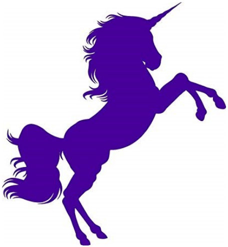
A visual tour of the beauty of group theory

Matthew Macauley

School of Mathematical and Statistical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Talk Math With Your Friends
October 14, 2021



What is a group? ("wrong" answers only)

Definition

A group is a set G satisfying the following properties:

1. There is an associative binary operation $*$ on G.
2. There is an identity element $e \in G$. That is, $e * g = g = g * e$ for all $g \in G$.
3. Every element $g \in G$ has an inverse, g^{-1}, satisfying $g * g^{-1} = e = g^{-1} * g$.

Every group has a presentation of generators and relations. For example:

- The **quaternion group**:

$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = -1 \rangle = \{\pm 1, \pm i, \pm j, \pm k\}$$

- The **dihedral group**:

$$D_n = \langle r, f \mid r^n = f^2 = rfr = f \rangle.$$

Groups you didn't know existed...

(and other you couldn't possibly live without!)

Some groups of order 16

- The **abelian group**:

$$C_8 \times C_2 = \langle r, s \mid r^8 = s^2 = 1,\ rs = sr \rangle.$$

- The **dihedral group**:

$$D_8 = \langle r, s \mid r^8 = s^2 = 1,\ sr = r^{-1}s \rangle.$$

- The **dicyclic group**:

$$\mathrm{Dic}_8 = \langle r, s \mid r^8 = s^4 = 1,\ r^4 = s^2 \rangle.$$

- The **semidihedral group**:

$$\mathrm{SD}_8 = \langle r, s \mid r^8 = s^2 = 1,\ srs = r^3 \rangle.$$

- The **semiabelian group**:

$$\mathrm{SA}_8 = \langle r, s \mid r^8 = s^2 = 1,\ srs = r^5 \rangle.$$

- The **Pauli group**

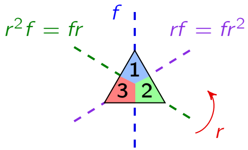
$$\mathrm{Pauli}_1 = \langle a, b, c \mid a^4 = c^2 = 1,\ a^2 = b^2,\ ac = ca,\ a^2b = cbc \rangle.$$

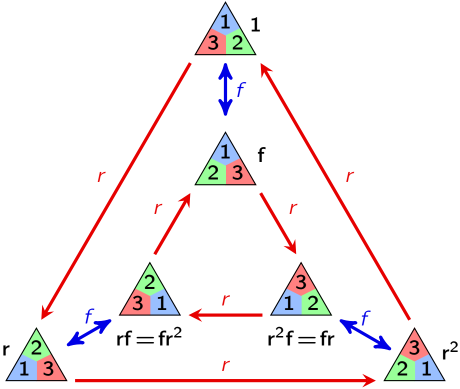
A Cayley diagram is a way to visualize a presentation

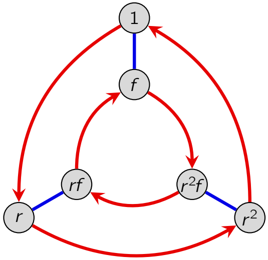
Here is a Cayley diagram for the **dihedral group**

$$D_3 = \langle r, f \mid r^3 = f^2 = 1, rf = fr^2 \rangle .$$

We'll always multiply left-to-right!







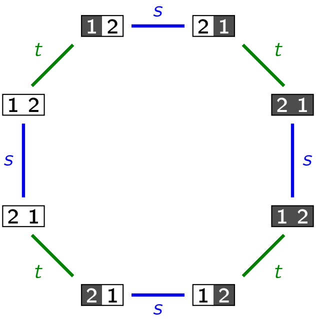
A group of size 8

Call the following rectangle configuration our *home state*: 

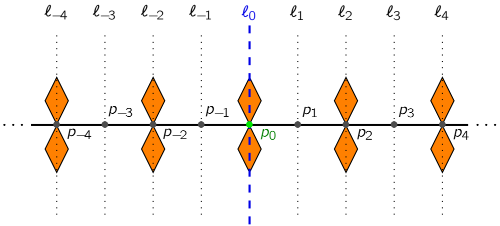
Suppose we are allowed the following operations, or "actions":

- s: swap the two squares
- t: toggle the color of the first square.

Here is a Cayley diagram:



Frieze groups



Definition

Let v be the unique vertical reflection. Other symmetries come in infinite families. Define

- t: minimal translation to the right
- $g = tv = vt$: min'l glide-reflection right
- h_i: horizontal reflection across ℓ_i
- r_i: 180° rotation around p_i

The symmetry group of the frieze above consists of the following symmetries:

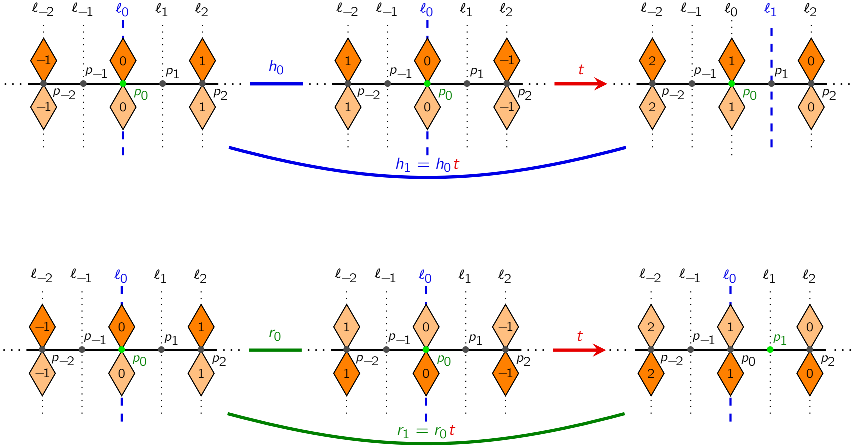
$$G_1 := \{v\} \cup \{h_i \mid i \in \mathbb{Z}\} \cup \{r_i \mid i \in \mathbb{Z}\} \cup \{t^i \mid i \in \mathbb{Z}\} \cup \{g^i \mid i \in \mathbb{Z}\}.$$

Letting $h := h_0$ and $r := r_0$, this frieze group is generated by

$$G_1 := \langle t, h, v \rangle = \langle t, h, r \rangle = \langle t, v, r \rangle = \langle g, h, v \rangle = \cdots$$

Frieze groups

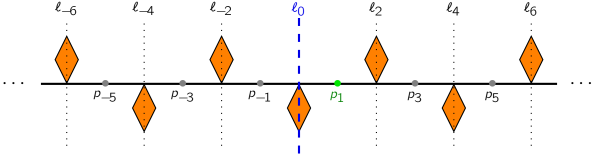
Let's look at how the various reflections and rotations are related:



Similarly, it follows that $h_i t = h_{i+1}$ and $r_i t = r_{i+1}$ for any $i \in \mathbb{Z}$.

A "smaller" frieze group

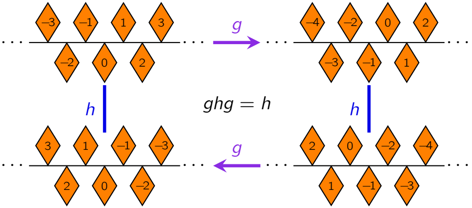
Let's eliminate the vertical symmetry from the previous frieze group.

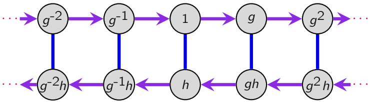


We lose half of the horizontal reflections and rotations in the process. The frieze group is

$$G_2 := \{g^i \mid i \in \mathbb{Z}\} \cup \{h^{2j} \mid j \in \mathbb{Z}\} \cup \{r^{2k+1} \mid k \in \mathbb{Z}\} = \langle g, h \rangle = \langle vt, h \rangle = \langle g, r_1 \rangle = \langle vt, rt \rangle.$$

To find a presentation, we just have to see how g and h are related:

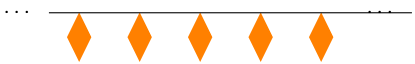


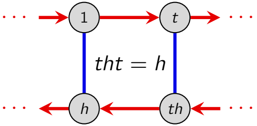


$$G_2 = \langle g, h \mid h^2 = 1,\ ghg = h \rangle$$

Other friezes generated by two symmetries

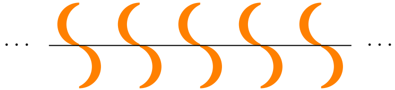
Frieze 3: eliminate the vertical flip and all rotations

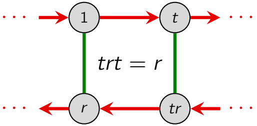




$$G_3 = \{t^i \mid i \in \mathbb{Z}\} \cup \{h^j \mid \mathbb{Z}\} = \langle t, h \mid h^2 = 1,\ tht = r \rangle$$

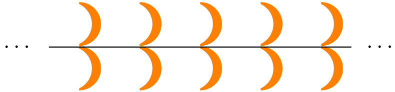
Frieze 4: eliminate the vertical flip and all horizontal flips

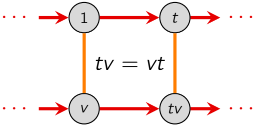




$$G_4 = \{t^i \mid i \in \mathbb{Z}\} \cup \{r^j \mid \mathbb{Z}\} = \langle t, r \mid r^2 = 1,\ trt = r \rangle$$

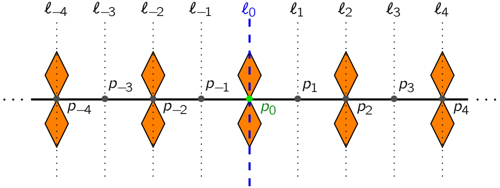
Frieze 5: eliminate all horizontal flips and rotations





$$G_5 = \{t^i \mid i \in \mathbb{Z}\} \cup \{g^j \mid \mathbb{Z}\} = \langle t, v \mid v^2 = 1,\ tv = vt \rangle$$

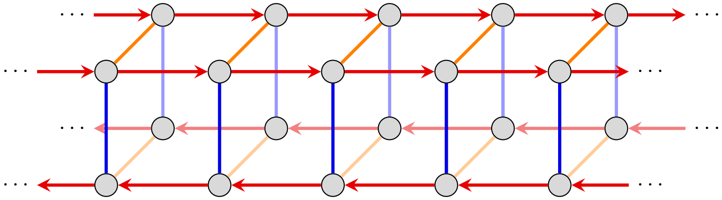
A Cayley diagram of our first frieze group



