Chapter 4: Maps between groups

Matthew Macauley

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

Math 4120 & 4130, Visual Algebra

Homomorphisms

Throughout this course, we've said that two groups are isomorphic if for some generating sets, they have Cayley graphs with the same structure.

This can be formalized by a "structure-preserving" function $\phi\colon G \to H$ between groups, called a homomorphism.

An **isomorphism** is simply a bijective homomorphism.

What we called a *re-wiring* when constructing semidirect products is an automorphism: an isomorphism $\phi\colon G \to G$.

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

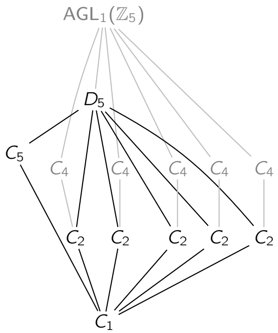
The homomorphism $\phi\colon G \to H$ is an

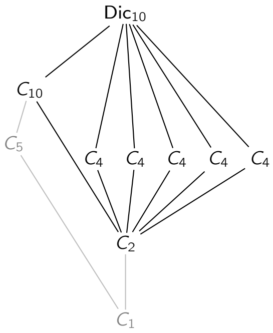
- embedding if ϕ is one-to-one: "*G is a subgroup of H.*"
- quotient map if ϕ is onto: "*H is a quotient of G.*"

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.

Embeddings vs. quotients: A preview

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





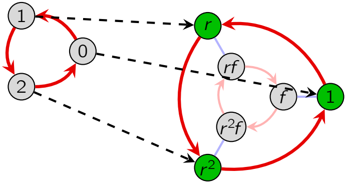
In one of these groups, D_5 is subgroup. In the other, it arises as a quotient.

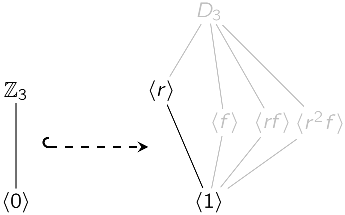
This, and much more, will be consequences of the celebrated **isomorphism theorems**.

A example embedding

When we say $\mathbb{Z}_3 \leq D_3$, we really mean that *the structure of* $\mathbb{Z}_3$ *appears in* D_3.

This can be formalized by a map $\phi\colon \mathbb{Z}_3 \to D_3$, defined by $\phi\colon n \mapsto r^n$.





In general, a homomorphism is a function $\phi\colon G \to H$ with some extra properties.

We will use standard function terminology:

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

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

The formal definition

Definition

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

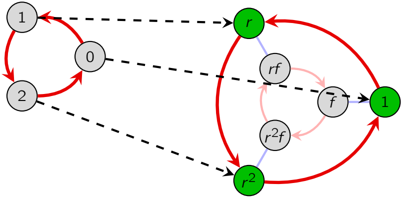
$$\phi(ab) = \phi(a)\phi(b), \qquad \text{for all } a, b \in G\,.$$

Note that the operation $a \cdot b$ is in the domain while $\phi(a) \cdot \phi(b)$ in the codomain.

For example, in this example the homomorphism condition is $\phi(a + b) = \phi(a) \cdot \phi(b)$.

$$\phi\colon \mathbb{Z}_3 \longrightarrow D_3$$

$$k \longmapsto r^k$$



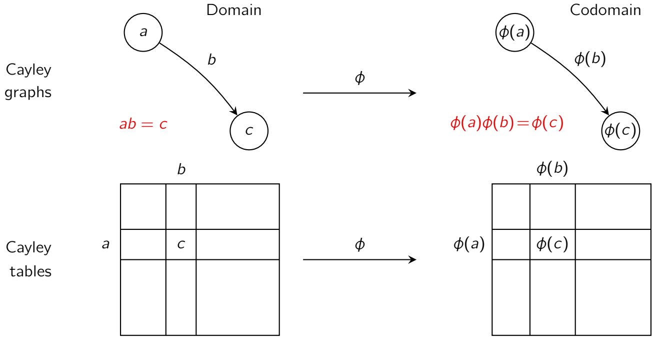
Not only is there a bijective correspondence between the elements in $\mathbb{Z}_3$ and those in the subgroup $\langle r \rangle$ of D_3, but the relationship between the corresponding nodes is the same.

Homomorphisms

Remark

Not every function from one group to another is a homomorphism! The condition $\phi(ab) = \phi(a)\phi(b)$ means that the map ϕ preserves the structure of G.

The $\phi(ab) = \phi(a)\phi(b)$ condition has visual interpretations on the level of Cayley graphs and Cayley tables.



Note that in the Cayley graphs, b and $\phi(b)$ are paths; they need not just be edges.

An example

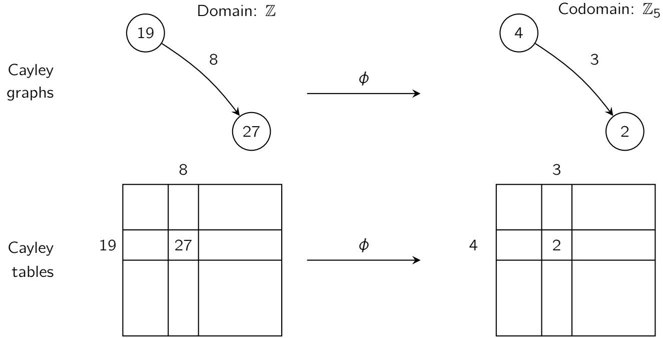
Consider the function ϕ that reduces an integer modulo 5:

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

Since the group operation is additive, the “homomorphism property” becomes

$$\phi(a+b) = \phi(a) + \phi(b)\,.$$

In plain English, this just says that one can “first add and then reduce modulo 5,” OR “first reduce modulo 5 and then add.”



Homomorphisms and generators

Remark

If we know where a homomorphism maps the generators of G, we can determine where it maps *all* elements of G.

For example, suppose $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6$ was a homomorphism, with $\phi(1) = 4$. Using this information, we can deduce:

$$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 4 + 4 = 2$$
$$\phi(0) = \phi(1+2) = \phi(1) + \phi(2) = 4 + 2 = 0.$$

Example

Suppose that $G = \langle a, b \rangle$, and $\phi \colon G \to H$, and we know $\phi(a)$ and $\phi(b)$. We can find the image of any $g \in G$. For example, for $g = a^3 b^2 ab$, we have

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

Note that if $k \in \mathbb{N}$, then $\phi(a^k) = \phi(a)^k$. What do you think $\phi(a^{-1})$ is?

Two basic properties of homomorphisms

Proposition

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 $\phi(g^{-1}) = \phi(g)^{-1}$. ✓

A word of caution

Just because a homomorphism $\phi\colon G \to H$ is determined by the image of its generators does *not* mean that every such image will work.

For example, let's try to define a homomorphism $\phi\colon \mathbb{Z}_3 \to \mathbb{Z}_4$ by $\phi(1) = 1$. Then we get

$$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 2,$$

$$\phi(0) = \phi(1+1+1) = \phi(1) + \phi(1) + \phi(1) = 3 \neq 0.$$

This is *impossible*, because $\phi(0)$ must be $0 \in \mathbb{Z}_4$.

That's not to say that there isn't a homomorphism $\phi\colon \mathbb{Z}_3 \to \mathbb{Z}_4$; note that there is always the trivial homomorphism between two groups:

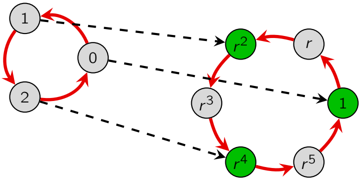
$$\phi\colon G \longrightarrow H\,, \qquad \phi(g) = 1_H \quad \text{for all } g \in G.$$

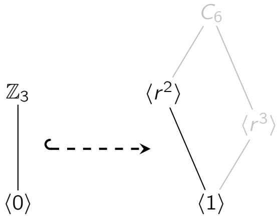
Exercise

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

Types of homomorphisms

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





It is easy to check that $\theta(a + b) = \theta(a)\theta(b)$: The red arrow in $\mathbb{Z}_3$ (representing 1) gets mapped to the 2-step path representing r^2 in C_6.

A homomorphism $\phi\colon G \to H$ that is one-to-one or "injective" is called an embedding: the group G "embeds" into H as a subgroup.

If $\phi(G) = H$, then ϕ is onto, or surjective, and we call it a quotient.

Definition

A homomorphism that is both injective and surjective is an **isomorphism**.

An **automorphism** is an isomorphism from a group to itself.

An example that is neither an embedding nor quotient

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

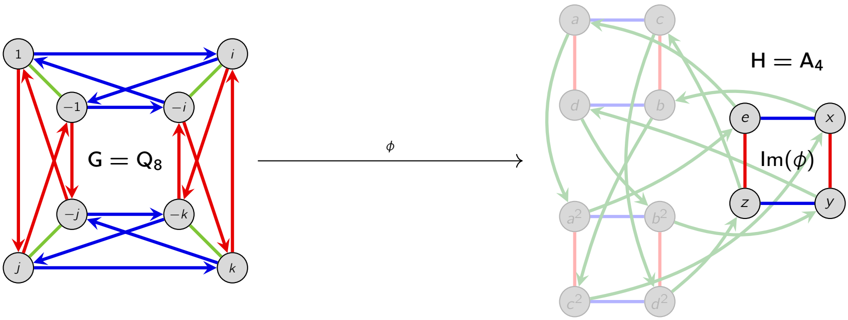
$$\phi(i) = (12)(34), \qquad \phi(j) = (13)(24).$$

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 $g = i, j, k$.



