Chapter 3: Group structure

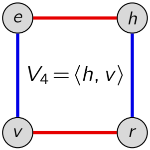
Matthew Macauley

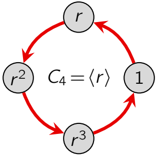
Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 8510, Abstract Algebra

Subgroup lattices

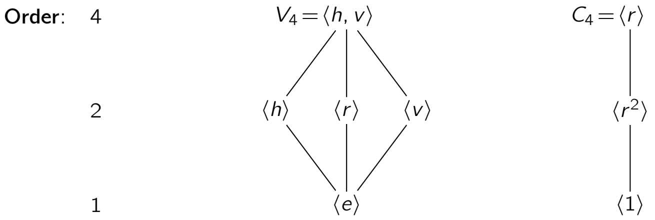
Let's compare the two groups of order 4:



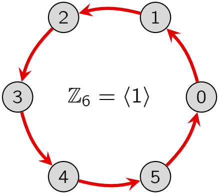


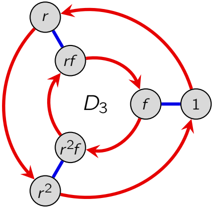
- Proper subgroups of V_4: $\langle h \rangle = \{e, h\}$, $\langle v \rangle = \{e, v\}$, $\langle r \rangle = \{e, r\}$, $\langle e \rangle = \{e\}$.
- Subgroups of C_4: $\langle r \rangle = \{1, r, r^2, r^3\} = \langle r^3 \rangle$, $\langle r^2 \rangle = \{1, r^2\}$, $\langle 1 \rangle = \{1\}$.

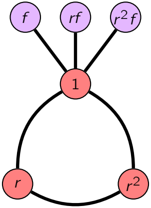
It is illustrative to arrange them in a subgroup lattice.



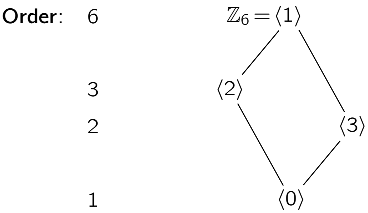
The two groups of order 6

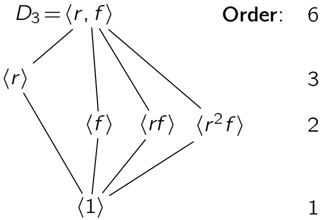






Here are their subgroup lattices:





Intersections of subgroups

Proposition (exercise)

For any collection $\{H_\alpha \mid \alpha \in A\}$ of subgroups of G, the intersection $\bigcap_{\alpha \in A} H_\alpha$ is a subgroup.

Every subset $S \subseteq G$, not necessarily finite, generates a subgroup, denoted

$$\langle S \rangle = \big\{ s_1^{e_1} s_2^{e_2} \cdots s_k^{e_k} \mid s_i \in S,\ e_i = \{1, -1\} \big\}.$$

That is, $\langle S \rangle$ consists finite words built from elements in S and their inverses.

Proposition (proof on board)

For any $S \subseteq G$, the subgroup $\langle S \rangle$ is the intersection of all subgroups containing S:

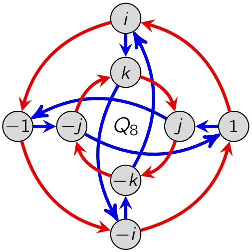
$$\langle S \rangle = \bigcap_{S \subseteq H_\alpha \leq G} H_\alpha \,,$$

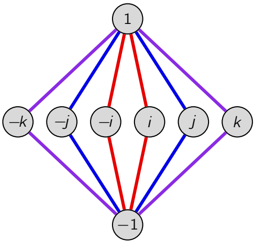
That is, the subgroup *generated by S* is the *smallest subgroup containing S*.

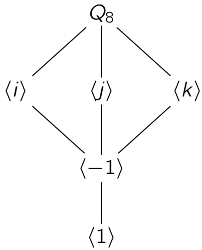
- LHS: the subgroup built "*from the bottom up*"
- RHS: the subgroup built "*from the top down*"

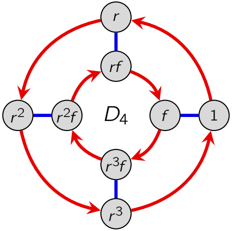
There are a number of mathematical objects that can be viewed in these two ways.