A presentation for this frieze group is

$$G_1 = \langle t, h, v \mid h^2 = v^2 = 1,\ hv = vh,\ tv = vt,\ tht = h \rangle.$$

We can make a Cayley diagram by piecing together the "tiles" on the previous slide:

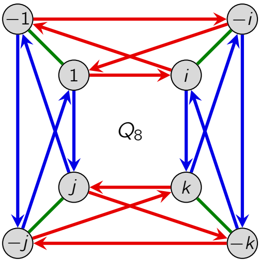


The quaternion group

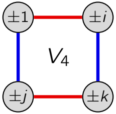
Recall that the **quaternion** group is

$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle = \langle i, j \mid i^4 = j^4 = 1,\ iji = j \rangle,$$

Here is a Cayley diagram and Cayley table:



	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	$\pm i$	$\pm j$	$\pm k$
± 1	± 1	$\pm i$	$\pm j$	$\pm k$
$\pm i$	$\pm i$	± 1	$\pm k$	$\pm j$
$\pm j$	$\pm j$	$\pm k$	± 1	$\pm i$
$\pm k$	$\pm k$	$\pm j$	$\pm i$	± 1

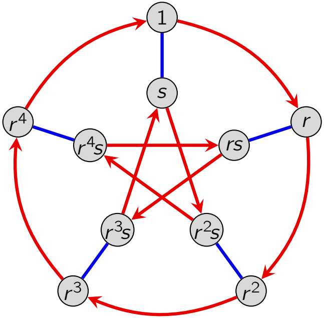
Key idea

"Collapsing" the group in this manner is a quotient $\phi\colon Q_8 \to V_4$.

If it looks like a group and quacks like a group. . .

It isn't necessarily a group. (Do you see why?)

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e



Remark

This is why we need the formal definition of a group.

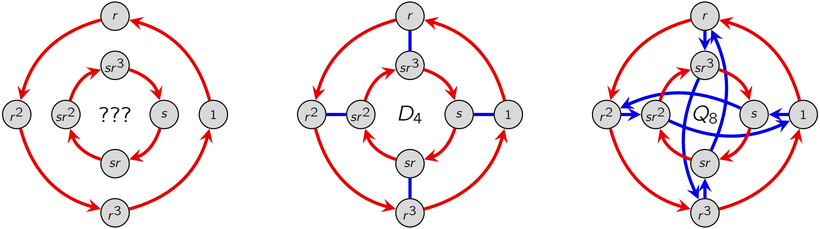
Representing groups with matrices

Finite cyclic groups can be represented by complex rotation matrices:

$$C_n \cong \langle R_n \rangle = \left\langle \begin{bmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{bmatrix} \right\rangle = \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta_n} \end{bmatrix} \right\rangle .$$

We get a dihedral group by throwing in a reflection matrix

$$D_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta_n} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle \cong \langle r, f \mid r^n = 1,\ f^2 = 1,\ rfr = f \rangle.$$



The **quaternion group** can be represented as follows:

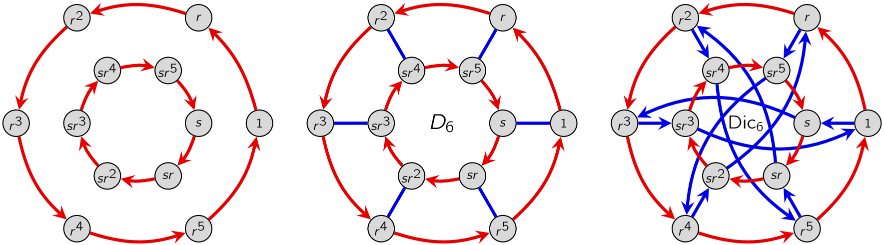
$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \cong \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \right\}.$$

Making new groups from old

What if we replaced $\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} \zeta_4 & 0 \\ 0 & \overline{\zeta_4} \end{bmatrix}$ with $\begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta_n} \end{bmatrix}$ in the quaternion group Q_8?

If n is even, then we get the **dicyclic group**:

$$\mathrm{Dic}_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta_n} \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\rangle = \langle r, s \mid r^n = 1,\ s^4 = 1,\ r^{n/2} = s^2,\ rsr = s \rangle.$$



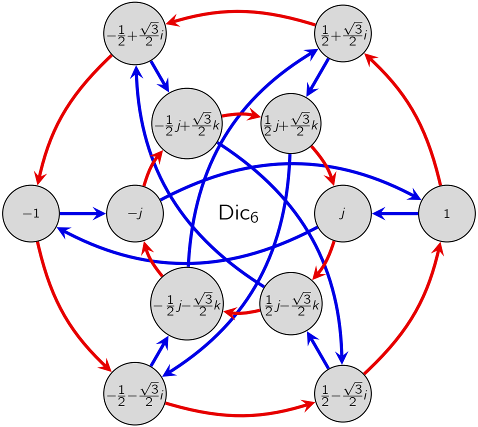
Compare to the **dihedral group**:

$$D_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta_n} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle \cong \langle r, f \mid r^n = 1,\ f^2 = 1,\ rfr = f \rangle.$$

Another way to think of the dicyclic groups

We can construct $\mathrm{Dic}_6 = \langle r, s \rangle = \langle \zeta_6, j \rangle$ as follows:

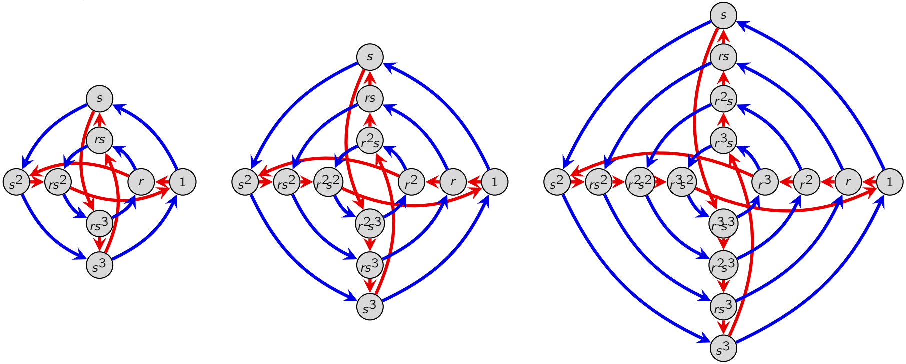
- start with the quaternion group $Q_8 = \langle i, j \rangle = \langle \zeta_4, j \rangle$
- replace $i = e^{2\pi i/4} = \zeta_4$ with the 6^{th} root of unity $\zeta_6 = e^{2\pi i/6} = \frac{1}{2} + \frac{\sqrt{3}}{2} i$
- multiplication rules $ij = k$ and $ji = -k$ remain unchanged.



The dicyclic groups

Here's another layout of the Cayley diagram of $\text{Dic}_n = \langle r, s \rangle = \langle \zeta_n, j \rangle$, for $n = 4, 6, 8$.

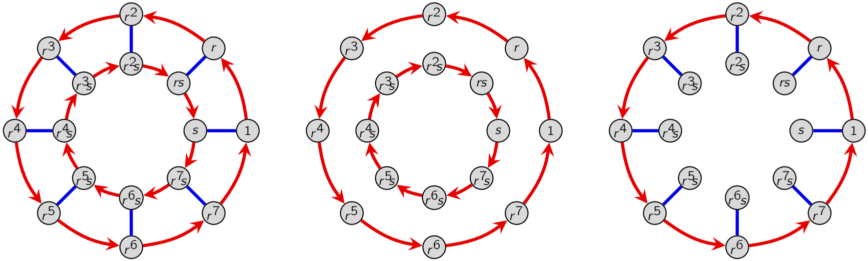
This empathizes different structural features.



When $n = 2^m$, Dic_n is also called the generalized quaternion group, Q_{2^m}.

Generalizing the dihedral groups

Let's consider another way to generalize D_n.

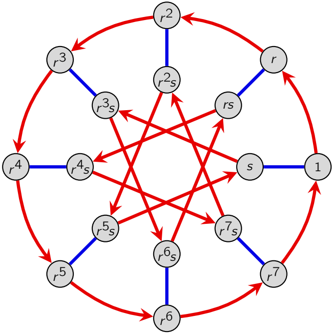


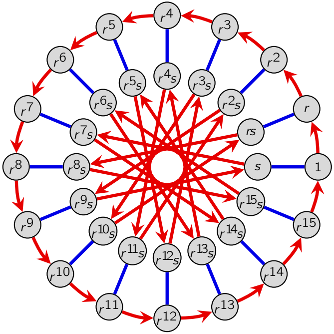
Equivalently, what can we replace the relation $srs = r^{n-1}$ with? That is,

$$G = \langle r, s \mid r^n = 1,\ s^2 = 1,\ ??? \rangle.$$

Semidihedral groups

If n is a power of 2, we can replace $srs = r^{n-1}$ with $srs = r^{n/2-1}$.





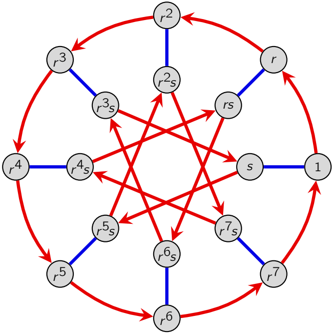
Definition

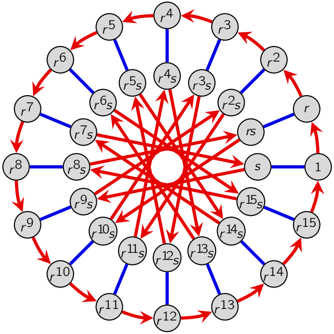
For each power of two, the semidihedral group of order 2^n is defined by

$$\mathrm{SD}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs = r^{2^{n-2}-1} \rangle.$$

Semiabelian groups

Still assuming n is a power of 2, let's replace $srs = r^{n/2-1}$ with $srs = r^{n/2+1}$.





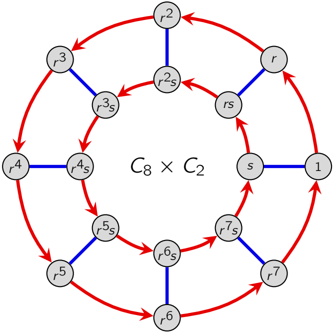
Definition

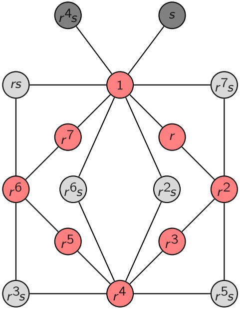
For each power of two, the semiabelian group of order 2^n is defined by

$$\mathrm{SA}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs = r^{2^{n-2}+1} \rangle.$$

One more re-wiring

Of course, there's one more way that we can re-wire D_n...