An example of an isomorphism

We have already seen that D_3 is isomorphic to S_3.

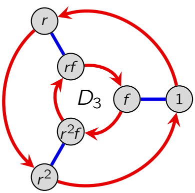
Which means that there's a bijective correspondence between these sets: $f\colon D_3 \to S_3$.

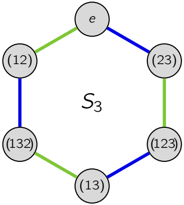
But not just any bijection will do. Intuitively,

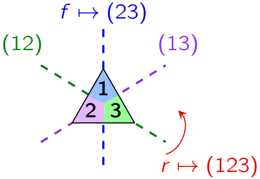
- (123) and (132) should be the rotations
- (12), (13), and (23) should be the reflections
- The identity permutation must be the identity symmetry.

It is easy to verify that the following is an isomorphism:

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







However, there are other isomorphisms between these groups.

Group representations

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

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

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

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

If $\phi \colon G \to H$ is onto, it is a quotient map.

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

Definition

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

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

The kernel is the "group theoretic" analogue of the nullspace of a matrix.

Another way to define the kernel is as the preimage of the identity.

Definition

If $\phi \colon G \to H$ is a homomorphism and $h \in \mathrm{Im}(\phi)$, define the preimage of h to be the set

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

Let's do some examples, and observe what the kernels and preimages are.

An example of a quotient

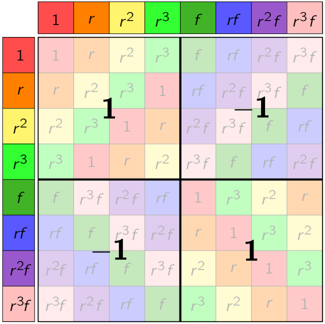
Recall that $C_2 = \{e^{0\pi i}, e^{1\pi i}\} = \{1, -1\}$. Consider the following quotient map:

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

Note that

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

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



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

$\mathrm{Ker}(\phi) = \phi^{-1}(1) = \langle r \rangle$ ("*rotations*"), $\qquad \phi^{-1}(-1) = f\langle r \rangle$ ("*reflections*").

An example of a quotient

Define the homomorphism

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

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

$$\phi(1)=e$$

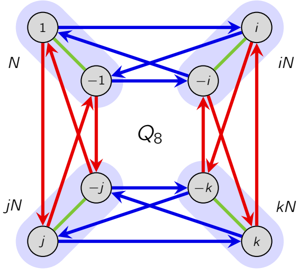
$$\phi(-1)=\phi(i^2)=\phi(i)^2=v^2=e$$

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

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

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

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



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

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

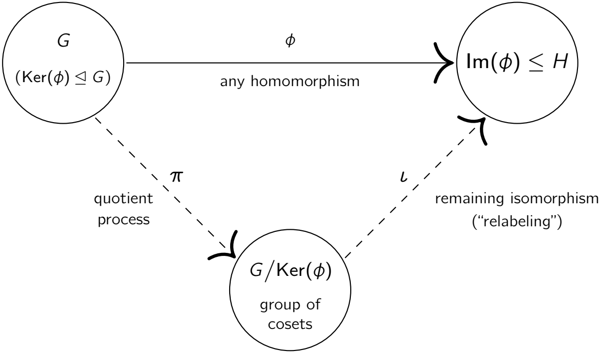
Every homomorphism image is a quotient

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

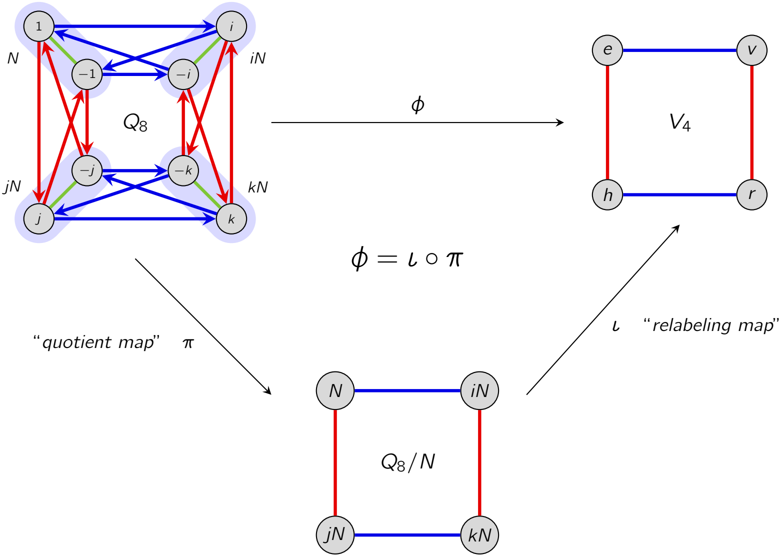
Fundamental homomorphism theorem (FHT)

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

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



Visualizing the FHT via Cayley graphs



$$\phi = \iota \circ \pi$$

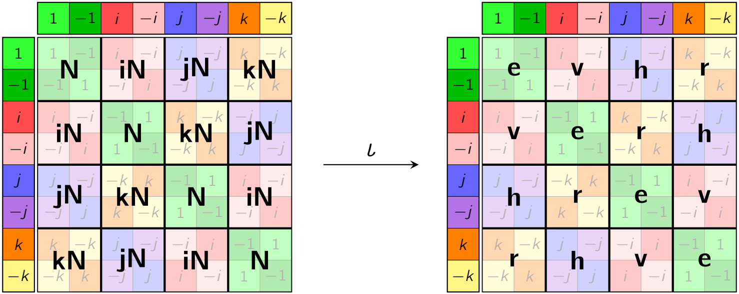
Visualizing the FHT via Cayley tables

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* $\iota\colon Q_8/N \to V_4$.



	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

	1, -1	i, $-i$	j, $-j$	k, $-k$
1, -1	**N**	**iN**	**jN**	**kN**
i, $-i$	**iN**	**N**	**kN**	**jN**
j, $-j$	**jN**	**kN**	**N**	**iN**
k, $-k$	**kN**	**jN**	**iN**	**N**

$$\xrightarrow{\iota}$$

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

	1, -1	i, $-i$	j, $-j$	k, $-k$
1, -1	**e**	**v**	**h**	**r**
i, $-i$	**v**	**e**	**r**	**h**
j, $-j$	**h**	**r**	**e**	**v**
k, $-k$	**r**	**h**	**v**	**e**

FHT preliminaries

Proposition

The kernel of any homomorphism $\phi\colon G \to H$, is a normal subgroup.

Proof

Let $N := \mathrm{Ker}(\phi)$. First, we'll show that it's a subgroup. Take any $a, b \in N$.

Identity: $\phi(e) = e$. ✓

Closure: $\phi(ab) = \phi(a)\,\phi(b) = e \cdot e = e$. ✓

Inverse: $\phi(a^{-1}) = \phi(a)^{-1} = e^{-1} = e$. ✓

Now we'll show it's normal. Take any $n \in N$. We'll show that $gng^{-1} \in N$ for all $g \in G$.

By the homomorphism property,

$$\phi(gng^{-1}) = \phi(g)\,\phi(n)\,\phi(g^{-1}) = \phi(g) \cdot e \cdot \phi(g)^{-1} = e.$$

Therefore, $gng^{-1} \in \mathrm{Ker}(\phi)$. □

Key observation

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

FHT preliminaries

Proposition

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

Proof

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

We claim that $\phi^{-1}(h) = gN$. We need to verify both $\subseteq$ and $\supseteq$.

"$\subseteq$": Take $a \in \phi^{-1}(h)$, i.e., $\phi(a) = h$. We need to show that $a \in gN$.

From basic properties of cosets, we have the equivalences

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

This last condition is true because

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

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

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

Proof of the FHT

Fundamental homomorphism theorem

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

Proof

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

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

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

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

Suppose $aN = bN$. We have

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

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

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

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

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

Proof (cont.)

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

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

Thus, ι is a homomorphism. ✓

- *Show ι is surjective (onto)*:

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

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

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 $aN = bN$.

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

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

Thus, ι is injective. ✓

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

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

Consequences of the FHT

Corollary

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

The two "extreme cases"

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

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

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

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

Consequences of the FHT

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

By the FHT,

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

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

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

Reminder

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

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

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

What does "well-defined" really mean?

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

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

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

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

Formally:

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

$$\text{if } \; a_1 N = a_2 N \; \text{ and } \; b_1 N = b_2 N, \; \text{ then } \; a_1 b_1 N = a_2 b_2 N.$$

- 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.