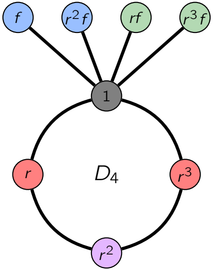
The two nonabelian groups of order 8

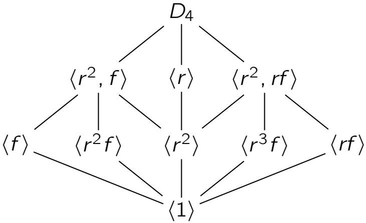




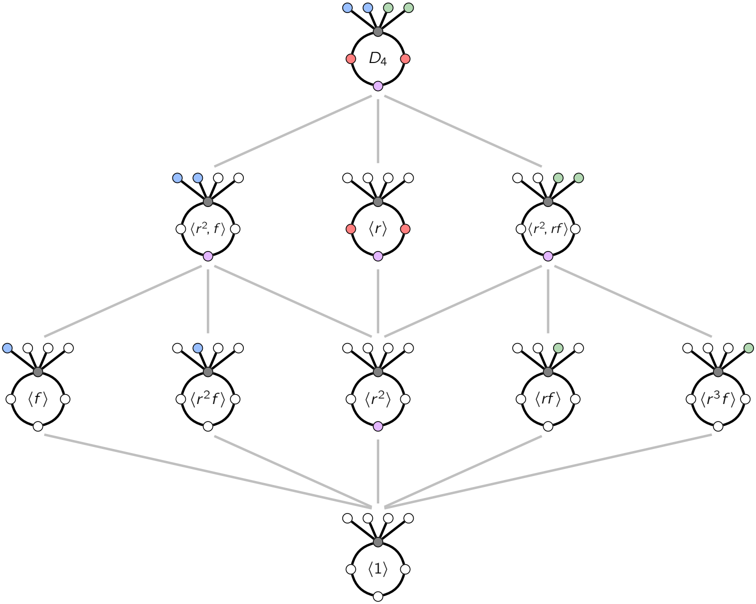




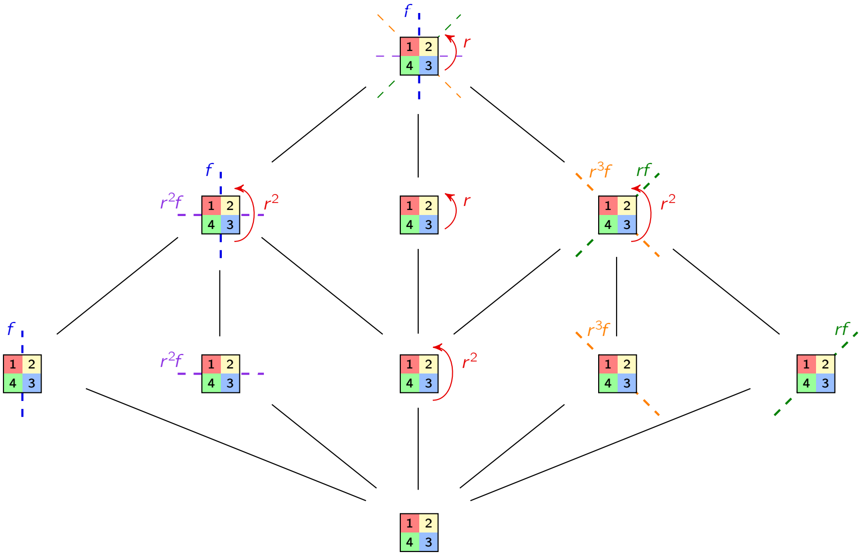




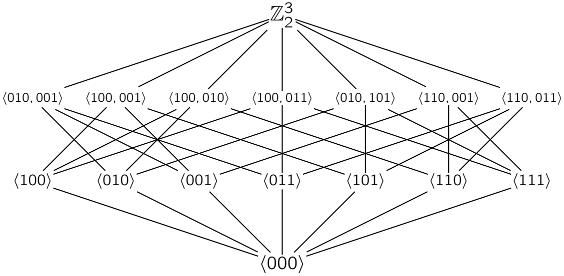
The subgroup lattice of D_4

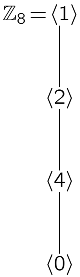


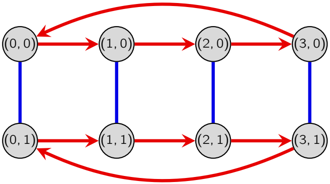
The subgroup lattice of D_4

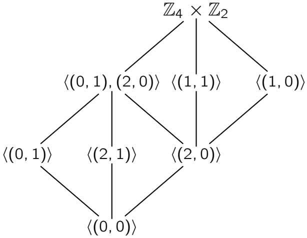


The three abelian groups of order 8









More on subgroups

Tip

It will be *essential* to learn the subgroup lattices of our standard examples of groups.

Let's summarize the sizes of the subgroups of the groups of order 8 that we have seen.

	C_8	Q_8	$C_4 \times C_2$	D_4	C_2^3
# elts. of order 8	4	0	0	0	0
# elts. of order 4	2	6	4	2	0
# elts. of order 2	1	1	3	5	7
# elts. of order 1	1	1	1	1	1
# subgroups	4	6	8	10	16

Rule of thumb

Groups with elements of small order tend to have more subgroups than those with elements of large order.

One-step subgroup test (exercise)

A subset $H \subseteq G$ is a subgroup if and only if if the following condition holds:

$$\text{If } x, y \in H, \text{ then } xy^{-1} \in H.$$

Subgroups of cyclic groups

Proposition

Every subgroup of a cyclic group is cyclic.

Proof

Let $H \leq G = \langle x \rangle$, and $|H| > 1$.

Let x^k be the smallest positive power of x in $H = \{x^k \mid k \in \mathbb{Z}\}$

We'll show that all elements of H have the form $(x^k)^m = x^{km}$ for some $m \in \mathbb{Z}$.

Take any other $x^\ell \in H$, with $\ell > 0$, and write $\ell = qk + r$, where $0 \leq r < k$.

We have $x^\ell = x^{qk+r}$, and hence

$$x^r = x^{\ell - qk} = x^\ell x^{-qk} = x^\ell (x^k)^{-q} \in H.$$

Minimality of $k > 0$ forces $r = 0$. $\square$

Corollary

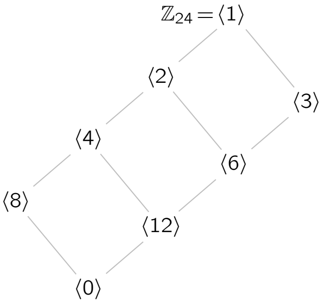
The subgroup of $G = \mathbb{Z}$ generated by $a_1, \dots, a_k$ is $\langle \gcd(a_1, \dots, a_k) \rangle \cong \mathbb{Z}$. $\square$

Subgroups of cyclic groups

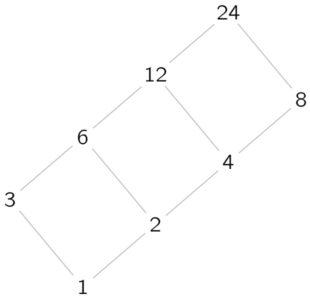
If d divides n, then $\langle d \rangle \leq \mathbb{Z}_n$ has order n/d. Moreover, all cyclic subgroups have this form.

Corollary

The subgroups of $\mathbb{Z}_n$ are of the form $\langle d \rangle$ for every divisor d of n. □



subgroup lattice



divisor lattice

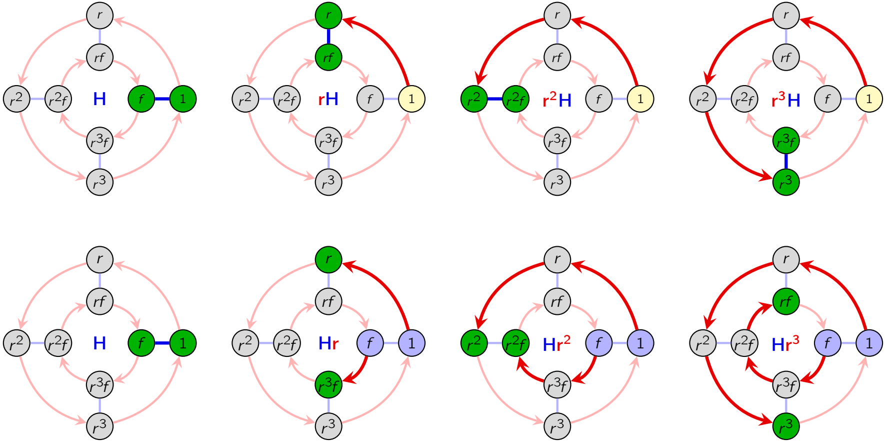
The order can be read off from the divisor lattice of 24.

Cosets

Definition

Let $H \leq G$. Given $x \in G$, its left coset xH and right coset Hx are:

$$xH = \{xh \mid h \in H\}, \qquad\qquad Hx = \{hx \mid h \in H\}.$$



Lagrange's theorem

Remark

For any $H \leq G$, the left cosets of H partition G into subsets of equal size (exercise).

The right cosets also partition G into subsets of equal size, but *they may be different.*

Let's compare these partitions for $H = \langle f \rangle$ in $G = D_4$.

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

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

Definition

The index of $H \leq G$, written $[G : H]$, is the number of distinct left (or equivalently, right) cosets of H in G.

Lagrange's theorem

If H is a subgroup of finite group G, then $|G| = [G : H] \cdot |H|$. □

The tower law

Proposition

Let G be a finite group and $K \leq H \leq G$ be a chain of subgroups. Then

$$[G : K] = [G : H][H : K].$$

Here is a "proof by picture":

$[G : H] = \#$ of cosets of H in G

$[H : K] = \#$ of cosets of K in H

$[G : K] = \#$ of cosets of K in G

zH	z_1K	z_2K	z_3K	$\cdots$	z_nK
	$\vdots$	$\vdots$	$\vdots$	$\iddots$	$\vdots$
aH	a_1K	a_2K	a_3K	$\cdots$	a_nK
H	K	h_2K	h_3K	$\cdots$	h_nK

Proof

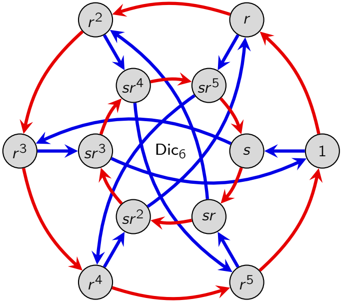
By Lagrange's theorem,

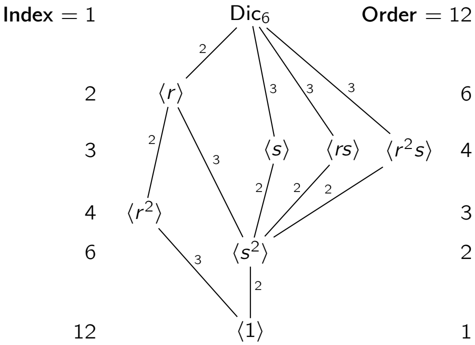
$$[G : H][H : K] = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = \frac{|G|}{|K|} = [G : K]. \qquad \square$$

The tower law

Another way to visualize the tower law involves subgroup lattices.