When this group has order 2^n, its presentation is

$$C_{2^n-1} \times C_2 = \langle r, s \mid r^{2^{n-1}} = s^2 = 1, \; srs = r \rangle.$$

Remarkably, this and the other three we've seen are the *only* possibilities:

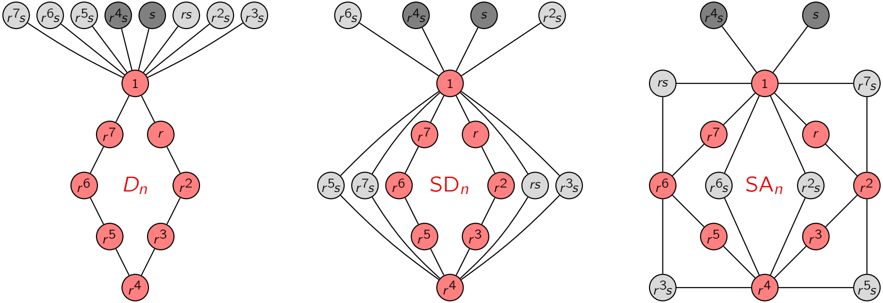
$srs = r^{-1}$ (dihedral), $\quad srs = r^{2^{n-2}-1}$ (semidihedral), $\quad srs = r^{2^{n-2}+1}$ (semiabelian).

Dihedral vs. semidiheral vs. semiabelian groups

In other words, there are exactly 4 groups of order 2^n with both:

- an element r of order 2^{n-1}
- an element $s \notin \langle r \rangle$ of order 2.

Let's compare the cycle diagrams of the three non-abelian groups from this list:



Remark

The semiabelian group SA_n and the abelian group $C_n \times C_2$ have the same orbit structure!

Groups you didn't know existed...

(and other you couldn't possibly live without!)

Theorem

There are exactly four nonabelian groups of order 2^n that have an element r of order 2^{n-1}:

1. The **dihedral group** $D_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs = r^{-1} \rangle$.
2. The dicyclic group $\mathrm{Dic}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^4 = 1,\ r^{2^{n-2}} = s^2,\ rsr = s \rangle$.
3. The semidihedral group $\mathrm{SD}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs = r^{2^{n-2}-1} \rangle$.
4. The semiabelian group $\mathrm{SA}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs = r^{2^{n-2}+1} \rangle$.

Compare our canonical representations of the **dihedral** and **dicyclic** groups:

$$D_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle, \qquad \mathrm{Dic}_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle.$$

If $n = 2^m$, we also get a **semidihedral** and **semiabelian group**:

$$\mathrm{SD}_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & -\overline{\zeta}_n \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle, \qquad \mathrm{SA}_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & -\zeta_n \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle.$$

Question: *What would happen if we took Q_8, and added in the reflection matrix?*

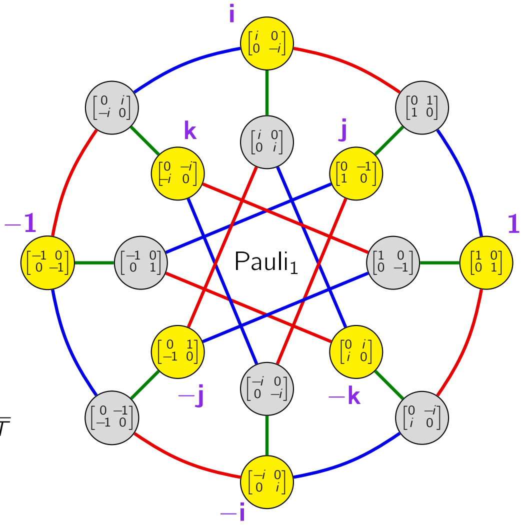
One more way to generalize quaternions: the Pauli group

$$X = F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

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

$$XY = R, \quad XZ = S, \quad YZ = \overline{T}$$



Generalizing the Pauli group

Let's replace $i = \zeta_4 = e^{2\pi i/4}$ with $\zeta_n = e^{2\pi i/n}$.

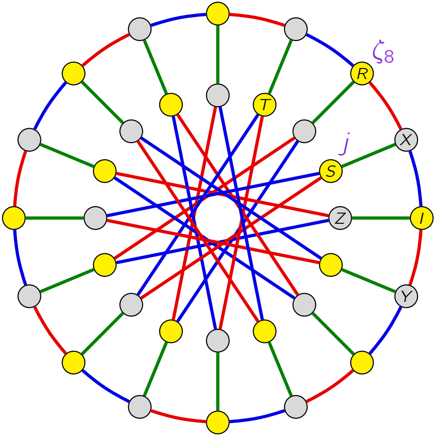
$$\langle \zeta_n, j, \zeta_n j, f \rangle \cong \Bigg\langle \underbrace{\begin{bmatrix} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{bmatrix}}_{R=R_n}, \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{S}, \underbrace{\begin{bmatrix} 0 & -\zeta_n \\ \bar{\zeta}_n & 0 \end{bmatrix}}_{T=T_n}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{F} \Bigg\rangle \cong \mathrm{Dic}_8 \rtimes_\theta C_2.$$

$$X = F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y := Y_8 = \begin{bmatrix} 0 & \bar{\zeta}_8 \\ \zeta_8 & 0 \end{bmatrix}$$

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

$$XY_8 = R_8, \qquad XZ = S, \qquad Y_8 Z = \overline{T}_8$$



The automorphism group of C_n

Each automorphism is defined by where it sends a generator: $r \mapsto r^k$.

"*each red arrow gets multiplied by k*"

The group $\text{Aut}(C_n)$ is isomorphic to the group with operation multiplication modulo n:

$$U_n = \{k > 0 \mid \gcd(n,k) = 1\}.$$

Example:

$$\text{Aut}(C_7) \cong U_7 = \{1,2,3,4,5,6\} = \langle 3 \rangle \cong C_6$$

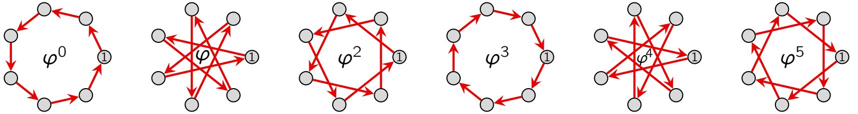
$$2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1$$

$$3^0 = 1, \quad 3^1 = 3, \quad 3^2 = 2$$

$$3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5$$

	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

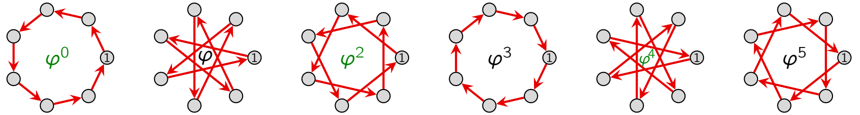
Since $U_7 = \langle 3 \rangle$, the re-wirings of C_7 are generated by the "*tripling map*" $r \overset{\varphi}{\longmapsto} r^3$.

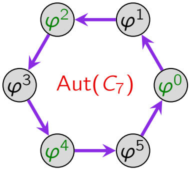


$C_7 = \langle r \rangle$ $\quad$ $r^1 \mapsto (r^1)^3 = r^3$ $\quad$ $r^3 \mapsto (r^3)^3 = r^2$ $\quad$ $r^2 \mapsto (r^2)^3 = r^6$ $\quad$ $r^6 \mapsto (r^6)^3 = r^4$ $\quad$ $r^4 \mapsto (r^4)^3 = r^5$

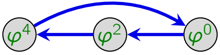
The smallest nonabelian group of odd order

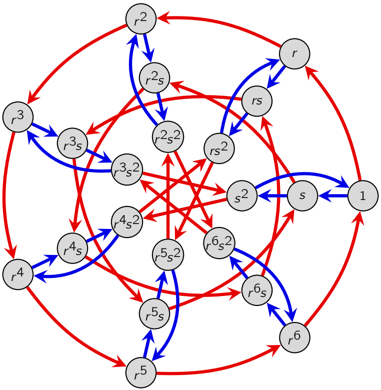
Here's how to constrct the semidirect product, $C_7 \rtimes_\theta C_3$.





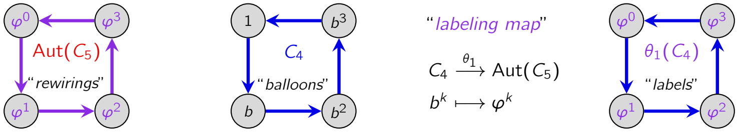
$$C_3 \xrightarrow{\theta} \mathrm{Aut}(C_7)$$
$$s^k \longmapsto \varphi^{2k}$$



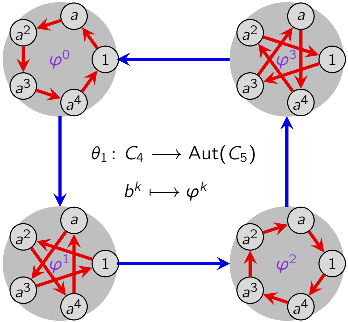


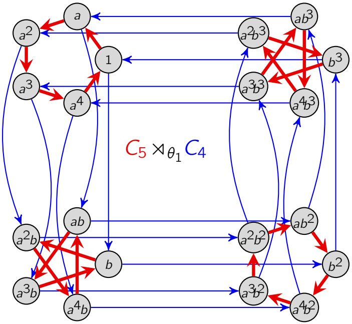
An example: the 1st semidirect product of C_5 and C_4

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



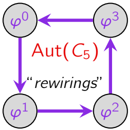
Stick in rewired copies of A, and then reconnect the B-arrows.