How to show two groups are isomorphic

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

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

Useful technique

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

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

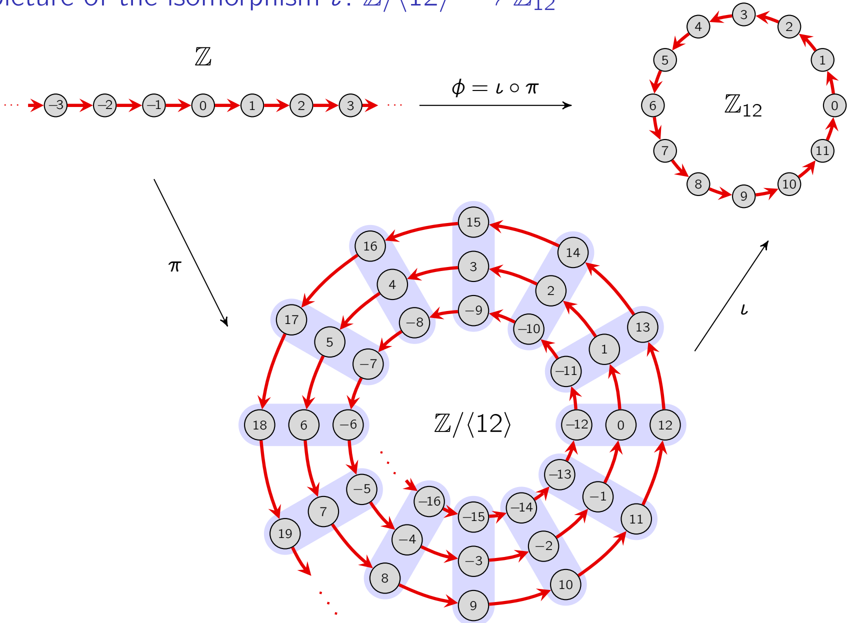
(ii) Define a map $\phi \colon G \to H$ and prove that it is a homomorphism, a surjection (onto), and that $\operatorname{Ker} \phi = N$.

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

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

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

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.

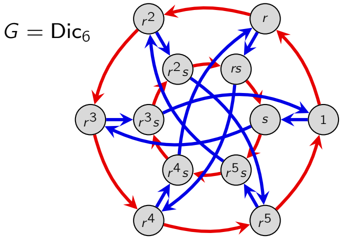
Moreover, "most properties" of $H/N \leq G/N$ are inherited from $H \leq G$.

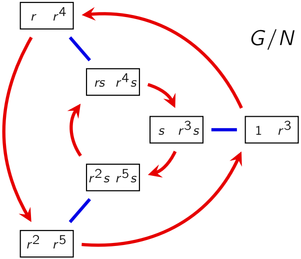
This is best understood by interpreting the subgroup lattices of G and G/N.

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

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

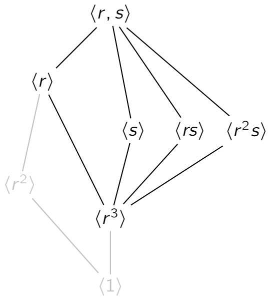
"*shoes out of the box*"

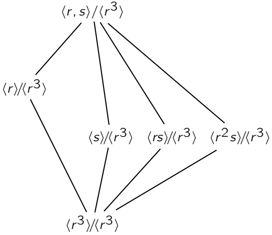
r^2N	r^2sN
rN	rsN
N	sN

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

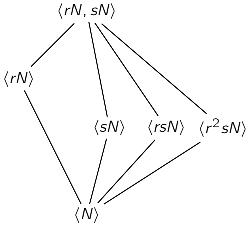
The correspondence theorem: subgroups of quotients

Here is the subgroup lattice of $G = \text{Dic}_6$, and of the quotient G/N, where $N = \langle r^3 \rangle$.





$\langle r, s\rangle/\langle r^3\rangle$
$\langle r\rangle/\langle r^3\rangle$
$\langle s\rangle/\langle r^3\rangle$
$\langle rs\rangle/\langle r^3\rangle$
$\langle r^2 s\rangle/\langle r^3\rangle$
$\langle r^3\rangle/\langle r^3\rangle$



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

$\langle s\rangle \leq G$

"*shoeboxes; lids off*"

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

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

"*shoeboxes; lids on*"

$r^2 N$	$r^2 sN$
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

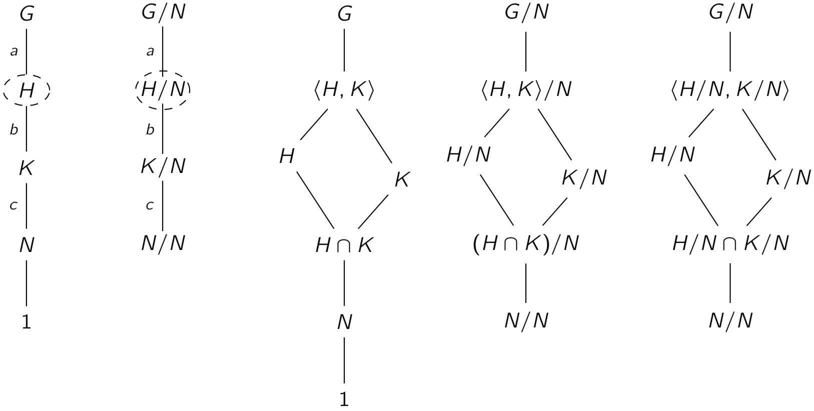
1. Subgroups of the quotient G/N are quotients of the subgroup $H \leq G$ that contain N.
2. $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$
3. $[G/N : H/N] = [G : H]$
4. $H/N \cap K/N = (H \cap K)/N$
5. $\langle H/N, K/N \rangle = \langle H, K \rangle / N$
6. H/N is conjugate to K/N in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

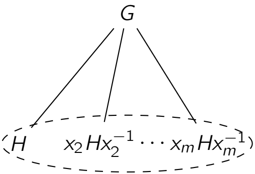
We've already interpreted the the first part.

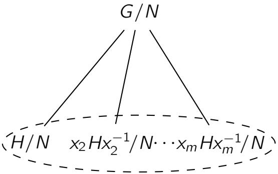
Here's what the next four parts say.



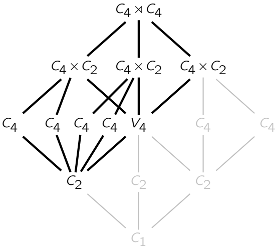
The correspondence theorem: subgroups of quotients

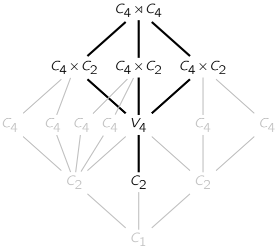
The last part says that we can characterize the conjugacy classes of G/N from those of G.

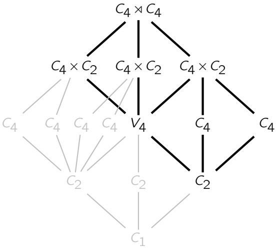




Let's apply that to find the conjugacy classes of $C_4 \rtimes C_4$ by inspection alone.







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.,

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

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 $N \leq H \leq G$.

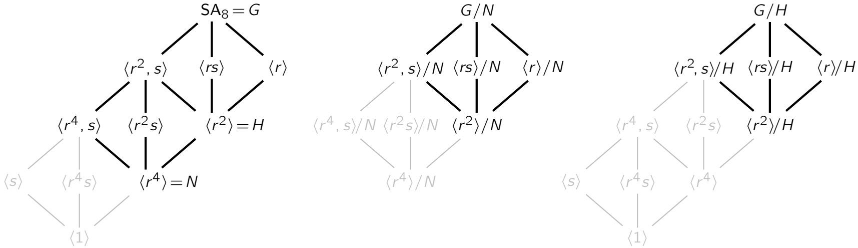
Moreover, if $H \trianglelefteq G$, then $H/N \trianglelefteq G/N$. In this case, we can ask:

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

Fraction theorem

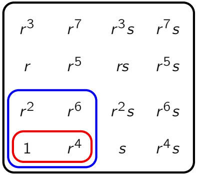
Given a chain $N \leq H \leq G$ of normal subgroups of G,

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

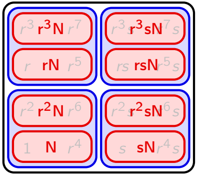


The fraction theorem: quotients of quotients

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



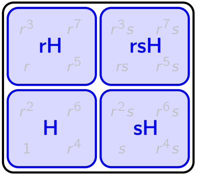
$N \leq H \leq G$



r^3 $\mathbf{r^3N}$ r^7
r^3s $\mathbf{r^3sN}$ r^7s
r $\mathbf{rN}$ r^5
rs $\mathbf{rsN}$ r^5s
r^2 $\mathbf{r^2N}$ r^6
r^2s $\mathbf{r^2sN}$ r^6s
1 $\mathbf{N}$ r^4
s $\mathbf{sN}$ r^4s

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

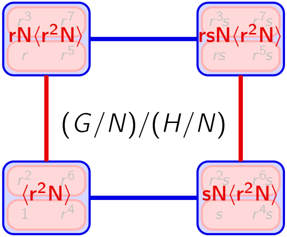
$H/N = \langle r^2N\rangle = \{N, r^2N\} \cong C_2$



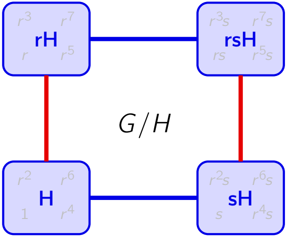
r^3 r^7 $\mathbf{rH}$ r r^5
r^3s r^7s $\mathbf{rsH}$ rs r^5s
r^2 r^6 $\mathbf{H}$ 1 r^4
r^2s r^6s $\mathbf{sH}$ s r^4s

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

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



$\mathbf{rN\langle r^2N\rangle}$
$\mathbf{rsN\langle r^2N\rangle}$
$(G/N)/(H/N)$
$\mathbf{\langle r^2N\rangle}$
$\mathbf{sN\langle r^2N\rangle}$
r^3 r^7 r r^5
r^3s r^7s rs r^5s
r^2 r^6 1 r^4
r^2s r^6s s r^4s



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 $g_1 N = g_2 N$. Then $g_1 = g_2 n$ for some $n \in N$. But $n \in H$ because $N \leq H$. Thus, $g_1 H = g_2 H$, i.e., $\phi(g_1 N) = \phi(g_2 N)$. ✓

- *ϕ is clearly onto and a homomorphism*. ✓

- *Apply the FHT*:

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

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.