It is often helpful to label the edge from H to K in a subgroup lattice with the index $[H : K]$.





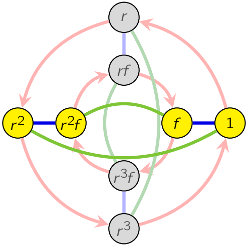
The tower law and subgroup lattices

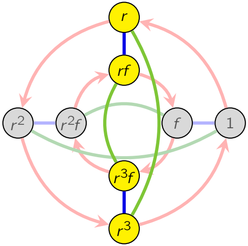
For any two subgroups $K \leq H$ of G, the index of K in H is just the *products of the edge labels* of any path from H to K.

Equality of sets vs. equality of elements

Caveat!

An equality of cosets $xH = Hx$ as sets *does not* imply an equality of elements $xh = hx$.





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

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

Proposition

If $[G : H] = 2$, then both left cosets of H are also right cosets.

The center of a group

Definition

The center of G is the set

$$Z(G) = \{z \in G \mid gz = zg, \ \forall g \in G\}.$$

If $z \in Z(G)$, we say that z is central in G.

Examples

Let's think about what elements commute with everything in the following groups:

- $Z(D_4) = \langle r^2 \rangle = \{1, r^2\}$
- $Z(D_3) = \{1\}$
- $Z(Q_8) = \langle -1 \rangle = \{1, -1\}$
- $Z(\mathbf{Frz}_1) = \langle v \rangle = \{1, v\}$
- $Z(S_4) = \{e\}$
- $Z(A_4) = \{e\}$

Clearly, if $H \leq Z(G)$, then $xH = Hx$ for all $x \in G$.

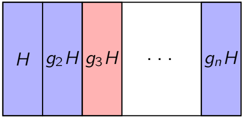
Proposition (exercise)

For any group G, the center $Z(G)$ is a subgroup.

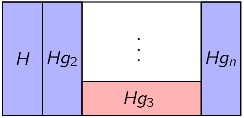
Normal subgroups and normalizers

Given a subgroup H of G, it is natural to ask the following question:

How many left cosets of H are right cosets?



Partition of G by the left cosets of H



Partition of G by the right cosets of H

Definition

A subgroup H is normal if $gH = Hg$ for *all* $g \in G$. We write $H \trianglelefteq G$.

The normalizer of H, denoted $N_G(H)$, is the set of elements $g \in G$ such that $gH = Hg$:

$$N_G(H) = \{g \in G \mid gH = Hg\},$$

i.e., the union of left cosets that are also right cosets.

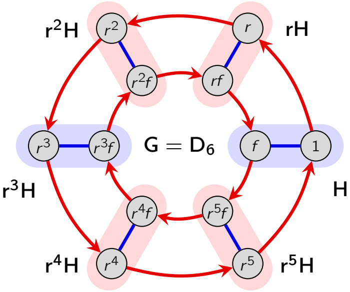
Proposition (exercise)

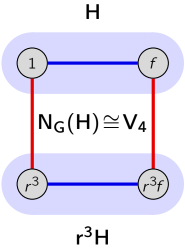
For any $H \leq G$,

$$H \trianglelefteq N_G(H) \leq G.$$

How to spot the normalizer in a Cayley graph

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





Remark

The normalizer of the subgroup $H = \langle f \rangle$ of D_n is

$$N_{D_n}(H) = \begin{cases} H \cup r^{n/2}H = \{1, f, r^{n/2}, r^{n/2}f\} & n \text{ even} \\ H = \{1, f\} & n \text{ odd.} \end{cases}$$

Conjugate subgroups

Definition

For a fixed $g \in G$, the (left) conjugate of H by g is

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

The set of all subgroups conjugate to H is its conjugacy class, denoted

$$\mathrm{cl}_G(H) = \{gHg^{-1} \mid g \in G\}.$$

Proposition (exercise)

1. gHg^{-1} is a subgroup of G;
2. conjugation is an equivalence relation on the set of subgroups of G.

Useful remark

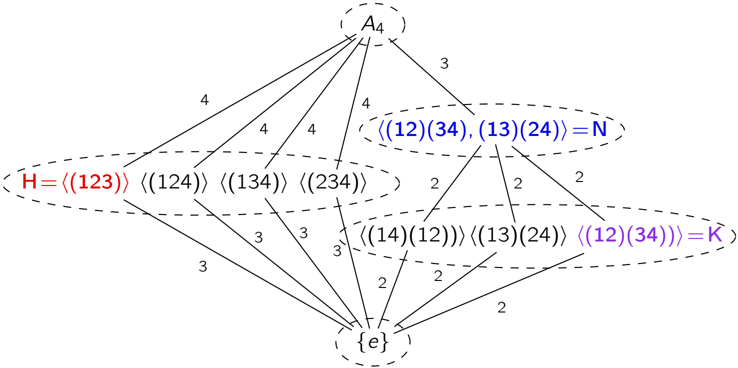
The following conditions are all equivalent to a subgroup $H \leq G$ being normal:

(i) $gH = Hg$ for all $g \in G$; ("left cosets are right cosets");

(ii) $gHg^{-1} = H$ for all $g \in G$; ("only one conjugate subgroup")

(iii) $ghg^{-1} \in H$ for all $g \in G$; ("closed under conjugation").

The alternating group A_4



Observations

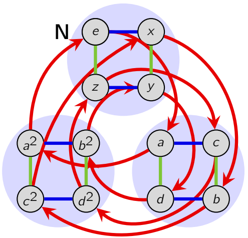
- A subgroup is normal if its conjugacy class has size 1.
- The size of a conjugacy class tells us *how close to being normal* a subgroup is.
- Remember these subgroups:

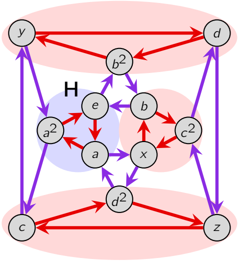
$$\left|\mathrm{cl}_{A_4}(N)\right| = 1 = \frac{1}{\mathrm{Deg}^{\lhd}_{A_4}(N)}, \quad \left|\mathrm{cl}_{A_4}(H)\right| = 4 = \frac{1}{\mathrm{Deg}^{\lhd}_{A_4}(H)}, \quad \left|\mathrm{cl}_{A_4}(K)\right| = 3 = \frac{1}{\mathrm{Deg}^{\lhd}_{A_4}(K)}.$$

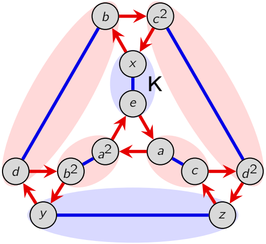
Three subgroups of A_4

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

$$\mathrm{Deg}_G^{\lhd}(H) := \frac{|N_G(H)|}{|G|} = \frac{1}{[G:N_G(H)]} = \frac{\#\text{ elements } x \in G \text{ for which } xH = Hx}{\#\text{ elements } x \in G}.$$

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

Big idea

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

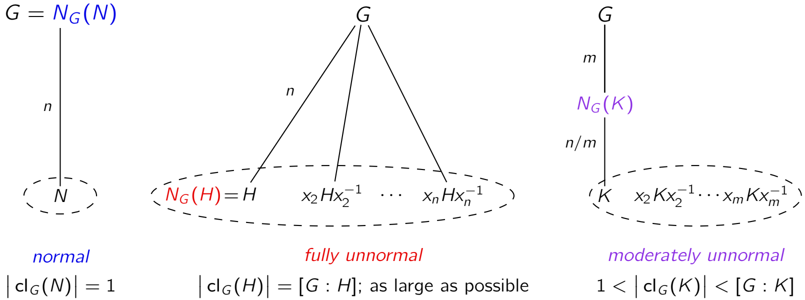
A special case of the orbit-stabilizer theorem

