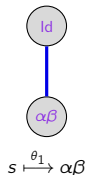
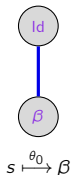
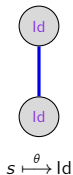
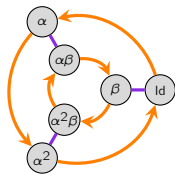
$$C_3 \xrightarrow{\theta} \text{Aut}(C_7)$$

$$s^k \mapsto \varphi^{2^k}$$



# The construction of $V_4 \rtimes C_2$

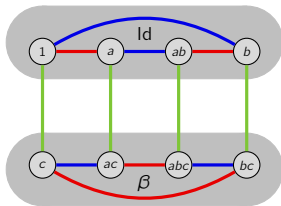
There are four labeling maps:  $\theta_i: C_2 \rightarrow \text{Aut}(V_4) \cong D_3$ :



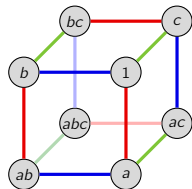
The nontrivial ones define isomorphic semidirect products,  $V_4 \rtimes C_2$ :



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

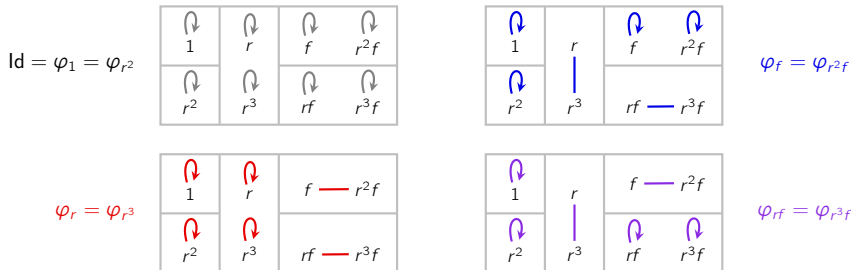
## Definition

An **inner automorphism** of  $G$  is an automorphism  $\varphi_x \in \text{Aut}(G)$  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  $D_4$ :



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)

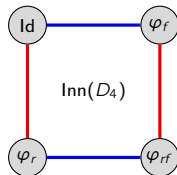
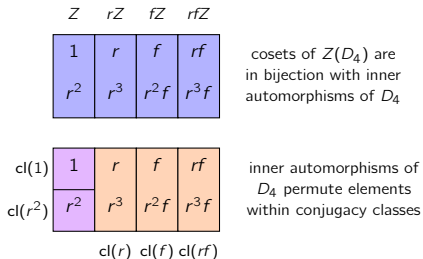
$\text{Inn}(G)$  is a normal subgroup of  $\text{Aut}(G)$ .

## 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.)



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

The result is now immediate from the FHT. □

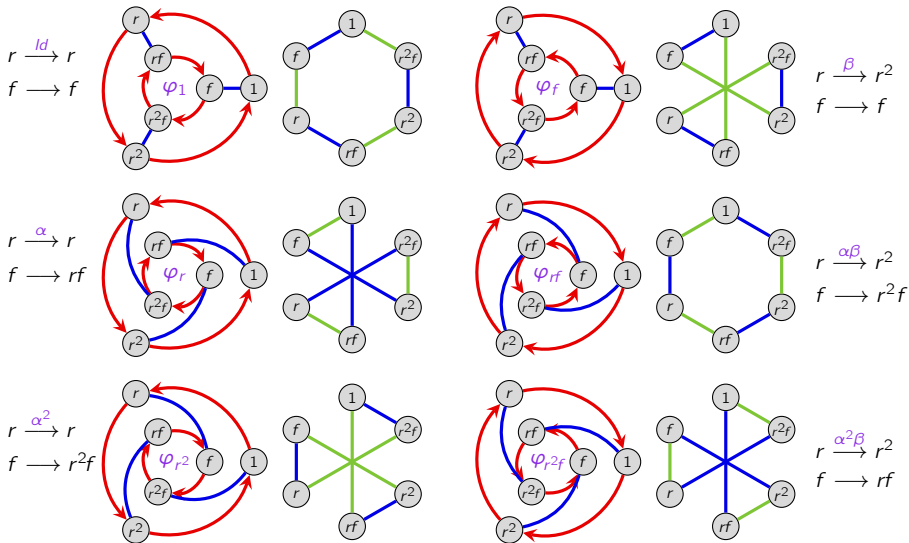
We just saw that  $\text{Aut}(D_3) \cong D_3$ , and we know that  $Z(D_3) = \langle 1 \rangle$ . Therefore,