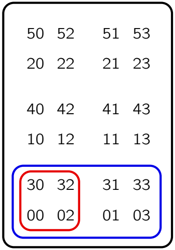
Consider the subgroups $N = \langle 30, 02\rangle \cong V_4$ and $H = \langle 30, 01\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

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

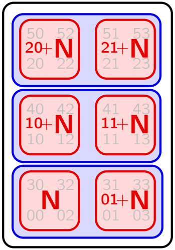
$$G/N = \big\{N,\ 01{+}N,\ 10{+}N,\ 11{+}N,\ 20{+}N,\ 21{+}N\big\}, \qquad H/N = \{N,\ 01{+}N\}$$

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

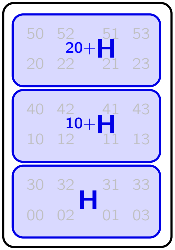
$$(G/N)/(H/N) = \Big\{\{N,\ 01{+}N\},\ \{10{+}N,\ 11{+}N\},\ \{20{+}N,\ 21{+}N\}\Big\}.$$



$N \leq H \leq G$



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

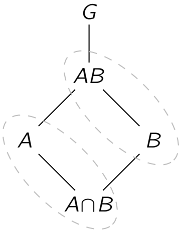
Diamond theorem

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

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

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

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

Corollary

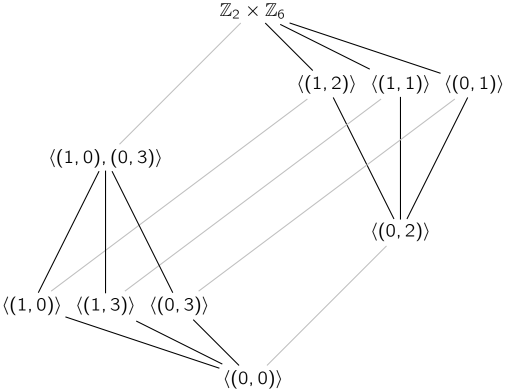
Let $A, B \leq G$, with one of them normalizing the other. Then $|AB| = \dfrac{|A| \cdot |B|}{|A \cap B|}$.

The diamond theorem: quotients of products by factors

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

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

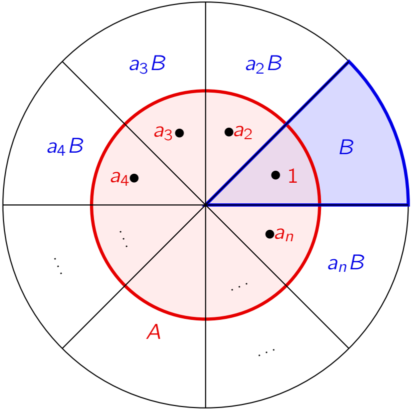
Let's interpret the diamond theorem $AB/B \cong A/A \cap B$ in terms of the subgroup lattice.



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

The diamond theorem 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

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

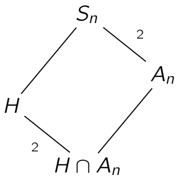
$A/(A \cap B) = \{\text{small pizza slices}\}$

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,

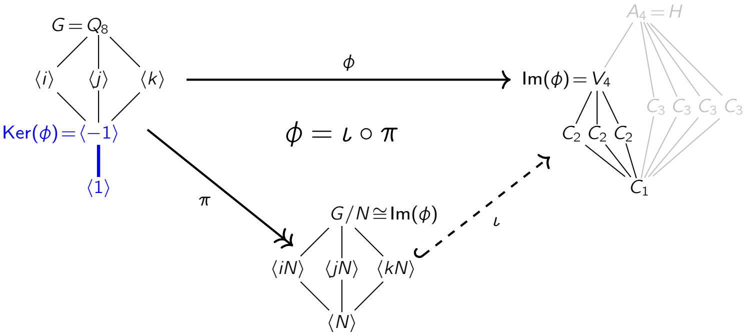
$$H/(H \cap A_n) = HA_n/A_n = S_n/A_n \cong C_2. \qquad \square$$

A generalization of the FHT

Theorem (exercise)

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

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


$G = Q_8$

$\langle i \rangle$ $\langle j \rangle$ $\langle k \rangle$

$\mathrm{Ker}(\phi) = \langle -1 \rangle$

$\langle 1 \rangle$

ϕ

$\mathrm{Im}(\phi) = V_4$

$A_4 = H$

C_2 C_2 C_2

C_3 C_3 C_3 C_3

C_1

$$\phi = \iota \circ \pi$$

π

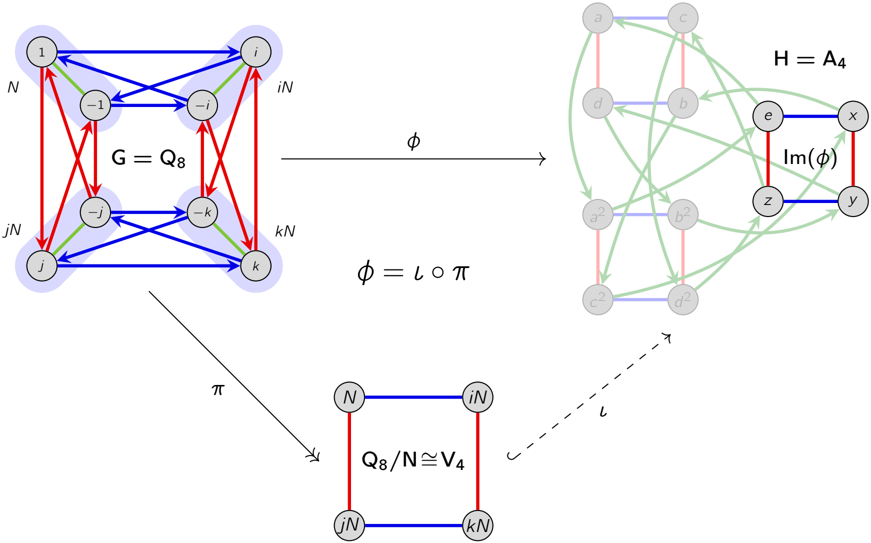
ι

$G/N \cong \mathrm{Im}(\phi)$

$\langle iN \rangle$ $\langle jN \rangle$ $\langle kN \rangle$

$\langle N \rangle$

A generalization of the FHT

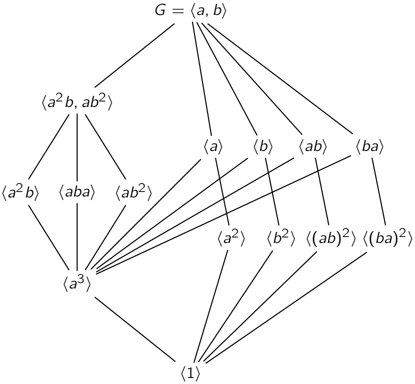


The “subgroup” and “quotient” operations commute

Key idea

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

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



$G = \langle a, b\rangle$

$\langle a^2b, ab^2\rangle$ $\langle a\rangle$ $\langle b\rangle$ $\langle ab\rangle$ $\langle ba\rangle$

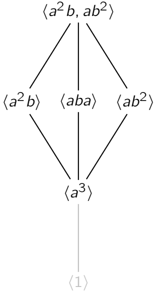
$\langle a^2b\rangle$ $\langle aba\rangle$ $\langle ab^2\rangle$

$\langle a^2\rangle$ $\langle b^2\rangle$ $\langle (ab)^2\rangle$ $\langle (ba)^2\rangle$

$\langle a^3\rangle$

$\langle 1\rangle$

subgroup $\mathbf{H \cong Q_8}$



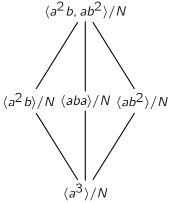
$\langle a^2b, ab^2\rangle$

$\langle a^2b\rangle$ $\langle aba\rangle$ $\langle ab^2\rangle$

$\langle a^3\rangle$

$\langle 1\rangle$

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



$\langle a^2b, ab^2\rangle/N$

$\langle a^2b\rangle/N$ $\langle aba\rangle/N$ $\langle ab^2\rangle/N$

$\langle a^3\rangle/N$

“*quotient of the subgroup*”

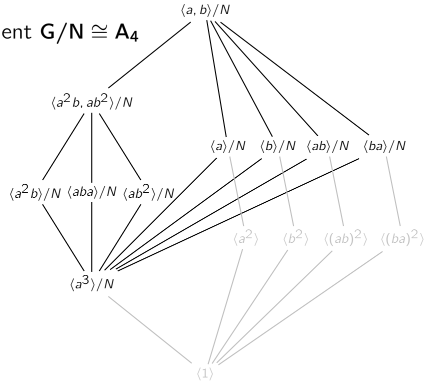
The “subgroup” and “quotient” operations commute

Key idea

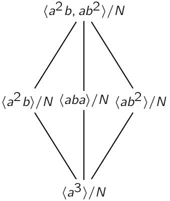
The quotient of a subgroup is just the subgroup of the quotient.