Theorem

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

$$\big|\operatorname{cl}_G(H)\big| = \frac{1}{\operatorname{Deg}_G^{\lhd}(H)} = [G : N_G(H)] = \frac{\#\text{ elements } x \in G \text{ for which } xH = Hx}{\#\text{ elements } x \in G}.$$

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

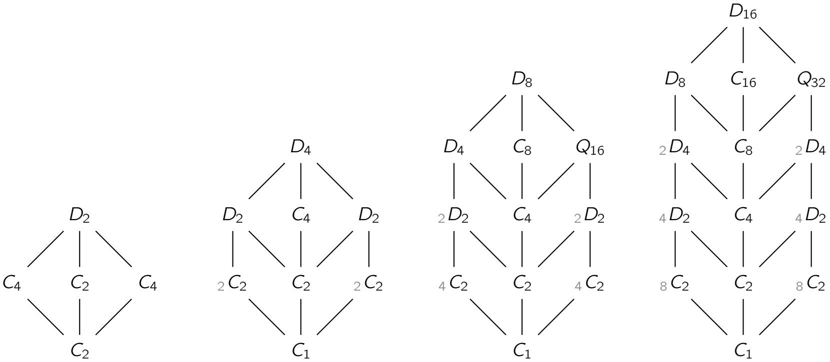


"Reducing" subgroup lattices

Sometimes it is convenient to collapse conjugacy classes into single nodes in the lattice.

We'll call this the reduced subgroups lattice (*caveat*: it need not be a lattice!). Sometimes it reveals patterns in new ways.

Here are the reduced lattices of the dihedral groups. (Note that $D_2 \cong V_4$.)



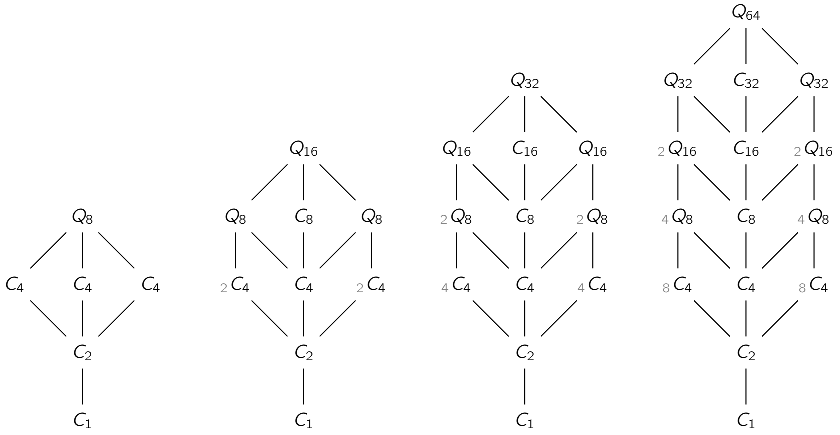
The left-subscript denotes the size.

"Reducing" subgroup lattices

Sometimes it is convenient to collapse conjugacy classes into single nodes in the lattice.

We'll call this the reduced subgroups lattice (*caveat*: it need not be a lattice!). Sometimes it reveals patterns in new ways.

Here are the reduced lattices of the generalized quaternion groups. What do you notice?



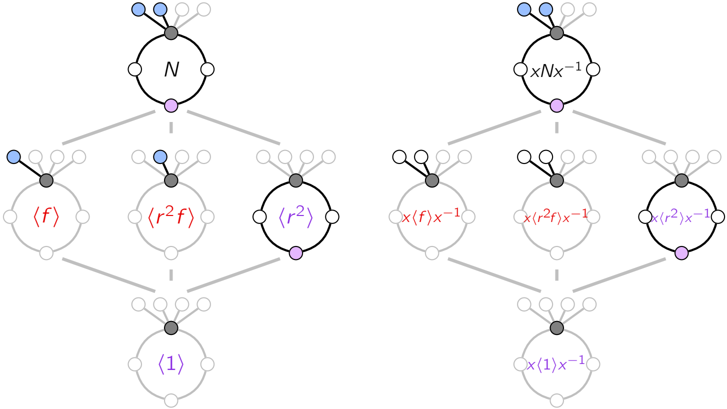
Conjugating normal subgroups

Proposition

If $H \leq N \trianglelefteq G$, then $xHx^{-1} \leq N$ for all $x \in G$.

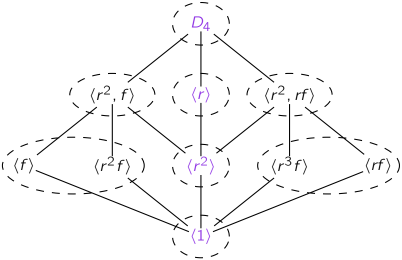
Proof

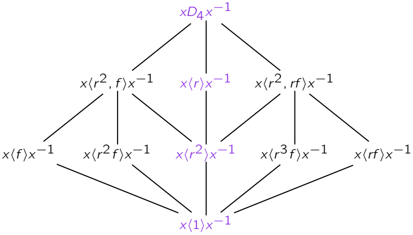
Conjugating $H \leq N$ by $x \in G$ yields $xHx^{-1} \leq xNx^{-1} = N$. $\square$



Determining the conjugacy classes by inspection

Suppose we conjugate $G = D_4$ by some element $x \in D_4$.





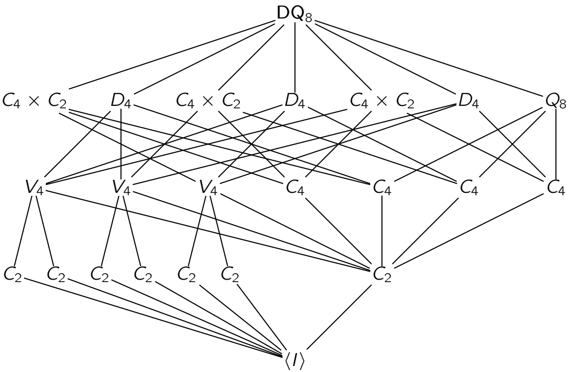
Remarks:

- Subgroups at a unique "lattice neighborhood," called **unicorns**, must be normal.
- all index-2 subgroups are normal.
- order-2 subgroups are normal iff they're central. (Why?)
- each nonnormal order-2 subgroup $\langle r^i f\rangle$ has a:
  - size-2 conjugacy class. (Why?)
  - index-2 normalizer, $N_{D_4}(\langle r^i f\rangle) = \langle r^i, f\rangle$.

Unicorns in the diquaternion group

Our definition of unicorn could be strengthened, but we want to keep things simple.

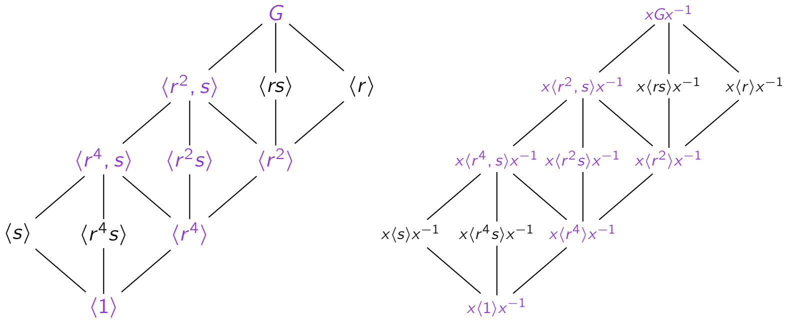
Are any of the C_4 subgroups of DQ_8 unicorns, i.e., "not like the others"?



What can we say about conjugacy classes of the subgroups of DQ_8 just from the lattice?

A mystery group of order 16

Let's repeat a previous exercise, for this lattice of an actual group. Unicorns are purple.



Every subgroup is normal, except possibly $\langle s\rangle$ and $\langle r^4 s\rangle$. (Why?)

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.