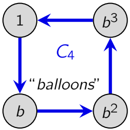




An example: the 2nd semidirect product of C_5 and C_4

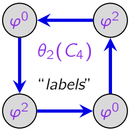
Let's now construct a different semidirect product, $C_5 \rtimes_{\theta_2} C_4$:



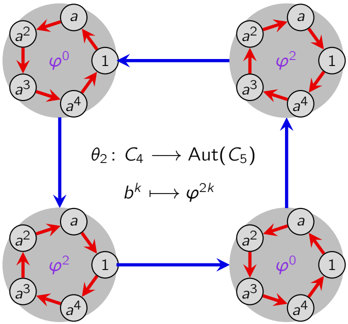


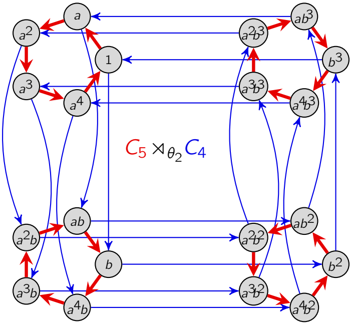
"*labeling map*"

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



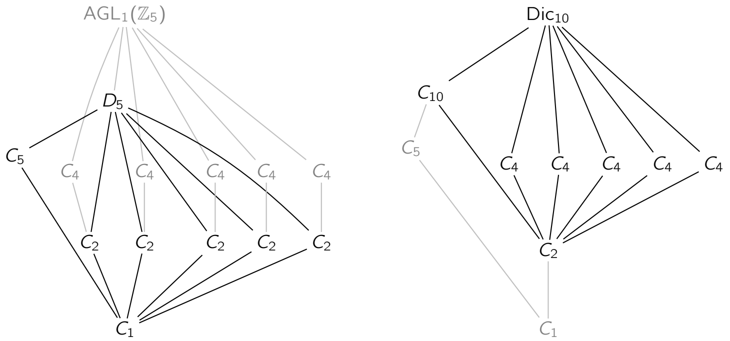
Stick in rewired copies of A, and then reconnect the B-arrows.





Embeddings vs. quotients: A preview

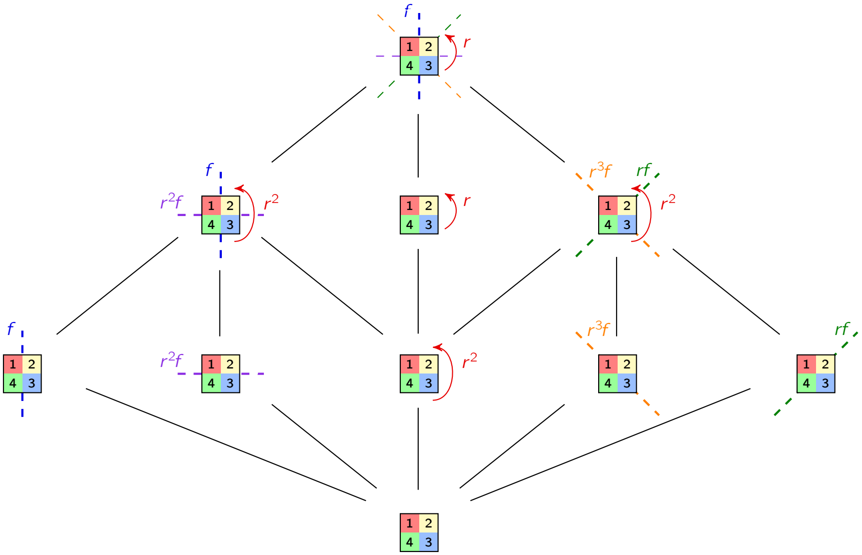
The difference between embeddings and quotient maps can be seen in the subgroup lattice:



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**.

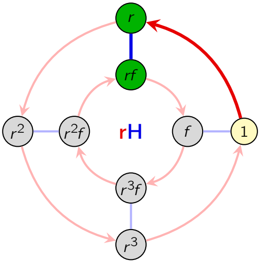
The subgroup lattice of D_4



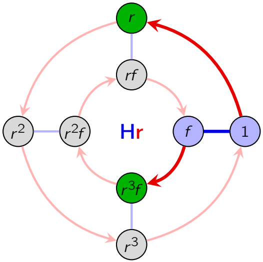
Cosets

Consider the subgroup $H = \langle f \rangle$ of D_4.

- The **left coset** rH in D_4: first go to r, then traverse all "H-paths".
- The **right coset** Hr in D_4: first traverse all H-paths, then traverse the r path.



$rH = r\{1, f\} = \{r, rf\} = rf\{f, 1\} = rfH$

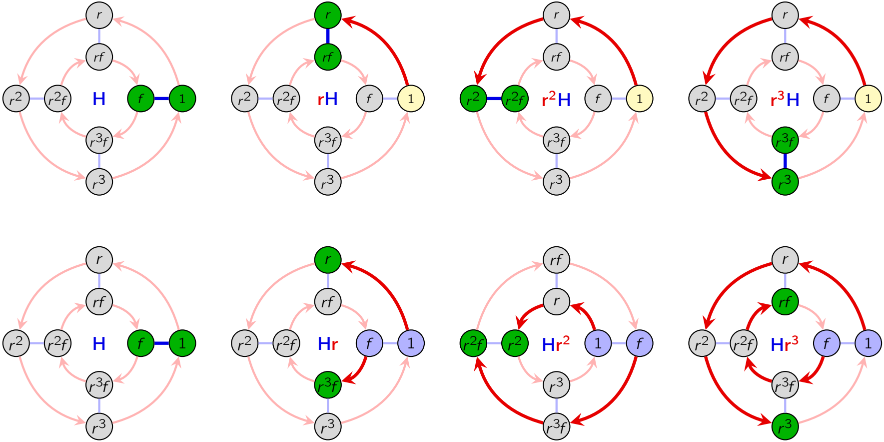


$Hr = \{1, f\}r = \{r, r^3f\} = \{f, 1\}r^3f = Hr^3f$

Key point

Left and right cosets are generally different.

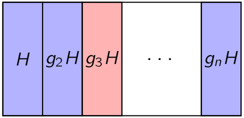
The normalizer is the union of left cosets that are right cosets



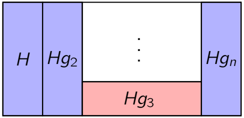
H	r^2H	rH	r^3H
f	r^2f	rf	r^3
1	r^2	r	r^3f

H	Hr^2			
f	r^2f	fr^3	r^3	Hr^3
1	r^2	r	fr	Hr

The normalizer is the union of "blue cosets"

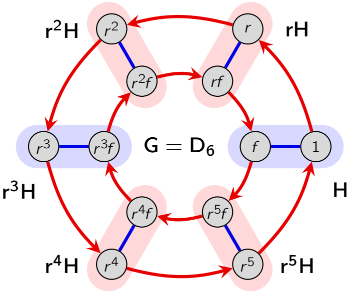


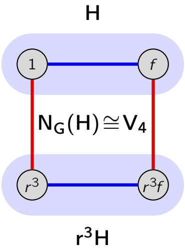
Partition of G by the left cosets of H



Partition of G by the right cosets of H

If we "collapse" G by the left cosets, then $N_G(H)$ consists of the cosets that are reachable from H by a unique path.

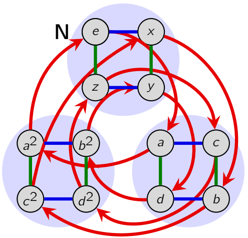


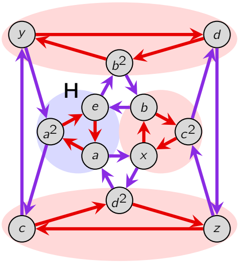


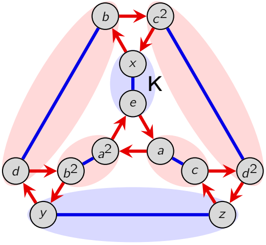
Three subgroups of A_4

The normalizer of each subgroup consists of the elements in the blue left cosets.

Here, take $a = (123)$, $x = (12)(34)$, $z = (13)(24)$, and $b = (234)$.







(124)	(234)	(143)	(132)
(123)	(243)	(142)	(134)
e	(12)(34)	(13)(24)	(14)(23)

$[A_4 : N_{A_4}(N)] = 1$

"normal"

(14)(23)	(142)	(143)
(13)(24)	(243)	(124)
(12)(34)	(134)	(234)
e	(123)	(132)

$[A_4 : N_{A_4}(H)] = 4$

"fully unnormal"

(124)	(234)	(143)	(132)
(123)	(243)	(142)	(134)
e	(12)(34)	(13)(24)	(14)(23)

$[A_4 : N_{A_4}(K)] = 3$

"moderately unnormal"

The degree of normality

Let $H \leq G$ have index $[G : H] = n < \infty$. Let's define a term that describes:

"*the proportion of cosets that are blue*"

Definition

Let $H \leq G$ with $[G : H] = n < \infty$. The **degree of normality** of H is

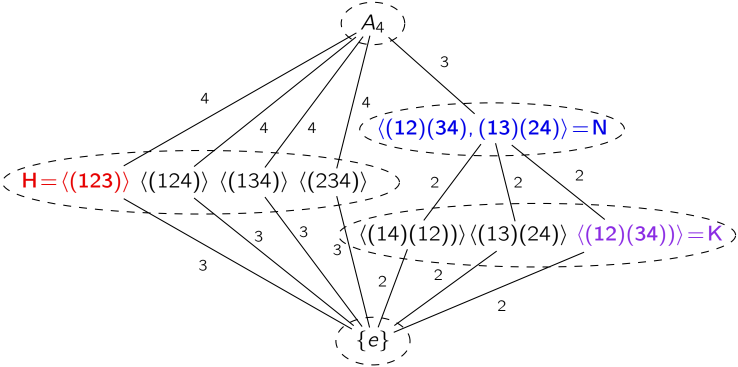
$$\mathrm{Deg}_G^{\triangleleft}(H) := \frac{|N_G(H)|}{|G|} = \frac{1}{[G : N_G(H)]}.$$

- If $\mathrm{Deg}_G^{\triangleleft}(H) = 1$, then H is normal.
- If $\mathrm{Deg}_G^{\triangleleft}(H) = \frac{1}{n}$, we'll say H is fully unnormal.
- If $\frac{1}{n} < \mathrm{Deg}_G^{\triangleleft}(H) < 1$, we'll say H is moderately unnormal.

Big idea

The degree of normality measures *how close to being normal* a subgroup is.