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

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



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



“*subgroup of the quotient*”

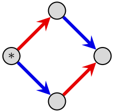
Commutators

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

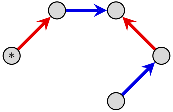
Now, suppose G is nonabelian. We'd like to divide G by its "non-abelian parts," making them zero and leaving only "abelian parts" in the resulting quotient.

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

$ab = ba$



$ab \neq ba$



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

Definition

The commutator subgroup G' of G is

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

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

The abelianization of a group

Definition

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

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

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

Universal property of commutator subgroups

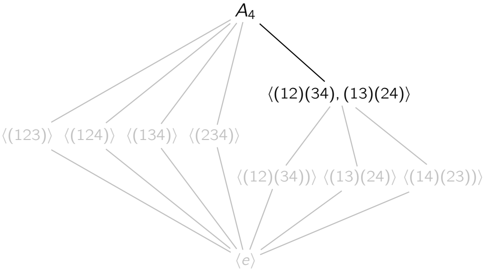
Suppose $f\colon G \to A$ is a homomorphism to an abelian group A. Then there is a unique homomorphism $h\colon G/G' \to A$ such that $f = h\pi$:

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & A \\
& G/G' \arrow[ur, dashed, "h"'] &
\end{tikzcd}$$

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

Some examples of abelianizations

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



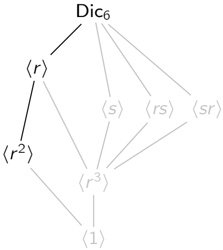
A_4

$\langle(12)(34),(13)(24)\rangle$

$\langle(123)\rangle$ $\langle(124)\rangle$ $\langle(134)\rangle$ $\langle(234)\rangle$

$\langle(12)(34)\rangle$ $\langle(13)(24)\rangle$ $\langle(14)(23)\rangle$

$\langle e\rangle$



Dic_6

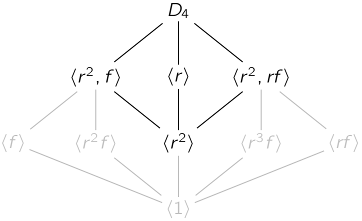
$\langle r\rangle$

$\langle s\rangle$ $\langle rs\rangle$ $\langle sr\rangle$

$\langle r^2\rangle$

$\langle r^3\rangle$

$\langle 1\rangle$

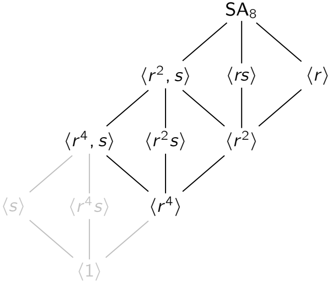


D_4

$\langle r^2,f\rangle$ $\langle r\rangle$ $\langle r^2,rf\rangle$

$\langle f\rangle$ $\langle r^2f\rangle$ $\langle r^2\rangle$ $\langle r^3f\rangle$ $\langle rf\rangle$

$\langle 1\rangle$



SA_8

$\langle r^2,s\rangle$ $\langle rs\rangle$ $\langle r\rangle$

$\langle r^4,s\rangle$ $\langle r^2s\rangle$ $\langle r^2\rangle$

$\langle s\rangle$ $\langle r^4s\rangle$ $\langle r^4\rangle$

$\langle 1\rangle$

Automorphisms

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

For a general group G, an automorphism is a isomorphism $\phi\colon G \to G$.

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

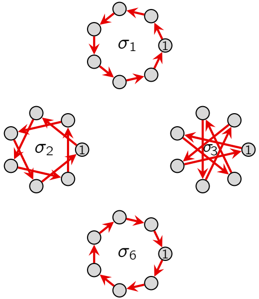
$$\sigma_a \colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_n\,, \qquad \sigma_a(1) = a\,.$$

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

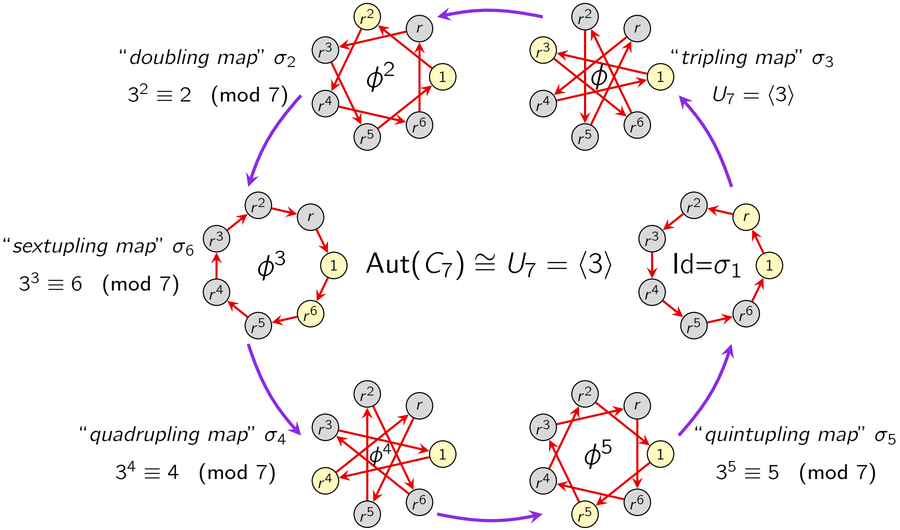
	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

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

	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



“*doubling map*” σ_2

$3^2 \equiv 2 \pmod{7}$

“*tripling map*” σ_3

$U_7 = \langle 3 \rangle$

“*sextupling map*” σ_6

$3^3 \equiv 6 \pmod{7}$

$\mathrm{Aut}(C_7) \cong U_7 = \langle 3 \rangle$

$\mathrm{Id}=\sigma_1$

“*quadrupling map*” σ_4

$3^4 \equiv 4 \pmod{7}$

“*quintupling map*” σ_5

$3^5 \equiv 5 \pmod{7}$

Automorphisms of noncyclic groups

An automorphism is determined by where it sends the generators.

Examples

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

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

   Every permutation of $\{h, v, r\}$ is an automorphism, and 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 automorphisms preserve order, if $\phi \in \mathrm{Aut}(D_3)$, then

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

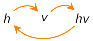
   Thus, $|\,\mathrm{Aut}(D_3)| \leq 6$. Both of the following define automorphisms of D_3:

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

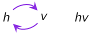
It is elementary to check that $\alpha\beta = \beta\alpha^2$, and so $\mathrm{Aut}(D_3) \cong D_3 \cong S_3$.

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

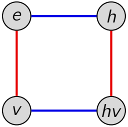
The following permutations are both automorphisms:

α : 

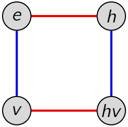
and

β : 

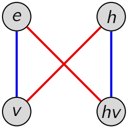
$$\begin{aligned} h &\xmapsto{id} h \\ v &\longmapsto v \\ hv &\longmapsto hv \end{aligned}$$



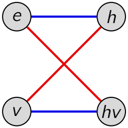
$$\begin{aligned} h &\xmapsto{\beta} v \\ v &\longmapsto h \\ hv &\longmapsto hv \end{aligned}$$



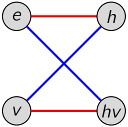
$$\begin{aligned} h &\xmapsto{\alpha} v \\ v &\longmapsto hv \\ hv &\longmapsto h \end{aligned}$$



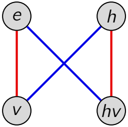
$$\begin{aligned} h &\xmapsto{\alpha\beta} h \\ v &\longmapsto hv \\ hv &\longmapsto v \end{aligned}$$



$$\begin{aligned} h &\xmapsto{\alpha^2} hv \\ v &\longmapsto h \\ hv &\longmapsto v \end{aligned}$$



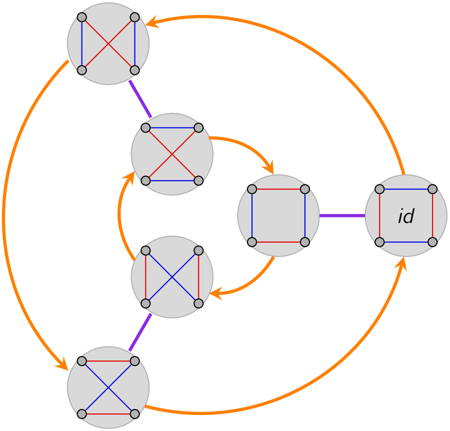
$$\begin{aligned} h &\xmapsto{\alpha^2\beta} hv \\ v &\longmapsto v \\ hv &\longmapsto h \end{aligned}$$

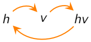


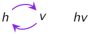
Automorphisms of $V_4 = \langle h, v \rangle$

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

	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



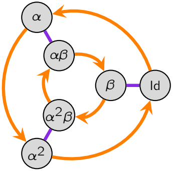
Recall that α and β can be thought of as the permutations 

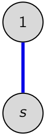
and 

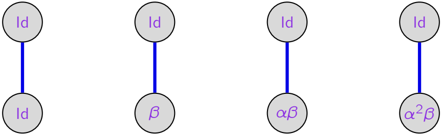
and so $\textbf{Aut}(G) \hookrightarrow \textbf{Perm}(G) \cong S_n$ always holds.