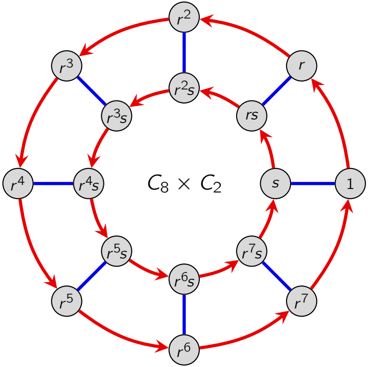
This doesn't necessarily mean that both of these are actually possible. . .

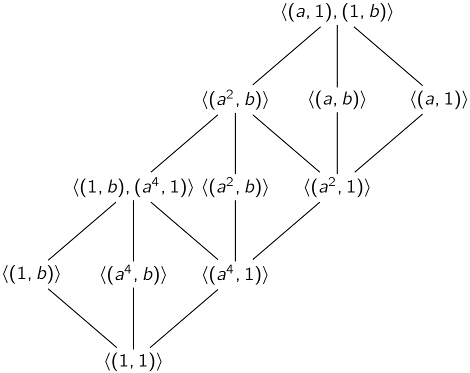
A mystery group of order 16

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

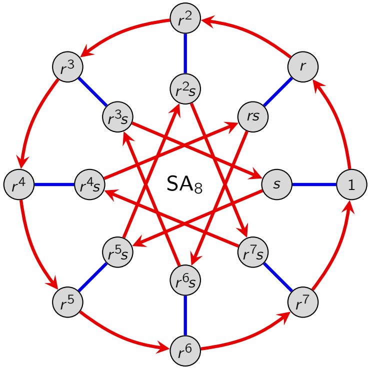


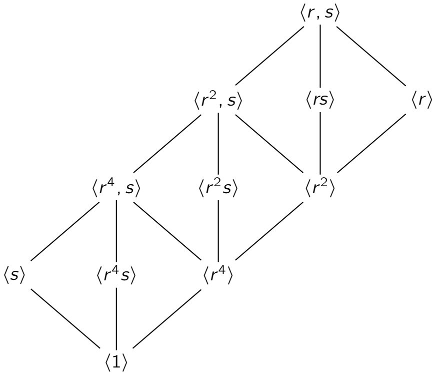


A mystery group of order 16

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

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

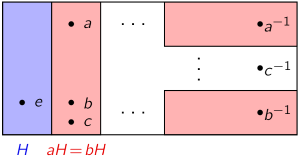


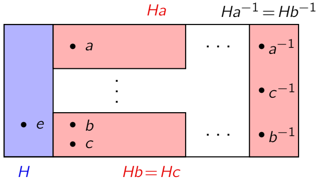


More on conjugate subgroups

Proposition (exercise)

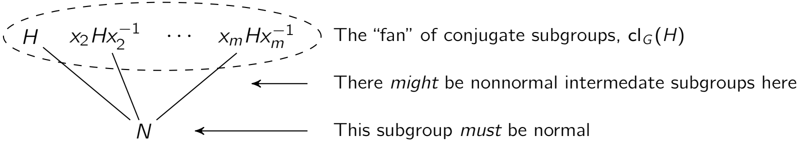
If $aH = bH$, then $Ha^{-1} = Hb^{-1}$, and hence $aHa^{-1} = bHb^{-1}$.



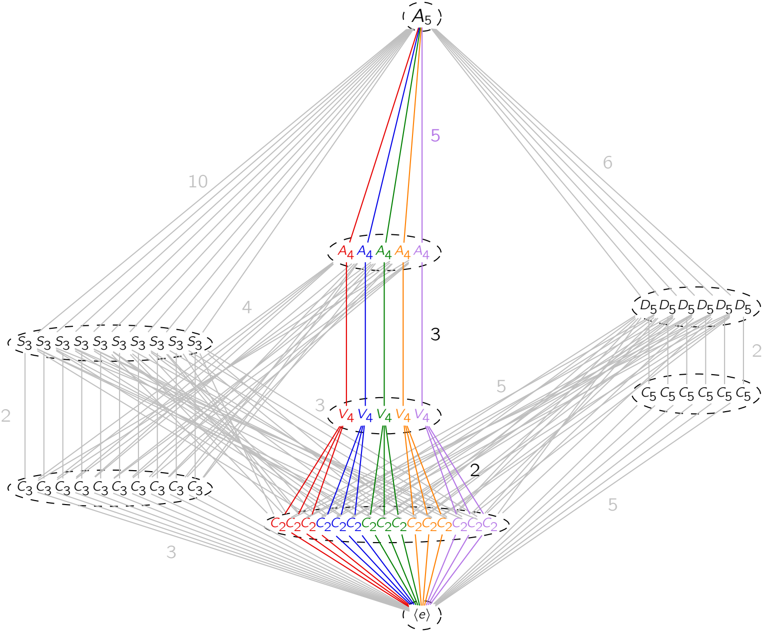


Proposition (HW)

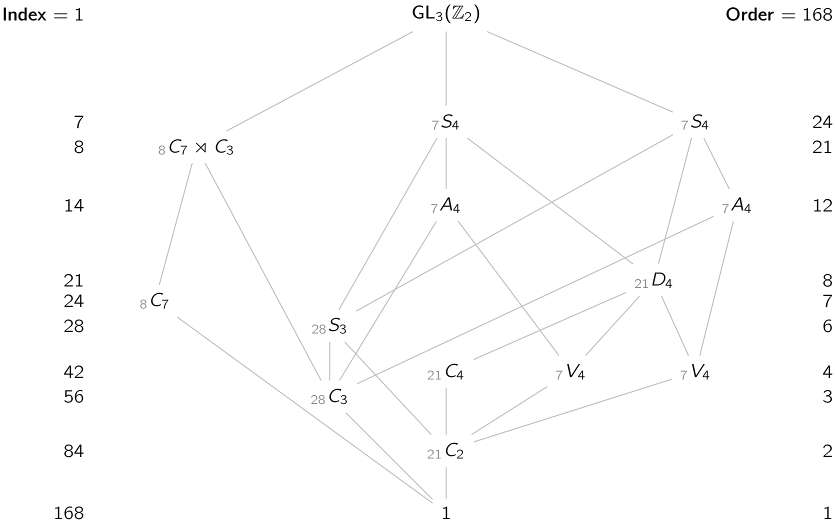
For any $H \leq G$, the intersection of all conjugates is normal: $N := \bigcap_{x \in G} xHx^{-1} \trianglelefteq G$.



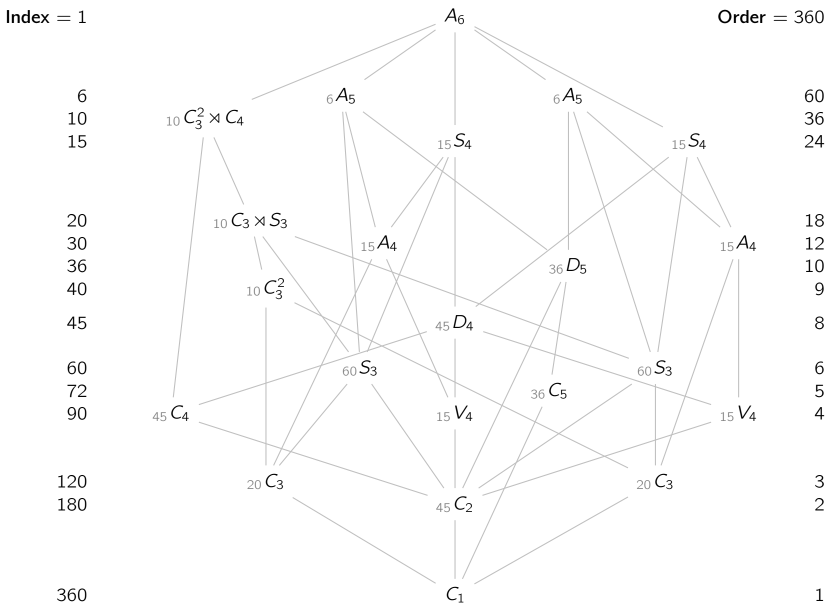
The subgroup lattice of the simple group A_5