Revisiting A_4



Observations

- A subgroup is normal if its conjugacy class has size 1.
- The size of a conjugacy class tells us *how close to being normal* a subgroup is.
- For our "three favorite subgroups of A_4":

$$\left|\mathrm{cl}_{A_4}(N)\right| = 1 = \frac{1}{\mathrm{Deg}^{\triangleleft}_{A_4}(N)}, \quad \left|\mathrm{cl}_{A_4}(H)\right| = 4 = \frac{1}{\mathrm{Deg}^{\triangleleft}_{A_4}(H)}, \quad \left|\mathrm{cl}_{A_4}(K)\right| = 3 = \frac{1}{\mathrm{Deg}^{\triangleleft}_{A_4}(K)}.$$

The number of conjugate subgroups

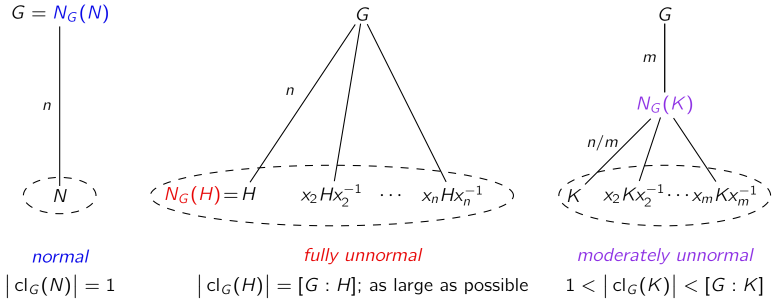
Though we do not yet have the tools to prove such a result, we will state it here.

Theorem

Let $H \leq G$ with $[G : H] = n < \infty$. Then

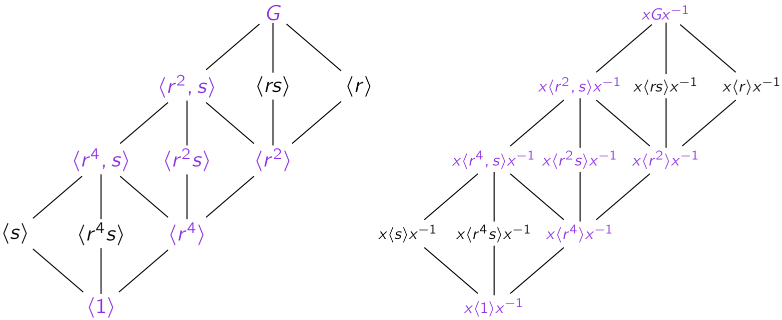
$$\left|\,\mathrm{cl}_G(H)\right| = \frac{1}{\mathrm{Deg}_G^{\triangleleft}(H)} = [G : N_G(H)].$$

That is, H has exactly $[G : N_G(H)]$ conjugate subgroups.



A mystery group of order 16

A subgroup is a **unicorn** if it's fixed by every lattice automorphism.



We can deduce that every subgroup is normal, except possibly $\langle s\rangle$ and $\langle r^4 s\rangle$.

There are two cases:

- $\langle s\rangle$ and $\langle r^4 s\rangle$ are normal $\Rightarrow s \in Z(G) \Rightarrow G$ is abelian.
- $\langle s\rangle$ and $\langle r^4 s\rangle$ are not normal $\Rightarrow \mathrm{cl}_G(\langle s\rangle) = \big\{\langle s\rangle, \langle r^4 s\rangle\big\} \Rightarrow G$ is nonabelian.

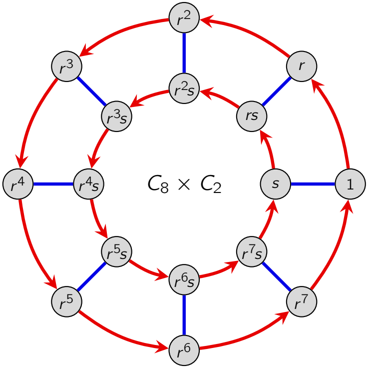
This doesn't necessarily mean that both of these are actually possible...

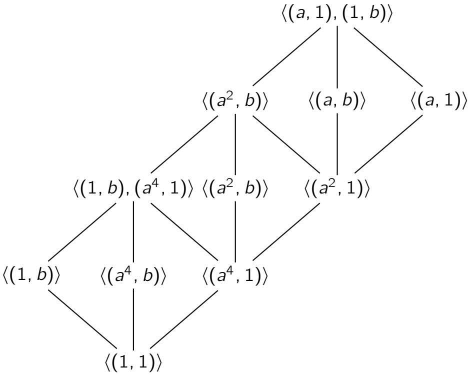
A mystery group of order 16

It's straightforward to check that this is the subgroup lattice of

$$C_8 \times C_2 = \langle r, s \mid r^8 = s^2 = 1, srs = r \rangle.$$

Let $r = (a, 1)$ and $s = (1, b)$, and so $C_8 \times C_2 = \langle r, s \rangle = \langle (a, 1), (1, b) \rangle$.

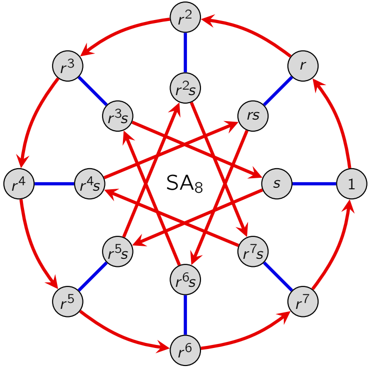


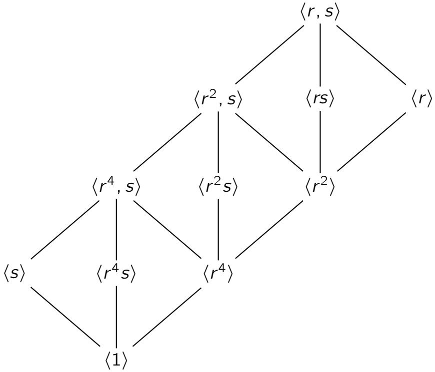


A mystery group of order 16

However, the nonabelian case is possible as well! The following also works:

$$SA_8 = \langle r, s \mid r^8 = s^2 = 1, srs = r^5 \rangle.$$

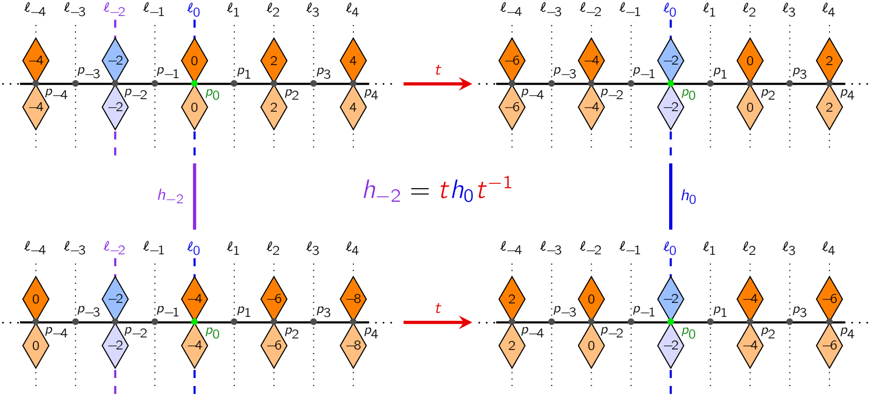




Conjugation preserves structure

Let $h = h_0$ denote the reflection across the central axis, ℓ_0.

Suppose we want to reflect across a different axis, say ℓ_{-2}.



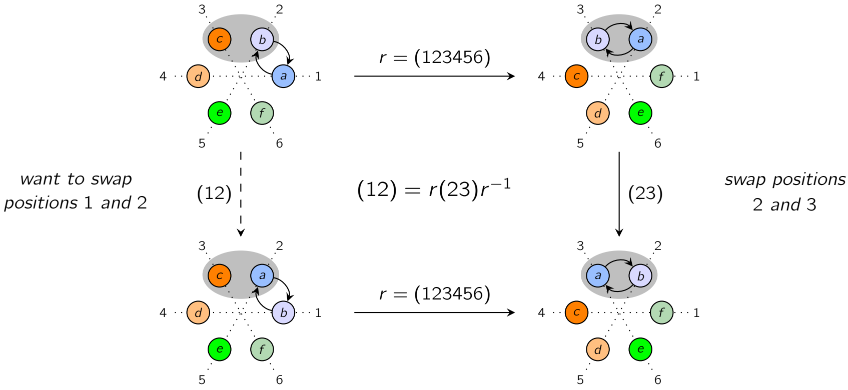
Conjugation preserves structure in the symmetric group

The symmetric group $G = S_6$ is generated by any transposistion and any n-cycle.

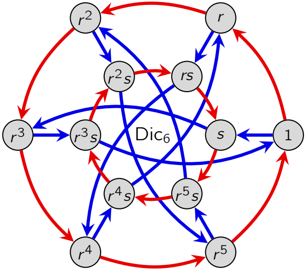
Consider the permutations of seating assignments around a circular table achievable by

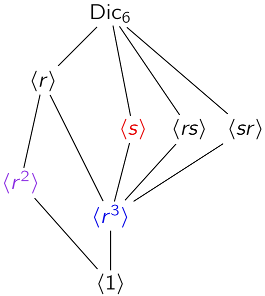
- (23): "*people in chairs* 2 *and* 3 *may swap seats*"
- (123456): "*people may cyclically rotate seats counterclockwise*"

Here's how to get people in chairs 1 and 2 to swap seats:



An example: conjugacy classes and centralizers in Dic_6





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

conjugacy classes

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

$[G : C_G(r^3)] = 1$

"central"

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

$[G : C_G(r^2)] = 2$

"moderately uncentral"

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

$[G : C_G(s)] = 3$

"fully unncentral"

The size of a conjugacy class

The following result is analogous to an earlier one on the degree of normality and $|\text{cl}_G(H)|$.

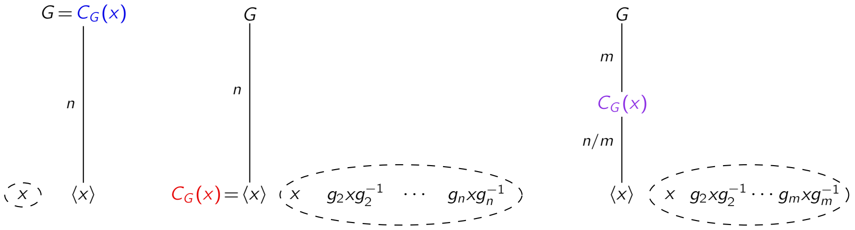
Theorem

Let $x \in G$ with $[G : \langle x \rangle] = n < \infty$. Then

$$\big|\text{cl}_G(x)\big| = \frac{1}{\text{Deg}_G^C(x)} = [G : C_G(x)].$$

That is, there are exactly $[G : C_G(x)]$ elements conjugate to x.