The construction of $V_4 \rtimes C_2$

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

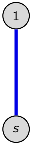




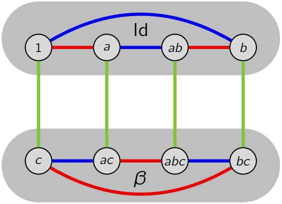


$s \xrightarrow{\theta} \mathrm{Id}$ $\quad s \xrightarrow{\theta_0} \beta$ $\quad s \xrightarrow{\theta_1} \alpha\beta$ $\quad s \xrightarrow{\theta_2} \alpha^2\beta$

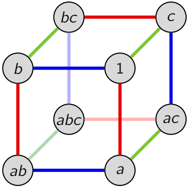
Let's now carry out our "inflation method" to construct $V_4 \rtimes C_2$.



Start with a copy of $B = C_2$



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

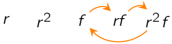


rearrange the Cayley graph

What familiar group is $V_4 \rtimes C_2$?

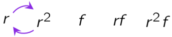
Automorphisms of D_3

α :



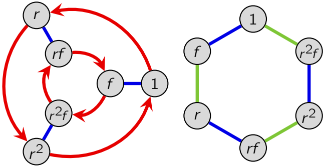
and

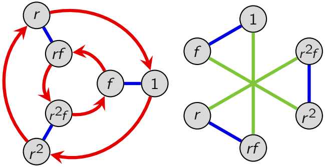
β :



$r \xrightarrow{id} r$

$f \longrightarrow f$



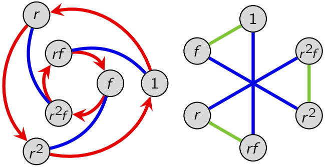


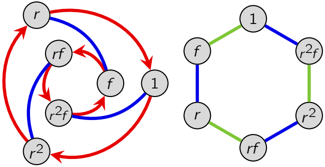
$r \xrightarrow{\beta} r^2$

$f \longrightarrow f$

$r \xrightarrow{\alpha} r$

$f \longrightarrow rf$



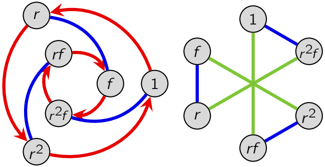


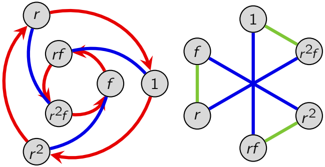
$r \xrightarrow{\alpha\beta} r^2$

$f \longrightarrow r^2 f$

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

$f \longrightarrow r^2 f$





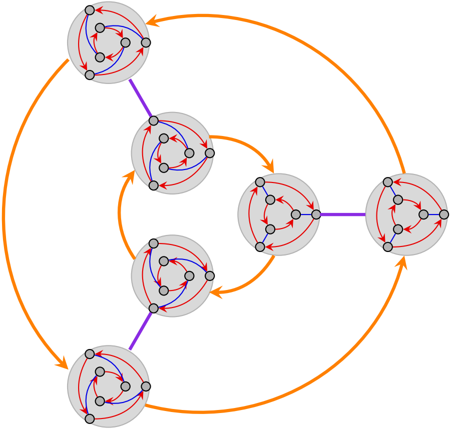
$r \xrightarrow{\alpha^2\beta} r^2$

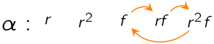
$f \longrightarrow rf$

Automorphisms of D_3

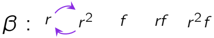
Here is the Cayley table and Cayley graph of $\mathbf{Aut}(D_3) = \langle \alpha, \beta \rangle$.

	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

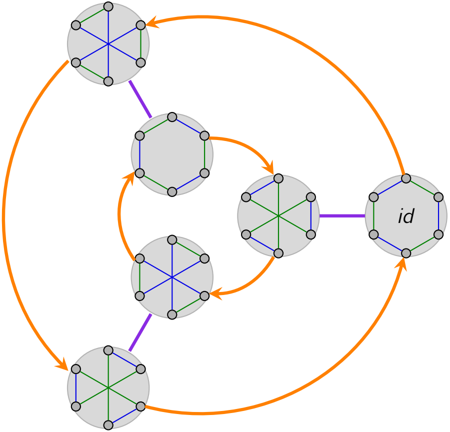
and


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



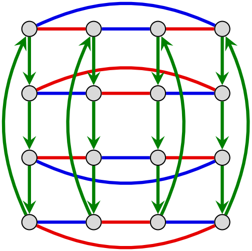
$$\begin{tikzcd}\alpha : & r & r^2 & f \arrow[r, bend left] & rf \arrow[r, bend left] & r^2 f \arrow[ll, bend left]\end{tikzcd}$$

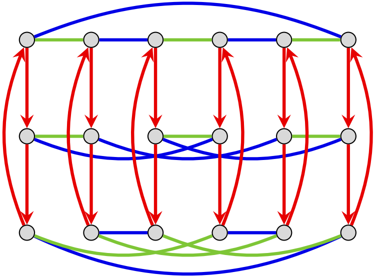
and

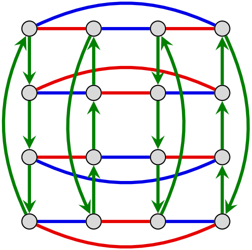
$$\begin{tikzcd}\beta : & r \arrow[r, bend left] & r^2 \arrow[l, bend left] & f & rf & r^2 f\end{tikzcd}$$

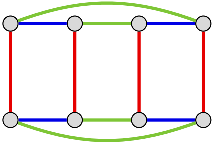
A few more examples of semidirect products

What groups are these?





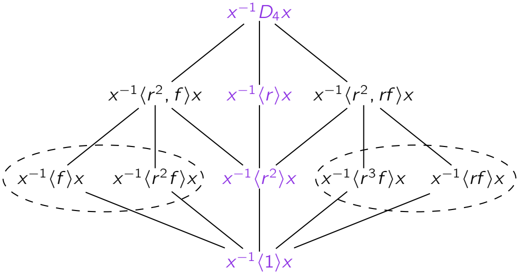


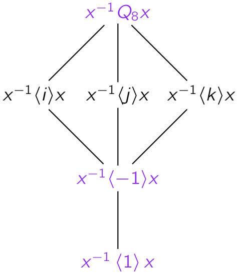


Inner and outer automorphisms

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

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


$x^{-1}D_4x$
$x^{-1}\langle r^2, f\rangle x$
$x^{-1}\langle r\rangle x$
$x^{-1}\langle r^2, rf\rangle x$
$x^{-1}\langle f\rangle x$
$x^{-1}\langle r^2 f\rangle x$
$x^{-1}\langle r^2\rangle x$
$x^{-1}\langle r^3 f\rangle x$
$x^{-1}\langle rf\rangle x$
$x^{-1}\langle 1\rangle x$


$x^{-1}Q_8x$
$x^{-1}\langle i\rangle x$
$x^{-1}\langle j\rangle x$
$x^{-1}\langle k\rangle x$
$x^{-1}\langle -1\rangle x$
$x^{-1}\langle 1\rangle x$

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

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

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

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

This is called an outer automorphism.

The inner automorphism group

Definition

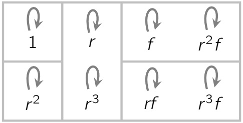
An inner automorphism of G is an automorphism $\varphi_x \in \mathrm{Aut}(G)$ defined by

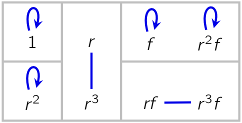
$$\varphi_x(g) := x^{-1}gx, \qquad \text{for some } x \in G.$$

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

There are four inner automorphisms of D_4:

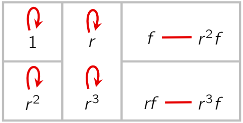
$\mathrm{Id} = \varphi_1 = \varphi_{r^2}$

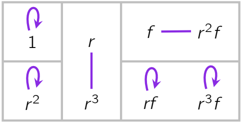




$\varphi_f = \varphi_{r^2f}$

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





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

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)

Inn(G) is a normal subgroup of 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 Inn(G):

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

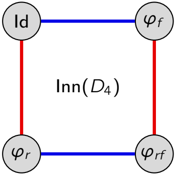
That is, if x and y are in the same coset of $Z(G)$, then $\varphi_x = \varphi_y$. (And conversely.)

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

cl(1)	1	r	f	rf
cl(r^2)	r^2	r^3	r^2f	r^3f
		cl(r)	cl(f)	cl(rf)

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,

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

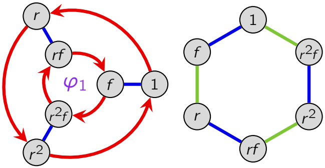
i.e., every automorphism is inner.