The second smallest nonabelian simple group

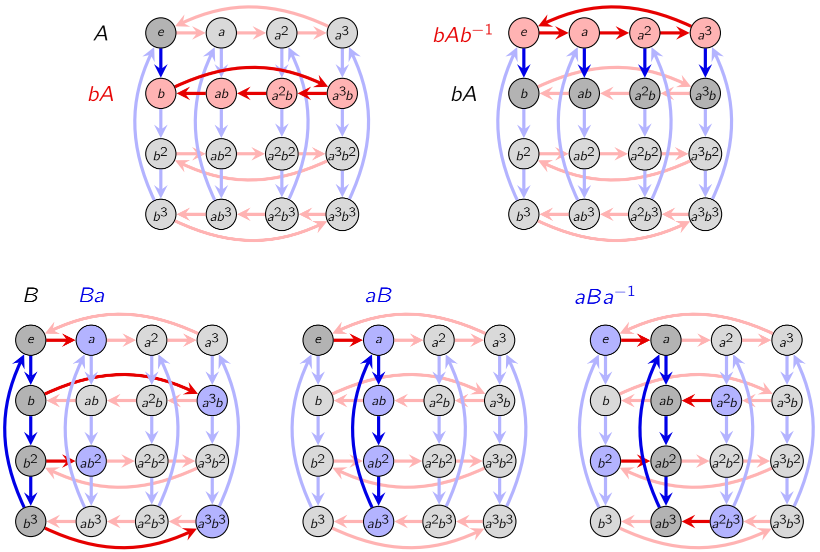


The third smallest nonabelian simple group



Conjugate subgroups, visually

Consider the subgroups $A = \langle a \rangle$ and $B = \langle b \rangle$ of $G = C_4 \rtimes C_4$.



Conjugate elements

Definition

The conjugacy class of an element $h \in G$ is the set

$$\mathrm{cl}_G(h) = \{xhx^{-1} \mid x \in G\}.$$

Proposition ("class equation")

For any finite group G,

$$|G| = |Z(G)| + \sum \left| \mathrm{cl}_G(h_i) \right|,$$

where the sum is taken over distinct conjugacy classes of size greater than 1.

Proof (sketch)

Immediate upon showing that:

- $|\,\mathrm{cl}_G(h)| = 1$ iff $h \in Z(G)$;
- conjugacy of elements is an equivalence relation.

Proposition (exercise)

Every normal subgroup is the union of conjugacy classes.

Conjugate elements

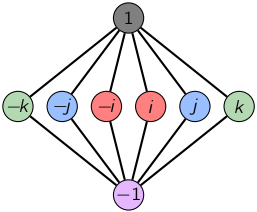
Often, we can determine the conjugacy classes by inspection.

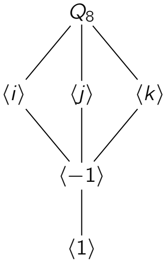
Let's look at Q_8, all of whose subgroups are normal.

- Since $i \notin Z(Q_8) = \{\pm 1\}$, we know $\big|\operatorname{cl}_{Q_8}(i)\big| > 1$.
- Also, $\langle i \rangle = \{\pm 1, \pm i\}$ is a union of conjugacy classes.
- Therefore $\operatorname{cl}_{Q_8}(i) = \{\pm i\}$.

Similarly, $\operatorname{cl}_{Q_8}(j) = \{\pm j\}$ and $\operatorname{cl}_{Q_8}(k) = \{\pm k\}$.

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

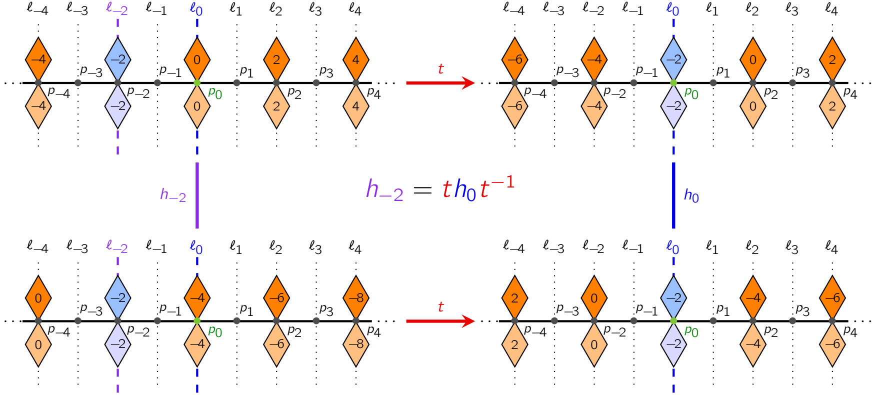




"Conjugation preserves structure"

Revisiting frieze groups, 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}.



It should be clear that all reflections (resp., rotations) of the "same parity" are conjugate.

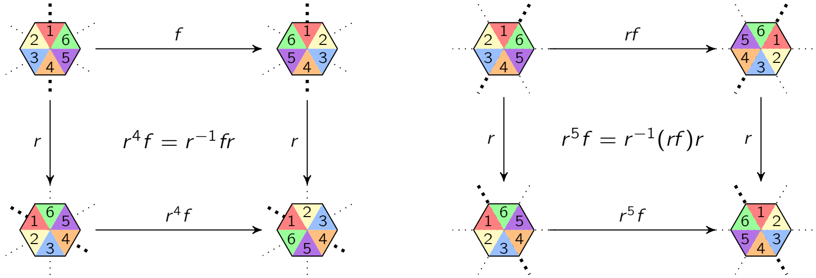
Conjugacy classes in D_n

The dihedral group D_n is a "finite version" of the previous frieze group.

When n is even, there are two "*types of reflections*" of an n-gon:

1. $r^{2k}f$ is across an axis that bisects two sides
2. $r^{2k+1}f$ is across an axis that goes through two corners.

Here is a visual reason why each of these two types form a conjugacy class in D_n.



What do you think the conjugacy classes of a reflection is in D_n when n is odd?

Centralizers

Definition

The centralizer of $h \subseteq G$ is the set of elements that commute with h

$$C_G(h) = \{x \in G \mid xh = hx\} \leq G.$$

Exercise: (i) $C_G(h)$ contains at least $\langle h \rangle$, (ii) if $xh = hx$, then $x\langle h \rangle \subseteq C_G(h)$.

Definition

Let $h \in G$ with $[G : \langle h \rangle] = n < \infty$. The **degree of centrality** of h is

$$\mathrm{Deg}^C_G(h) := \frac{|C_G(h)|}{|G|} = \frac{1}{[G : C_G(h)]} = \frac{\#\text{ elements } x \in G \text{ for which } xh = hx}{\#\text{ elements } x \in G}.$$

- If $\mathrm{Deg}^C_G(h) = 1$, then h is central.
- If $\mathrm{Deg}^C_G(h) = \frac{1}{n}$, we'll say h is fully uncentral.
- If $\frac{1}{n} < \mathrm{Deg}^C_G(h) < 1$, we'll say h is moderately uncentral.

Big idea

The degree of centrality measures *how close to being central* an element is.