Both of these are special cases of the **orbit-stabilizer theorem**, about group actions.



central

$\big|\text{cl}_G(x)\big| = 1$

fully uncentral

$\big|\text{cl}_G(x)\big| = [G : \langle x \rangle]$; as large as possible

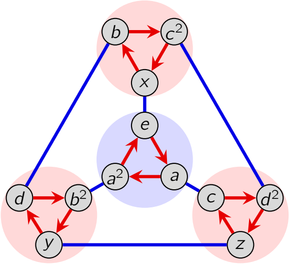
moderately uncentral

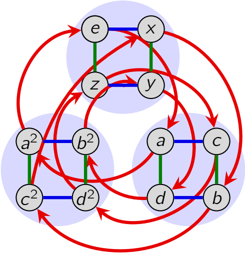
$1 < \big|\text{cl}_G(x)\big| < [G : \langle x \rangle]$

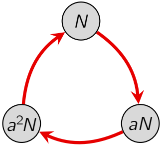
Quotient groups

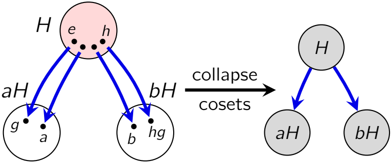
Big idea

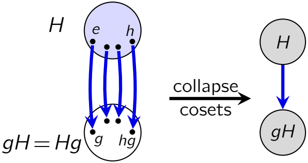
The quotient group G/N exists iff $N \trianglelefteq G$.



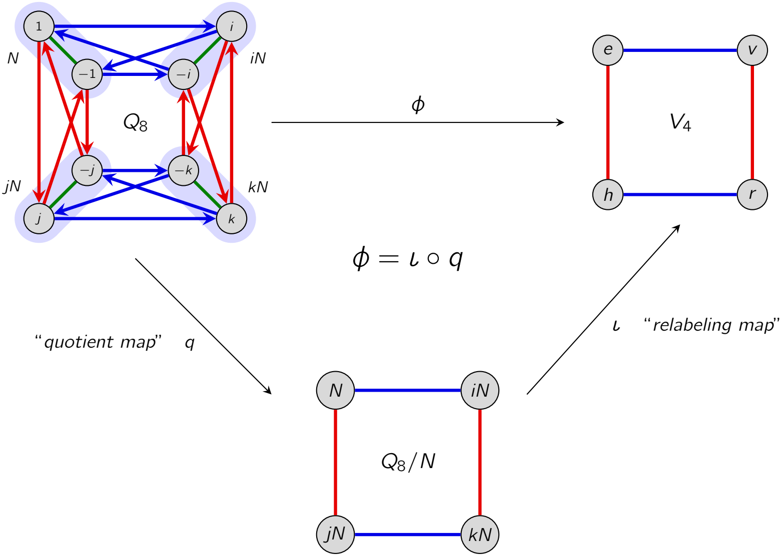








The 1st isomorphism theorem: "*all homomorphic images are quotients*"



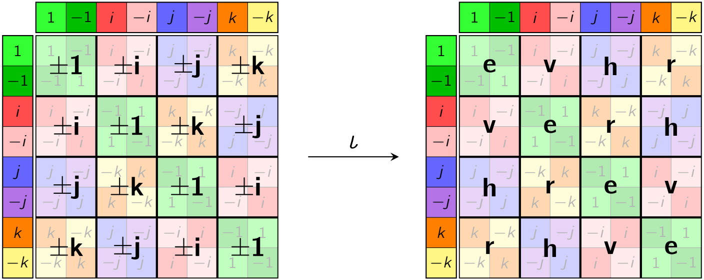
The 1st isomorphism theorem: "*all homomorphic images are quotients*"

The 1st isomorphism theorem, $G/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$, says that

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

decomposes as the composition of:

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



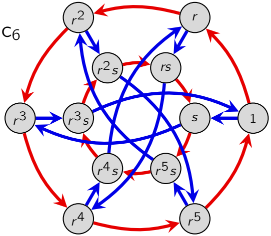
Next natural question

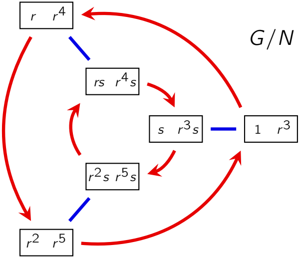
What do we know about quotients?

The ~~4th~~ 2nd isomorphism theorem: "*subgroups of quotients*"

Subgroups of G/N are simply quotients of subgroups of G by N.

$G = \mathrm{Dic}_6$





G/N

The element of G/N are cosets, or "**shoeboxes**"

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

$\langle r \rangle \leq G$

items out of the box

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

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

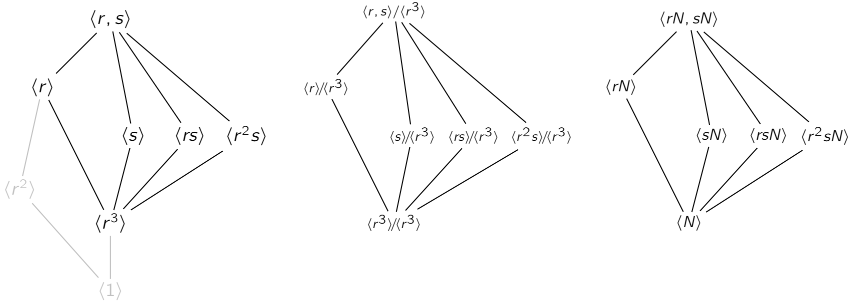
shoeboxes w/ lids off

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

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

shoeboxes w/ lids on

The ~~4th~~ 2nd isomorphism theorem: "*subgroups of quotients*"



Moreover, $H/N \trianglelefteq G/N$ iff $H \trianglelefteq G$.

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

$\langle s\rangle \leq G$

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

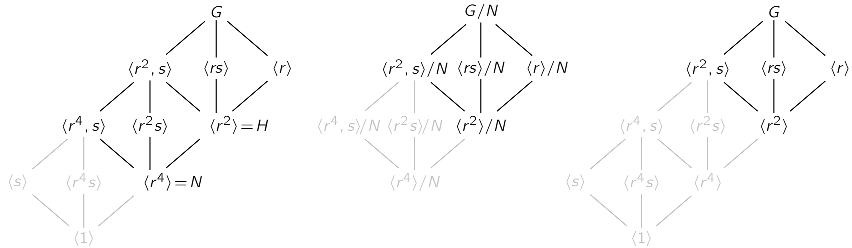
$\langle s\rangle/N \leq G/N$

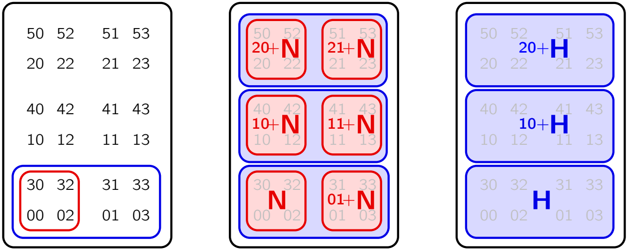
$r^2 N$	$r^2 sN$
rN	rsN
N	sN

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

The 3rd isomorphism theorem: "*quotients of quotients*"

If $H/N \lhd G/N$, then $(G/N)/(H/N) \cong G/H$. "*So easy, even a freshman can do it!*"





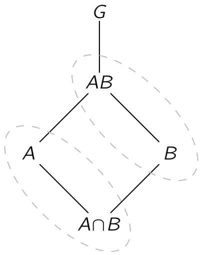
$N \leq H \leq G$

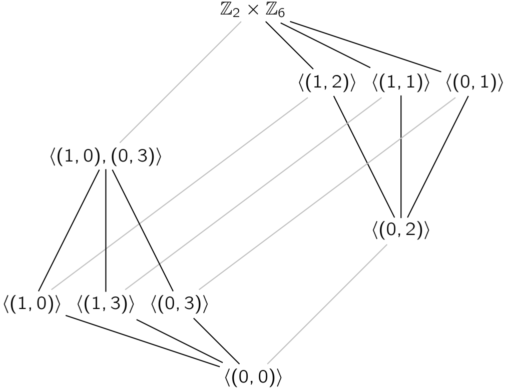
G/N consists of 6 cosets
$H/N = \{N,\ 01+N\}$

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

The ~~2nd~~ 4th isomorphism theorem: "*quotients of products by factors*"

If A normalizes B, then $AB/B \cong A/(A \cap B)$. (*Your freshman will get this one wrong.*)





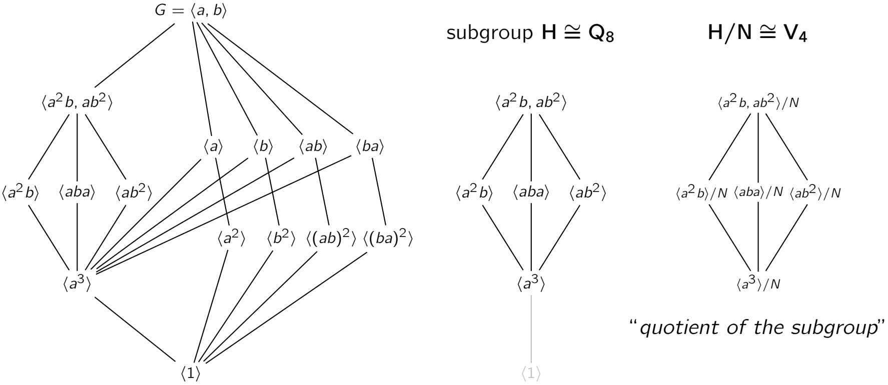
The fact that the subgroup lattice of V_4 is diamond shaped is coincidental.

The 5th isomorphism theorem: "*subgroups and quotients commute*"

Key idea

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

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



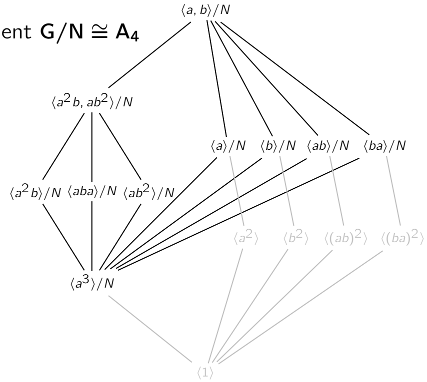
The 5th isomorphism theorem: "*subgroups and quotients commute*"

Key idea

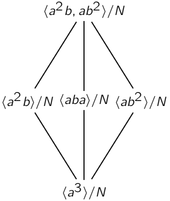
The quotient of a subgroup is just the subgroup of the quotient.