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

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 $D_4$

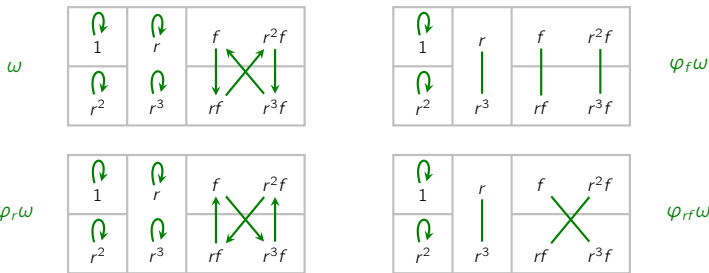
Every automorphism of  $D_4 = \langle r, f \rangle$  is determined by where it sends the generators:

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

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.



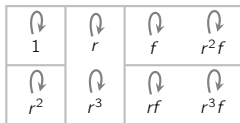
$$\text{Aut}(D_4) = \{Id, \varphi_r, \varphi_f, \varphi_{rf}, \omega, \varphi_r \omega, \varphi_f \omega, \varphi_{rf} \omega\} = \text{Inn}(D_4) \cup \text{Inn}(D_4)\omega \cong D_4.$$



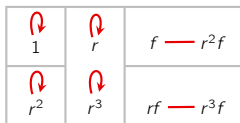
# The full automorphism group of $D_4$

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

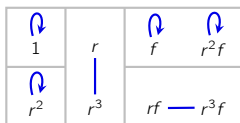
$$Id = \varphi_1$$



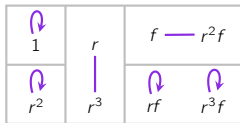
$$\varphi_r$$



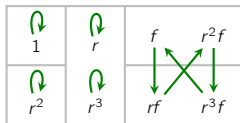
$$\varphi_f$$



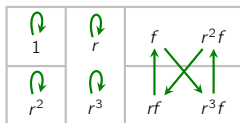
$$\varphi_{rf}$$



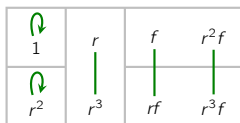
$$\text{Inn}(D_4)\omega$$



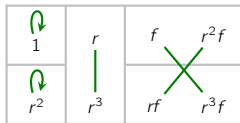
$$\omega$$



$$\varphi_r\omega$$



$$\varphi_f\omega$$



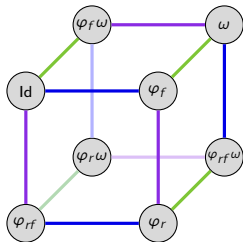
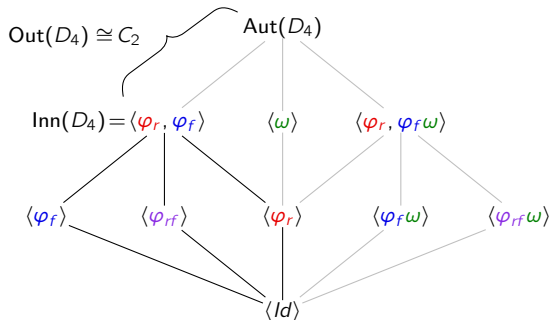
$$\varphi_{rf}\omega$$

# 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.

## 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**

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

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

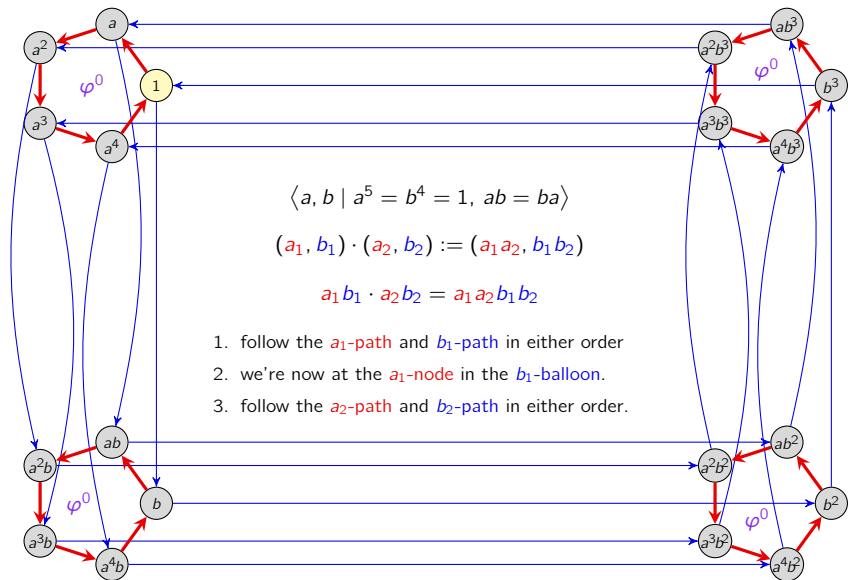
$$\theta: B \longrightarrow \text{Aut}(A),$$