The number of conjugate elements

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

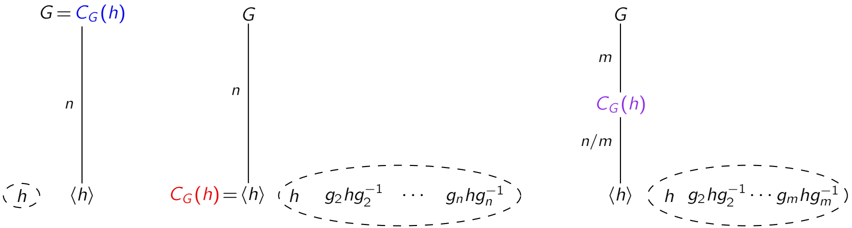
Theorem

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

$$\big|\mathrm{cl}_G(h)\big| = \frac{1}{\mathrm{Deg}_G^C(h)} = [G : C_G(h)] = \frac{\#\text{ elements } x \in G \text{ for which } xh = hx}{\#\text{ elements } x \in G}.$$

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

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



central

$\big|\mathrm{cl}_G(h)\big| = 1$

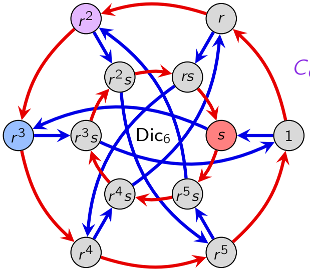
fully uncentral

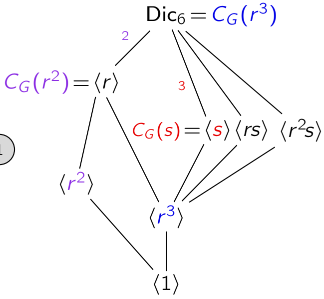
$\big|\mathrm{cl}_G(h)\big| = [G : \langle h \rangle]$; as large as possible

moderately uncentral

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

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^5	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^3s	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

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

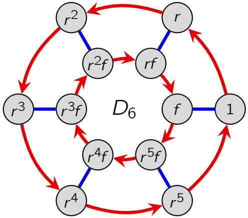
"fully unncentral"

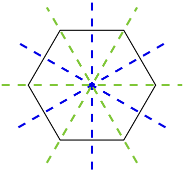
Conjugacy classes in D_6

Let's find the conjugacy classes of D_6 by inspection. The centralizers are:

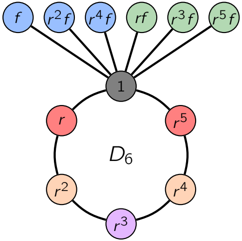
- $C_{D_6}(1) = C_{D_6}(r^3) = D_6$, (order 12; index 1)
- $C_{D_6}(r^i) = \langle r \rangle$, for $i = 2, 3, 4, 5$, (order 6; index 2)
- $C_{D_6}(r^i f) = \langle r^3, r^i f \rangle = \{1, r^3, r^i f, r^{3+i} f\}$, (order 4; index 3).

This is enough information to determine the conjugacy classes!



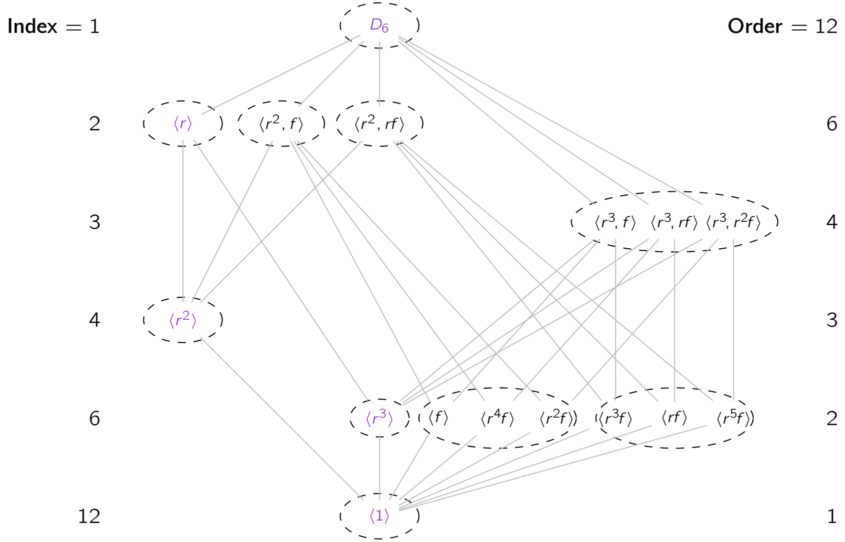


1	r	r^2	f	$r^2 f$	$r^4 f$
r^3	r^5	r^4	rf	$r^3 f$	$r^5 f$

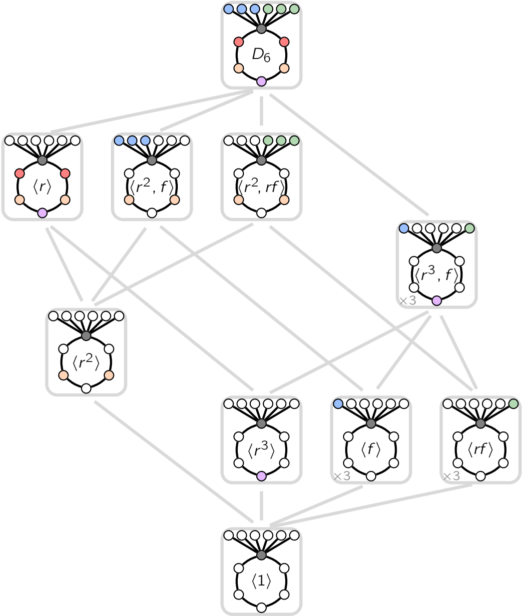


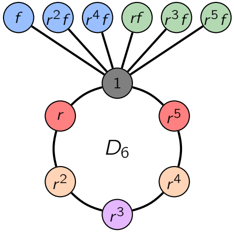
The subgroup lattice of D_6

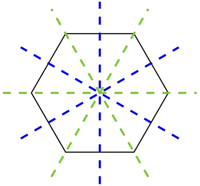
We can now deduce the conjugacy classes of the subgroups of D_6.



The reduced subgroup lattice of D_6

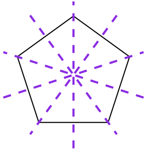






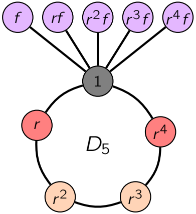
Conjugacy classes in D_5

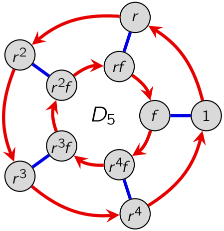
Since $n = 5$ is odd, all reflections in D_5 are conjugate.

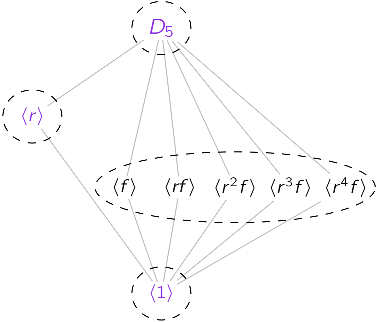


Centralizers

- $C_{D_5}(1) = D_5$ (index 1),
- $C_{D_5}(r^i) = \langle r \rangle$ (index 2),
- $C_{D_5}(r^i f) = \langle r^2 f \rangle$ (index 5).







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

Cycle type and conjugacy in the symmetric group

We introduced **cycle type** in back in Chapter 2.

This is best seen by example. There are five cycle types in S_4:

example element	e	(12)	(234)	(1234)	(12)(34)
parity	even	odd	even	odd	even
# elts	1	6	8	6	3

Definition

Two elements in S_n have the same cycle type if when written as a product of disjoint cycles, there are the same number of length-k cycles for each k.

Theorem

Two elements $g, h \in S_n$ are conjugate if and only if they have the same cycle type.

For example, permutations in S_5 fall into seven cycle types (conjugacy classes):

$$\text{cl}(e), \quad \text{cl}((12)), \quad \text{cl}((123)), \quad \text{cl}((1234)), \quad \text{cl}((12345)), \quad \text{cl}((12)(34)), \quad \text{cl}((12)(345)).$$

Big idea

Conjugate permutations have the same structure – they are *the same up to renumbering*.