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*"

What is a group action? ("wrong" answers only)

Definition

A left group action is a mapping

$$G \times S \longrightarrow S\,, \qquad (a, s) \longmapsto a.s$$

such that

- $(ab).s = a.(b.s)$, for all $a, b \in G$ and $s \in S$
- $e.s = s$, for all $s \in S$.

A right group action is a mapping

$$G \times S \longrightarrow S\,, \qquad (a, s) \longmapsto s.a$$

such that

- $s.(ab) = (s.a).b$, for all $a, b \in G$ and $s \in S$
- $s.e = s$, for all $s \in S$.

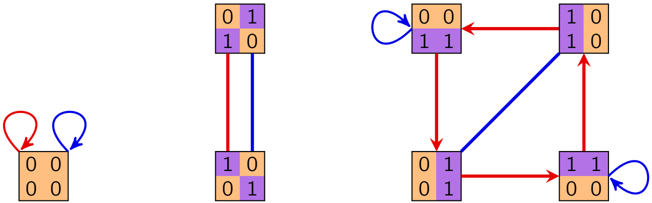
Group actions

Imagine a "group switchboard:" every element of $D_4 = \langle r, f \rangle$ has a **button**, that permutes the set:

$$S = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}$$

The group action rule

Pressing the *a*-**button** followed by the *b*-**button**, is the same as pressing the *ab*-**button**.



Formally, this is just a homomorphism $\phi \colon G \to \mathrm{Perm}(S)$, because

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

Five features of every group action

Every group action has **five fundamental features** that we will always try to understand.

Local features

- The orbit of $s \in S$ is the "*what elements can we reach from s?*":

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

- The stabilizer of s in G is "*the buttons that fix s*"

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

(iii) The fixed point set of $g \in G$ are "*the set elements fixed by g-button*":

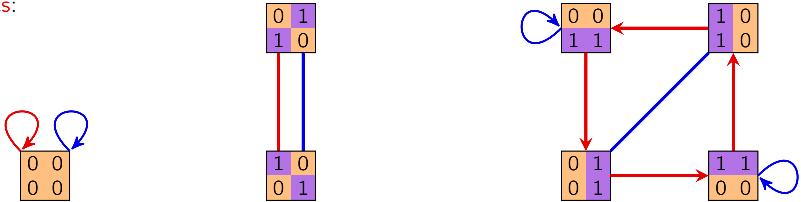
$$\text{fix}(g) = \{s \in S \mid s.\phi(g) = s\}.$$

Global features

- **kernel**: $\text{Ker}(\phi) = \bigcap_{s \in S} \text{stab}(s)$ "*broken buttons*"
- **fixed points** $\text{Fix}(\phi) = \bigcap_{g \in G} \text{fix}(g)$ "*set elements that never move*"

Local features of our "binary square" example

Orbits:



The stabilizers are:

$$\mathrm{stab}\left(\begin{bmatrix}0&0\\0&0\end{bmatrix}\right)=D_4,\qquad \mathrm{stab}\left(\begin{bmatrix}0&1\\1&0\end{bmatrix}\right)=\mathrm{stab}\left(\begin{bmatrix}1&0\\0&1\end{bmatrix}\right)=\{1,r^2,rf,r^3f\}$$

$$\mathrm{stab}\left(\begin{bmatrix}0&0\\1&1\end{bmatrix}\right)=\mathrm{stab}\left(\begin{bmatrix}1&1\\0&0\end{bmatrix}\right)=\langle f\rangle$$

$$\mathrm{stab}\left(\begin{bmatrix}0&1\\0&1\end{bmatrix}\right)=\mathrm{stab}\left(\begin{bmatrix}1&1\\0&0\end{bmatrix}\right)=\langle r^2f\rangle$$

The fixed point sets are $\mathrm{fix}(1)=S$, and

$$\mathrm{fix}(r)=\mathrm{fix}(r^3)=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix}\right\}\qquad \mathrm{fix}(r^2)=\mathrm{fix}(rf)=\mathrm{fix}(r^3f)=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\1&0\end{bmatrix},\begin{bmatrix}1&0\\0&1\end{bmatrix}\right\}$$

$$\mathrm{fix}(f)=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}0&0\\1&1\end{bmatrix},\begin{bmatrix}1&1\\0&0\end{bmatrix}\right\}\qquad \mathrm{fix}(r^2f)=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&1\end{bmatrix},\begin{bmatrix}1&0\\1&0\end{bmatrix}\right\}$$

"Fixed point tables": a checkmark at (g, s) means g fixes s

	0 0 0 0	0 1 1 0	1 0 0 1	0 0 1 1	0 1 0 1	1 0 1 0	1 1 0 0
1	✓	✓	✓	✓	✓	✓	✓
r	✓						
r^2	✓	✓	✓				
r^3	✓						
f	✓			✓			✓
rf	✓	✓	✓				
$r^2 f$	✓				✓	✓	
$r^3 f$	✓	✓	✓				

- $\text{stab}(s)$: read off the column.
- $\text{fix}(g)$: read off the rows:
- $\text{Ker}(\phi)$: rows with all checkmarks
- $\text{Fix}(\phi)$: columns with all checkmarks
- $|\text{Orb}(\phi)|$ = average #checkmarks per row = $24/|D_4| = 3$

Groups acting on themselves by conjugation

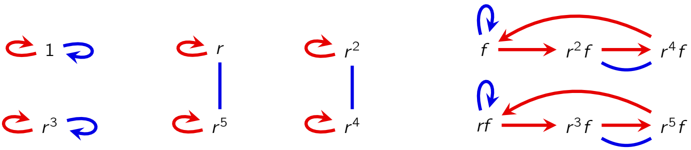
1. **Orbit-stabilizer theorem**. "*the size of an orbit is the index of the stabilizer*":

$$\big|\operatorname{cl}_G(x)\big| = [G : C_G(x)] = \frac{|G|}{|C_G(x)|}.$$

2. **Orbit-counting theorem**. "*the number of orbits is the average number of elements fixed by a group element*":

$$\#\text{conjugacy classes of } G = \text{average size of a centralizer}.$$

Example. $D_6 = \langle r, f \rangle$:



Stabilizers (i.e., centralizers):

$$\text{stab}(r) = \text{stab}(r^2) = \text{stab}(r^4) = \text{stab}(r^5) = \langle r \rangle,$$

$$\text{stab}(1) = \text{stab}(r^3) = D_6, \qquad \text{stab}(f) = \langle r^3, f \rangle, \qquad \text{stab}(r^i f) = \langle r^3, r^i f \rangle.$$

Groups acting on themselves by conjugation

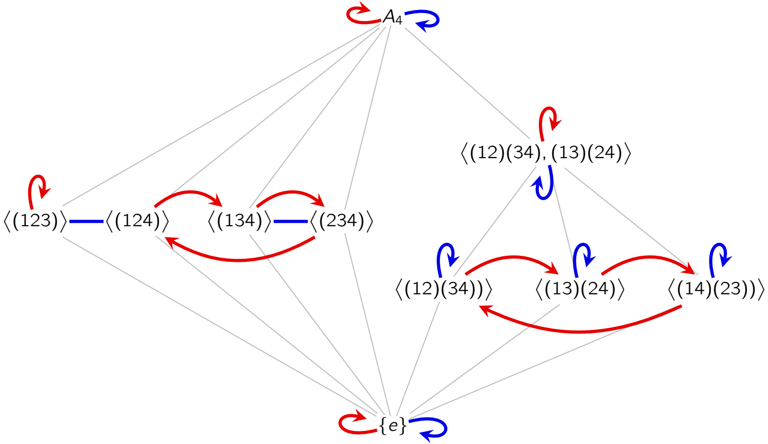
Here is the "*fixed point table*". Note that $\text{Ker}(\phi) = \text{Fix}(\phi) = \langle r^3 \rangle$.

	1	r	r^2	r^3	r^4	r^5	f	rf	r^2f	r^3f	r^4f	r^5f
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
r	✓	✓	✓	✓	✓	✓						
r^2	✓	✓	✓	✓	✓	✓						
r^3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
r^4	✓	✓	✓	✓	✓	✓						
r^5	✓	✓	✓	✓	✓	✓						
f	✓			✓			✓			✓		
rf	✓			✓				✓			✓	
r^2f	✓			✓					✓			✓
r^3f	✓			✓			✓			✓		
r^4f	✓			✓				✓			✓	
r^5f	✓			✓					✓			✓

By the **orbit-counting theorem**, there are $|\text{Orb}(\phi)| = 72/|D_6| = 6$ conjugacy classes.

Groups acting on subgroups by conjugation

Here is an example of $G = A_4 = \langle (123), (12)(34) \rangle$ acting on its subgroups.



Let's take a moment to revisit our "*three favorite examples*" from Chapter 3.

$$N = \langle (12)(34), (13)(24) \rangle, \qquad H = \langle (123) \rangle, \qquad K = \langle (12)(34) \rangle.$$

Groups acting on subgroups by conjugation

Here is the "*fixed point table*". Note that $\mathrm{Ker}(\phi) = \{e\}$ and $\mathrm{Fix}(\phi) = \{\langle e\rangle, A_4, N\}$.

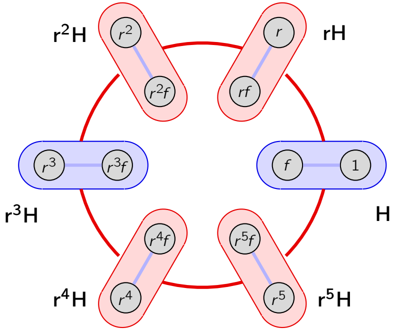
	$\langle e\rangle$	$\langle(123)\rangle$	$\langle(124)\rangle$	$\langle(134)\rangle$	$\langle(234)\rangle$	$\langle(12)(34)\rangle$	$\langle(13)(24)\rangle$	$\langle(14)(23)\rangle$	$\langle(12)(34),(13)(24)\rangle$	A_4
e	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
(123)	✓	✓							✓	✓
(132)	✓	✓							✓	✓
(124)	✓		✓						✓	✓
(142)	✓		✓						✓	✓
(134)	✓			✓					✓	✓
(143)	✓			✓					✓	✓
(234)	✓				✓				✓	✓
(243)	✓				✓				✓	✓
$(12)(34)$	✓					✓	✓	✓	✓	✓
$(13)(24)$	✓					✓	✓	✓	✓	✓
$(14)(23)$	✓					✓	✓	✓	✓	✓

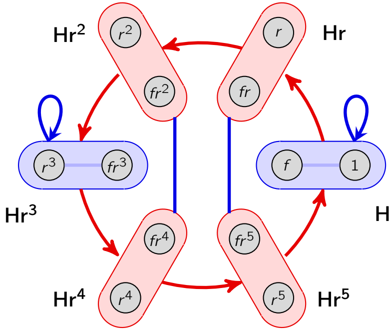
By the **orbit-counting theorem**, there are $|\mathrm{Orb}(\phi)| = 60/|A_4| = 5$ conjugacy classes.