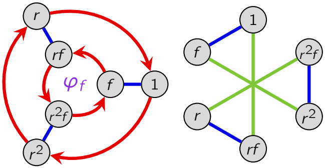
Inner automorphisms of D_3

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

$r \xrightarrow{Id} r$

$f \longrightarrow f$



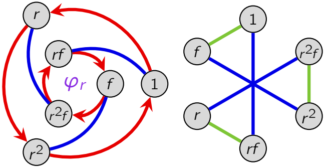


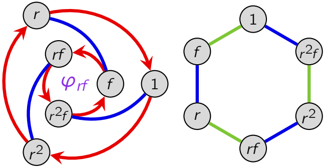
$r \xrightarrow{\beta} r^2$

$f \longrightarrow f$

$r \xrightarrow{\alpha} r$

$f \longrightarrow rf$



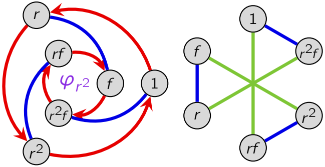


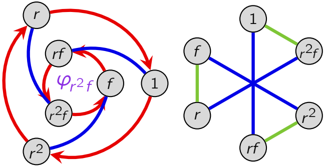
$r \xrightarrow{\alpha\beta} r^2$

$f \longrightarrow r^2f$

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

$f \longrightarrow r^2f$





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

$f \longrightarrow rf$

Automorphisms of D_4

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

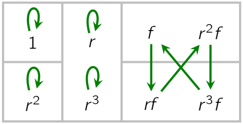
$$\phi(r) = \underbrace{r \text{ or } r^3}_{\text{2 choices}}, \qquad \phi(f) = \underbrace{f,\ rf,\ r^2f,\ r^3f, \text{ or } r^2}_{\text{5 choices}}.$$

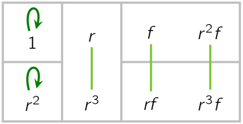
Thus $|\operatorname{Aut}(D_4)| \leq 10$. But $\operatorname{Inn}(D_4) \leq \operatorname{Aut}(D_4)$, forces $|\operatorname{Aut}(D_4)| = 4$ or 8. Moreover,

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

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

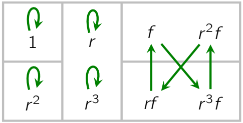
ω

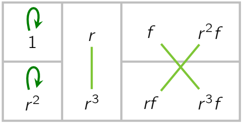




$\varphi_f\omega$

$\varphi_r\omega$





$\varphi_{rf}\omega$

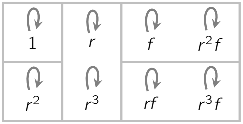
$$\operatorname{Aut}(D_4) = \left\{ Id,\ \varphi_r,\ \varphi_f,\ \varphi_{rf},\ \omega,\ \varphi_r\omega,\ \varphi_f\omega,\ \varphi_{rf}\omega \right\} = \operatorname{Inn}(D_4) \cup \operatorname{Inn}(D_4)\omega \cong D_4.$$

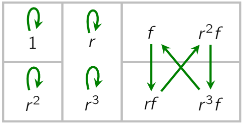
The full automorphism group of D_4

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

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

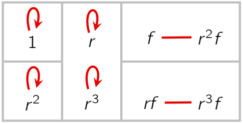
$Id = \varphi_1$

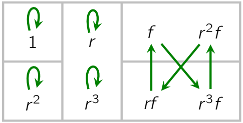




ω

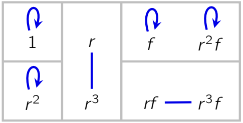
φ_r

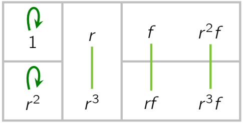




$\varphi_r\omega$

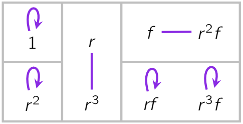
φ_f

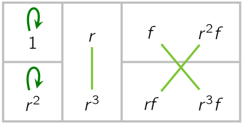




$\varphi_f\omega$

φ_{rf}





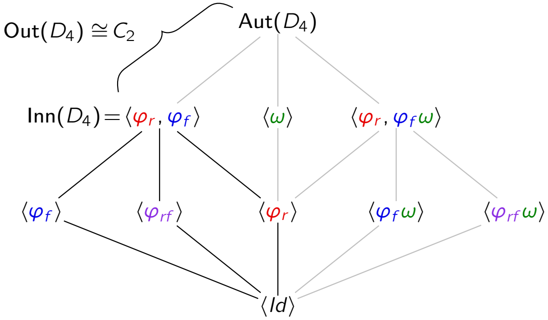
$\varphi_{rf}\omega$

The outer automorphism group

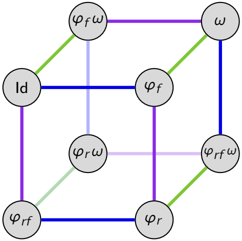
Definition

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

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



$\mathrm{Out}(D_4) \cong C_2$
$\mathrm{Aut}(D_4)$
$\mathrm{Inn}(D_4) = \langle \varphi_r, \varphi_f \rangle$
$\langle \omega \rangle$
$\langle \varphi_r, \varphi_f\omega \rangle$
$\langle \varphi_f \rangle$
$\langle \varphi_{rf} \rangle$
$\langle \varphi_r \rangle$
$\langle \varphi_f\omega \rangle$
$\langle \varphi_{rf}\omega \rangle$
$\langle Id \rangle$



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

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

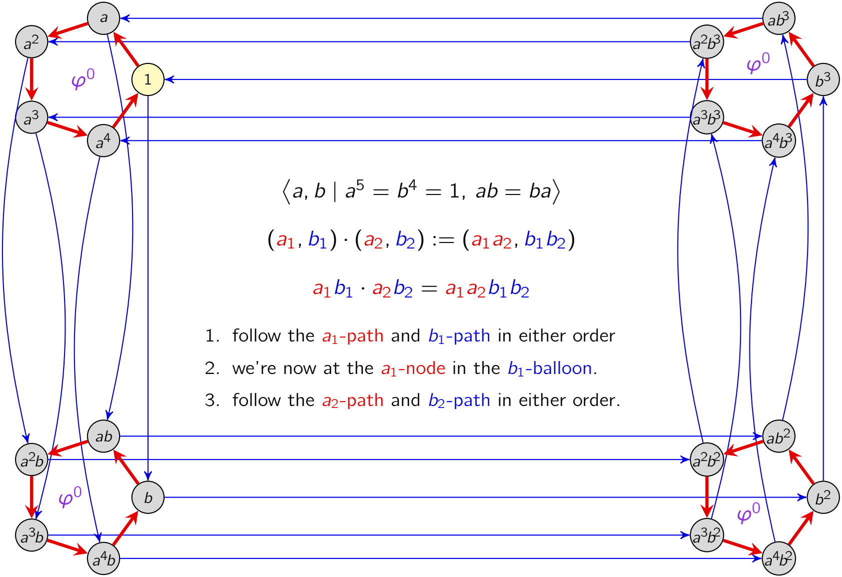
$$\theta \colon B \longrightarrow \mathrm{Aut}(A),$$

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 $C_5 \times C_4$



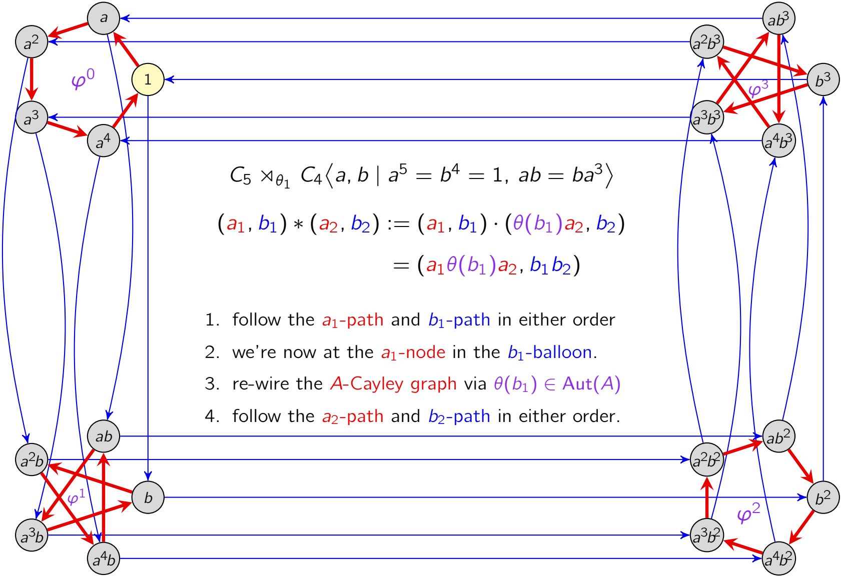
$$\langle a, b \mid a^5 = b^4 = 1,\ ab = ba \rangle$$

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

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

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.

Revisiting semidirect products

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:

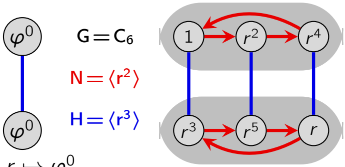
- In $A \times B$, both factors are normal (technically, $A \times \{1\}$ and $\{1\} \times B$).
- In $A \rtimes B$, the group on the "open" side of $\rtimes$ is normal.

Internal products

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

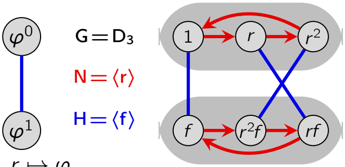
Now, we'll explore when a group $G = NH$ is isomorphic to a direct or semidirect product.