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

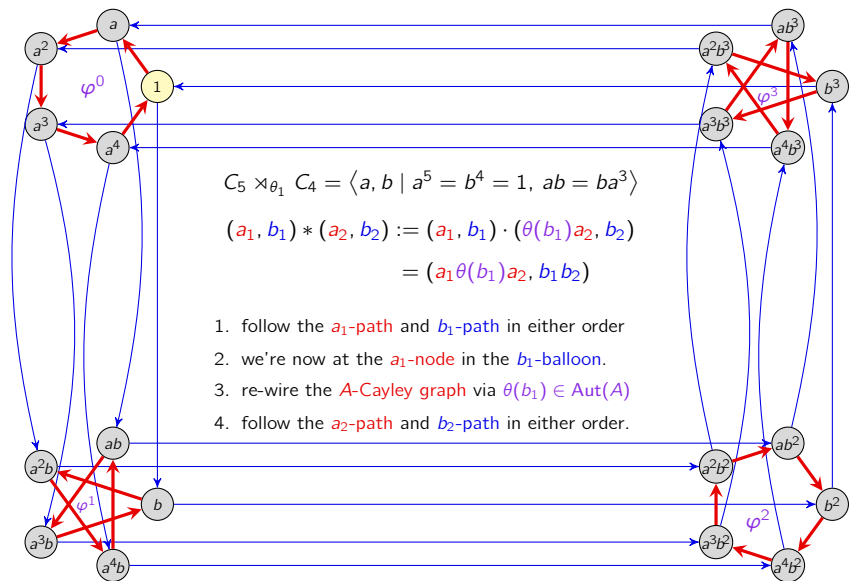
$$(a_1, b_1) * (a_2, b_2) := (a_1, b_1) \cdot (\theta(b_1)a_2, b_2) = (a_1\theta(b_1)a_2, b_1 b_2).$$

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 $C_5 \rtimes_{\theta} C_4$



## Semidirect products, algebraically

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

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

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

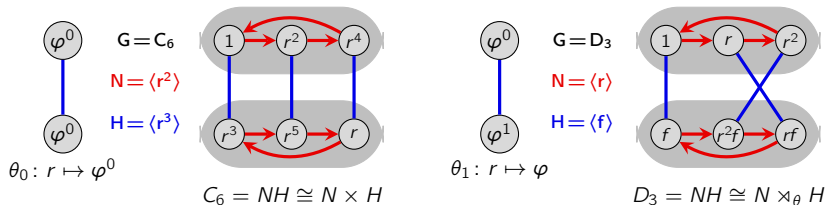
- In  $A \times B$ , both factors are normal (technically,  $A \times \{1\}$  and  $\{1\} \times B$ ).
- In  $A \rtimes B$ , the group on the “open” side of  $\rtimes$  is normal.

## 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:



### 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:

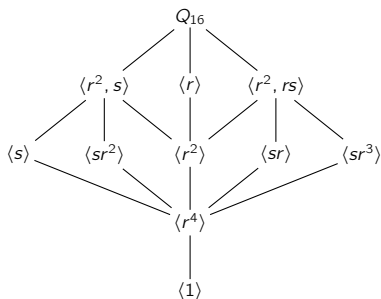
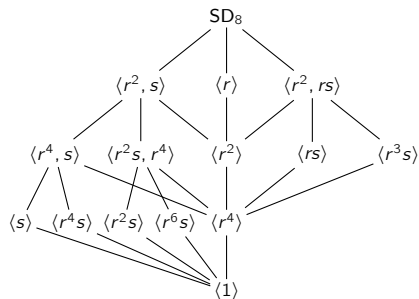
- (i)  $N$  is normal in  $G$
- (ii)  $N \cap H = \{e\}$
- (iii)  $G = NH$ ,

and the homomorphism  $\theta$  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:

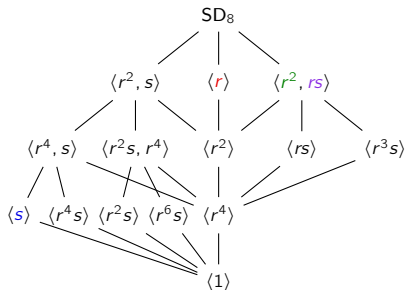
$$N = \langle r \rangle \cong C_8, \quad H = \langle s \rangle \cong C_2, \quad SD_8 = NH \cong C_8 \rtimes_{\theta_3} C_2.$$

or alternatively,

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

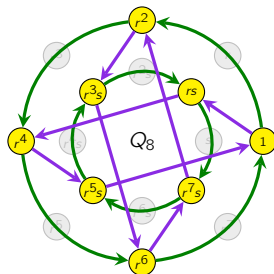
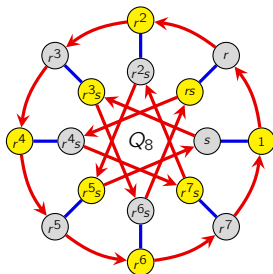
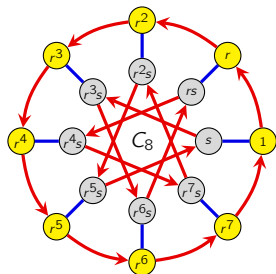
- The group  $Q_{16}$  does *not* decompose as a semidirect product!

# Semidihedral groups as semidirect products



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

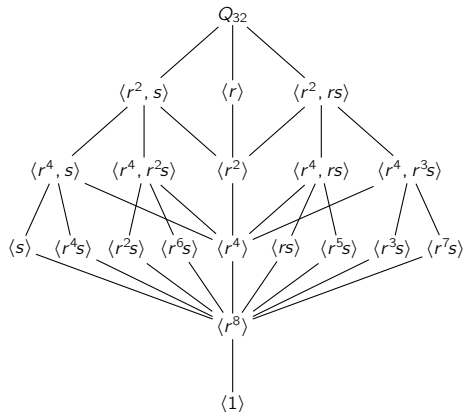
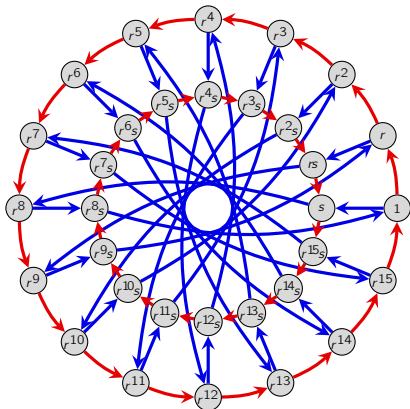
$$SD_8 \cong \langle r^2, rs \rangle \rtimes \langle s \rangle \cong Q_8 \rtimes C_2$$



## 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  $\theta$  sends  $h$  to the inner automorphism  $\varphi_h$ :

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

## Proof

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

Take  $n_1h_1$  and  $n_2h_2$  in  $NH$ . Their product is

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

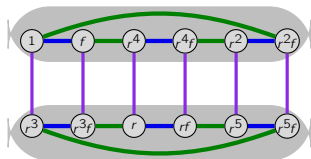
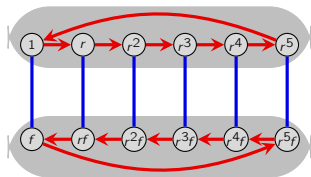
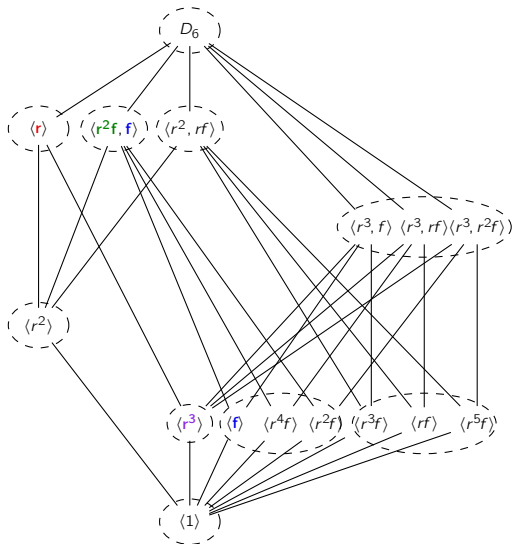
for some  $\theta(h_1) \in \text{Aut}(N)$ .

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

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 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 diquaternion 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