Groups acting on cosets of H by right-multiplication

The quotient process is done by collapsing the Cayley diagram by the left cosets of H.

In contrast, this action is the result of collapsing the Cayley diagram by the right cosets.





What are solvable and nilpotent groups ("wrong" answers only)

Definition

A group G is **solvable** if there are subgroups

$$1 = G_0 \leq G_1 \leq \cdots \leq G_k = G$$

such that $G_{j-1} \trianglelefteq G_j$ and G_j / G_{j-1} is abelian.

Definition

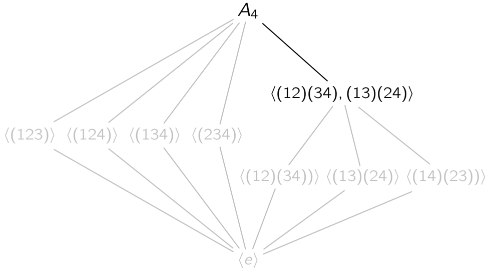
A group G is **nilpotent** if there are subgroups

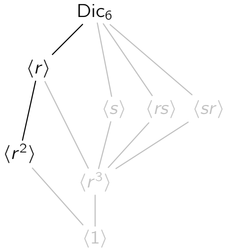
$$1 = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots \trianglelefteq Z_k = G$$

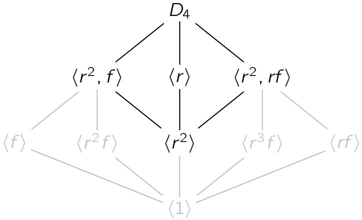
where $Z_1 = Z(G)$ and $Z_{i+1}/Z_i = Z(G/Z_i)$.

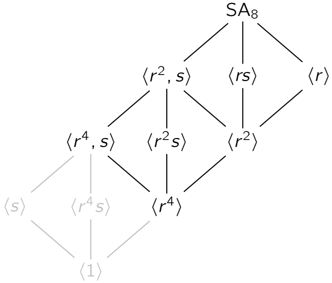
Commutator subgroups and abelianizations

The commutator subgroup G' is the smallest such that G/G' is abelian.





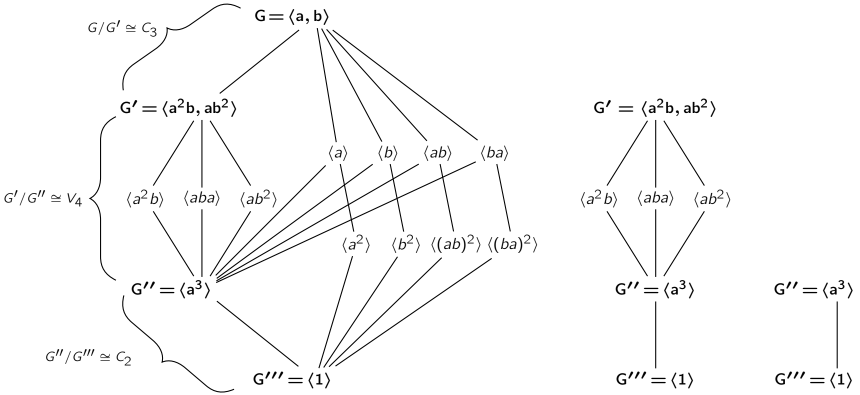




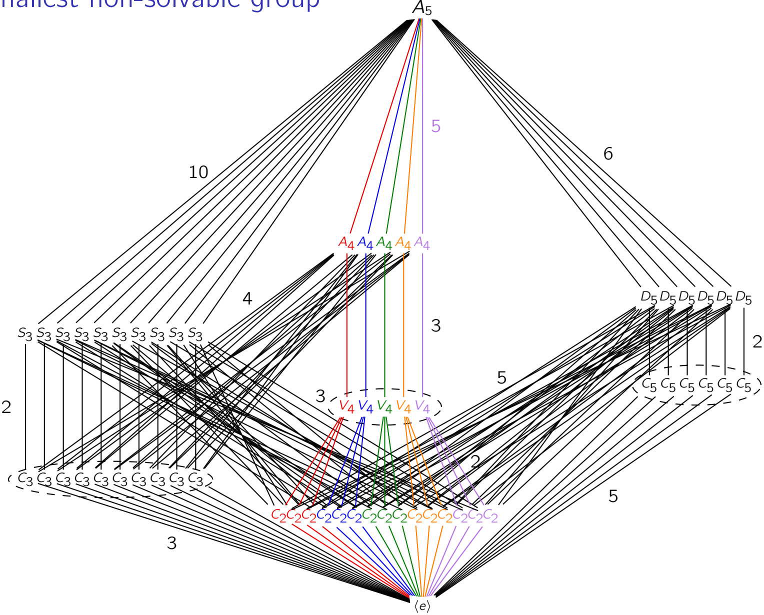
Solvable groups: "*lattices we can climb down*"

Start at the top of a subgroup lattice, and take successive maximal abelian steps down.

A group is solvable if we reach the bottom.



The smallest non-solvable group

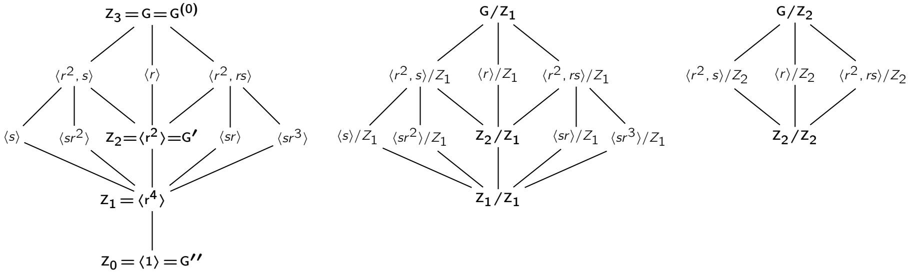


Nilpotent groups: "*lattices we can climb up*"

Start at the bottom of a lattice. Climb up to the center, $Z(G)$.

Chop everything off below, i.e., take the quotient, $G/Z(G)$.

Repeat this process. If we reach the top, then G is nilpotent.



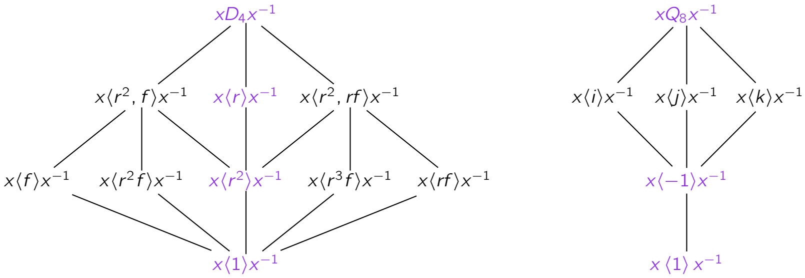
Theorem

A group is nilpotent iff it has no fully unnormal subgroups.

In particular, p-groups are nilpotent.

Inner and outer automorphisms

Conjugating G by a fixed element $x \in G$ is an inner automorphism



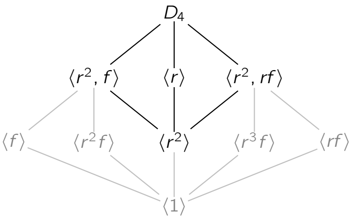
The inner automorphism group is $\mathrm{Inn}(G) \cong G/Z(G)$.

Inner automorphism permute elements within conjugacy classes.

Remark

The group Q_8 has "*outer automorphism(s)*" that permute i, j, and k.

Automorphisms of D_4



$\mathrm{Inn}(D_4) \cong D_4/\langle r^2\rangle \cong V_4$

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

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

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

inner automorphisms of D_4 permute elements within conjugacy classes

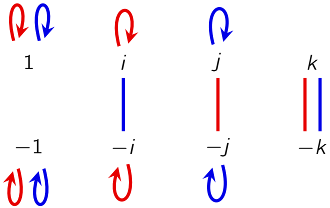
There is also an outer automorphism

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

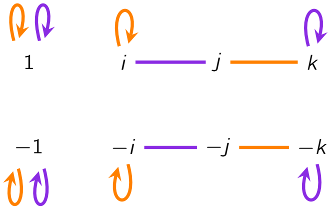
that swaps the "two types" of reflections of the square.

Automorphisms of Q_8

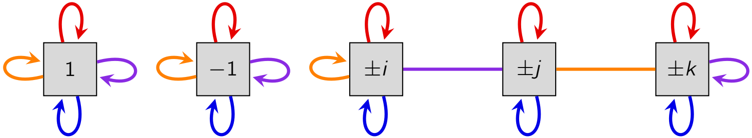
$\mathrm{Inn}(Q_8) \cong V_4$



$\mathrm{Out}(Q_8) \cong S_3$



The group $\mathrm{Aut}(Q_8)$ acts on the conjugacy classes:



Overlaying these two diagrams gives

$$\mathrm{Aut}(Q_8) \cong \mathrm{Inn}(Q_8) \rtimes \mathrm{Out}(Q_8) \cong V_4 \rtimes S_3 \cong S_4.$$

Closing remarks (Are we having fun yet?)

The first introductory algebra book to take a Cayley diagram approach is *Visual group theory* by Nathan Carter (2009).

Steven Strogatz called it the "*best introduction to group theory, or any branch of higher mathematics, that I've ever seen*."

However, it's a "general audience" book, not at the level of standard algebra texts.

Dana Ernst (Northern Arizona) has a (googlable) set of IBL notes using a visual approach.

I'm writing a visual algebra book at the approx. level of Dummit & Foote.

I will continue to post all course materials (slides, HW, etc.) on my webpage.

`http://www.math.clemson.edu/~macaule/classes/f21_math4120/`

I am happy to share the LaTeX source code.

Going forward...

- *I need a title for my book!* Any ideas?
- Nathan, Dana, and I have discussed organizing a workshop or special session on teaching visual algebra.
- If you like these ideas, please spread the word!
- I would love to explore the pedagogy of this with math ed folk(s).

Thank you for coming!