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



$\theta_0 \colon r \mapsto \varphi^0$

$C_6 = NH \cong N \times H$



$\theta_1 \colon r \mapsto \varphi$

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

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

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

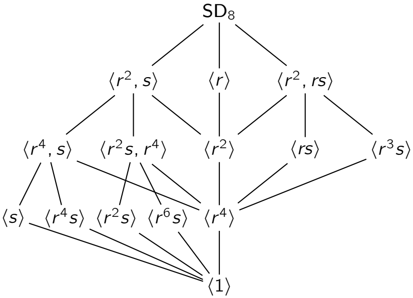
(iii) $G = NH$,

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



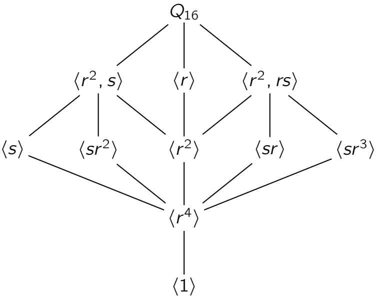
SD_8

$\langle r^2, s\rangle$ $\langle r\rangle$ $\langle r^2, rs\rangle$

$\langle r^4, s\rangle$ $\langle r^2 s, r^4\rangle$ $\langle r^2\rangle$ $\langle rs\rangle$ $\langle r^3 s\rangle$

$\langle s\rangle$ $\langle r^4 s\rangle$ $\langle r^2 s\rangle$ $\langle r^6 s\rangle$ $\langle r^4\rangle$

$\langle 1\rangle$



Q_{16}

$\langle r^2, s\rangle$ $\langle r\rangle$ $\langle r^2, rs\rangle$

$\langle s\rangle$ $\langle sr^2\rangle$ $\langle r^2\rangle$ $\langle sr\rangle$ $\langle sr^3\rangle$

$\langle r^4\rangle$

$\langle 1\rangle$

Observations

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

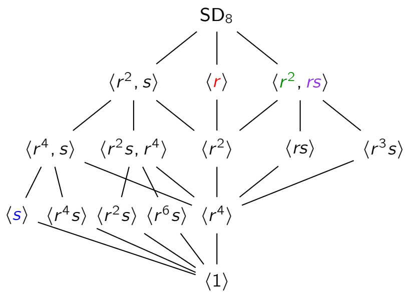
$$N = \langle r\rangle \cong C_8, \quad H = \langle s\rangle \cong C_2, \qquad \mathrm{SD}_8 = NH \cong C_8 \rtimes_{\theta_3} C_2.$$

  or alternatively,

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

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

Semidihedral groups as semidirect products



SD_8

$\langle r^2, s\rangle$ $\langle r\rangle$ $\langle r^2, rs\rangle$

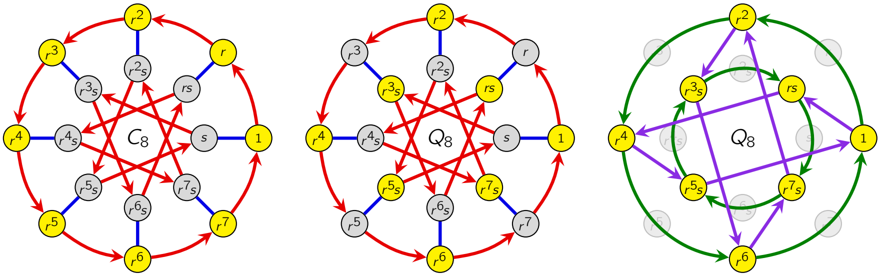
$\langle r^4, s\rangle$ $\langle r^2 s, r^4\rangle$ $\langle r^2\rangle$ $\langle rs\rangle$ $\langle r^3 s\rangle$

$\langle s\rangle$ $\langle r^4 s\rangle$ $\langle r^2 s\rangle$ $\langle r^6 s\rangle$ $\langle r^4\rangle$

$\langle 1\rangle$

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

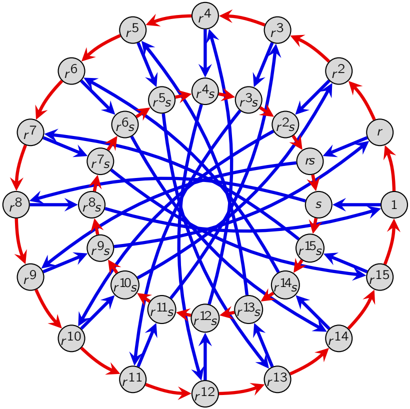
$$\mathrm{SD}_8 \cong \langle r^2, rs\rangle \rtimes \langle s\rangle \cong Q_8 \rtimes C_2$$

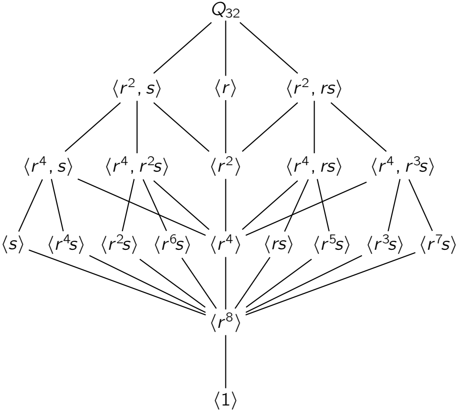


Generalized quaternion groups

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.





Q_{32}

$\langle r^2, s\rangle$ $\langle r\rangle$ $\langle r^2, rs\rangle$

$\langle r^4, s\rangle$ $\langle r^4, r^2s\rangle$ $\langle r^2\rangle$ $\langle r^4, rs\rangle$ $\langle r^4, r^3s\rangle$

$\langle s\rangle$ $\langle r^4s\rangle$ $\langle r^2s\rangle$ $\langle r^6s\rangle$ $\langle r^4\rangle$ $\langle rs\rangle$ $\langle r^5s\rangle$ $\langle r^3s\rangle$ $\langle r^7s\rangle$

$\langle r^8\rangle$

$\langle 1\rangle$

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:

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

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

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

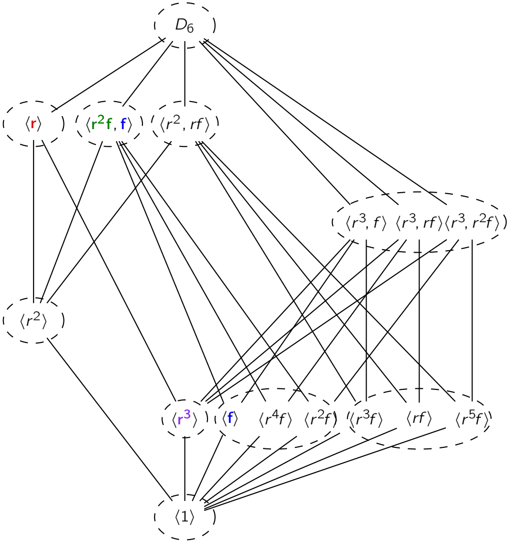
for some $\theta(h_1) \in \mathbf{Aut}(N)$.

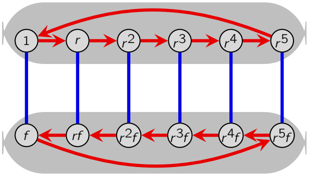
To see why $\theta(h_1)$ is the inner automorphism φ_{h_1}, note that

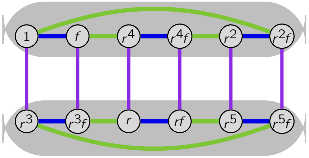
$$n_1\varphi_{h_1^{-1}}(n_2)h_1h_2 = n_1(h_1^{-1}n_2h_1)h_1h_2 = (n_1h_1) * (n_2h_2). \qquad \square$$

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 $G \cong H \circ K$.

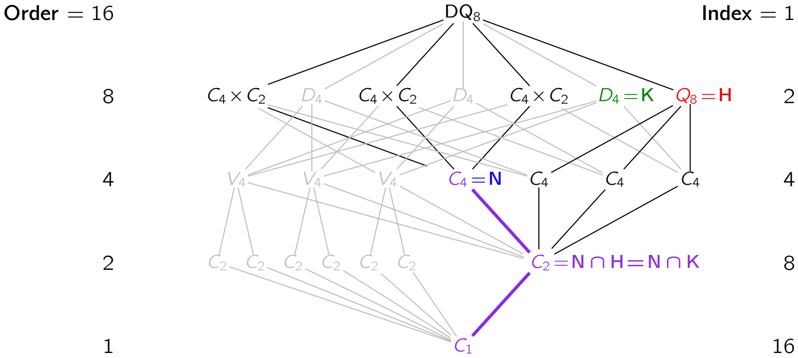
We can also define an *external central product* of A and B, but we won't do that here.

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


Order = 16
8
4
2
1
DQ_8
$C_4 \times C_2$
D_4
$C_4 \times C_2$
D_4
$C_4 \times C_2$
$D_4 = \mathbf{K}$
$Q_8 = \mathbf{H}$
V_4
V_4
V_4
$C_4 = \mathbf{N}$
C_4
C_4
C_4
C_2
C_2
C_2
C_2
C_2
C_2
$C_2 = \mathbf{N} \cap \mathbf{H} = \mathbf{N} \cap \mathbf{K}$
C_1
Index = 1
2
4
8
16