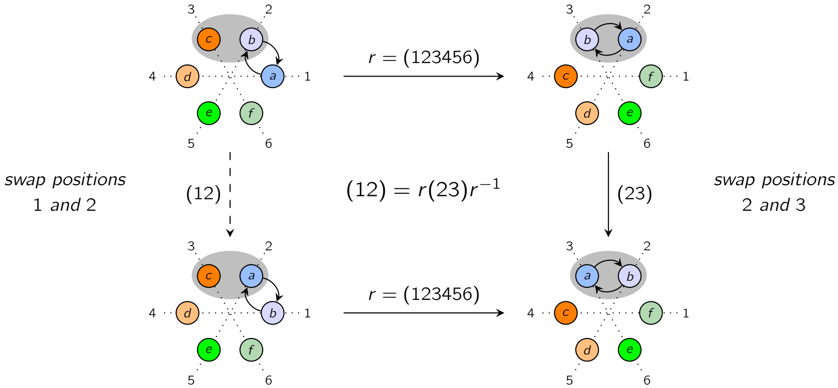
Conjugation preserves structure in the symmetric group

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*"

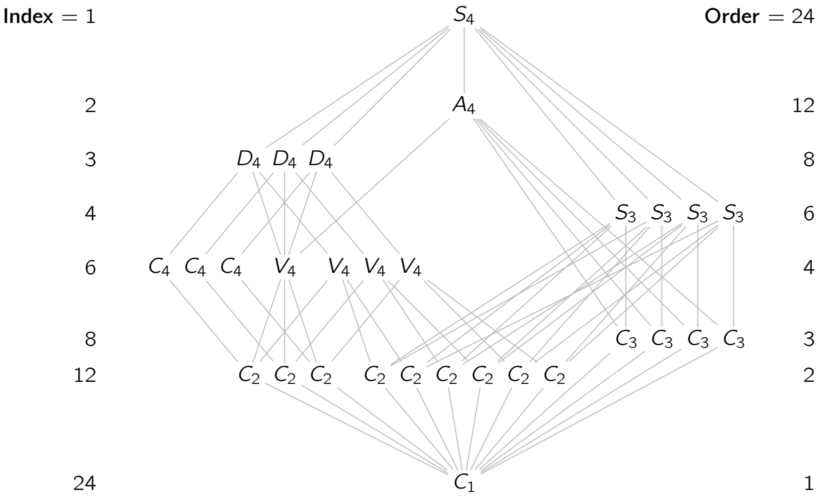
Here's how to get people in chairs 1 and 2 to swap seats:



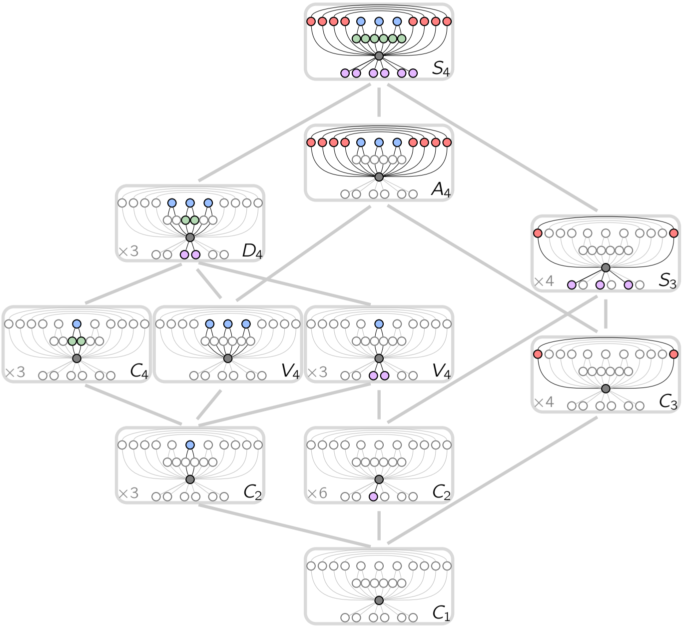
The subgroup lattice of S_4

Exercise

Partition the subgroup lattice of S_4 into conjugacy classes by inspection alone.



The reduced subgroup lattice of S_4



Conjugacy class size

Theorem (number of conjugate subgroups)

The conjugacy class of $H \leq G$ contains exactly $[G : N_G(H)]$ subgroups.

Proof (roadmap)

Construct a bijection between left cosets of $N_G(H)$ and conjugate subgroups of H:

"$xHx^{-1} = yHy^{-1}$ *iff x and y are in the same left coset of* $N_G(H)$."

Define $\phi\colon \{\text{left cosets of } N_G(H)\} \longrightarrow \{\text{conjugates of } H\}, \qquad \phi\colon xN_G(H) \longmapsto xHx^{-1}.$

Theorem (number of conjugate elements)

The conjugacy class of $h \in G$ contains exactly $[G : C_G(h)]$ elements.

Proof (roadmap)

Construct a bijection between left cosets of $C_G(h)$, and elements in $\mathrm{cl}_G(h)$:

"$xhx^{-1} = yhy^{-1}$ *iff* x and y are in the same left coset of $C_G(h)$."

Define $\phi\colon \{\text{left cosets of } C_G(h)\} \longrightarrow \{\text{conjugates of } h\}, \qquad \phi\colon xC_G(h) \longmapsto xhx^{-1}.$

Quotients

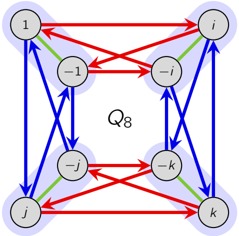
Denote the set of left cosets of H in G by

$$G/H := \{xH \mid x \in G\}.$$

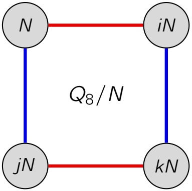
Key idea

The quotient of G by a subgroup H exists when the (left) cosets of H form a group.

This is well-defined precisely when H is normal.



Cluster the left cosets of N

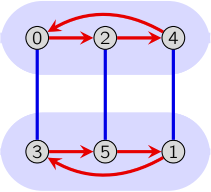


Collapse cosets into single nodes

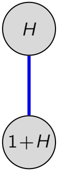
	N	iN	jN	kN
N	N	iN	jN	kN
iN	iN	N	kN	jN
jN	jN	kN	N	iN
kN	kN	jN	iN	N

Elements of the quotient are cosets of N

Quotients



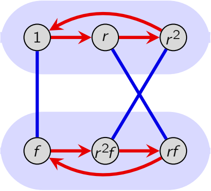
Cluster the
left cosets of $H \leq \mathbb{Z}_6$



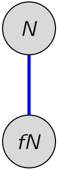
Collapse cosets
into single nodes

	H	$1+H$
H	H	$1+H$
$1+H$	$1+H$	H

Elements of the quotient
are cosets of H



Cluster the
left cosets of $N \leq D_3$



Collapse cosets
into single nodes

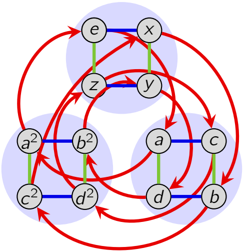
	N	fN
N	N	fN
fN	fN	N

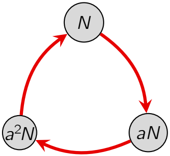
Elements of the quotient
are cosets of N

We say that $\mathbb{Z}_6/\langle 2\rangle \cong \mathbb{Z}_2$ and $D_3/\langle r\rangle \cong C_2$.

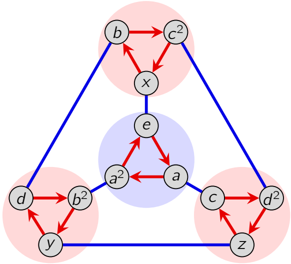
Quotients

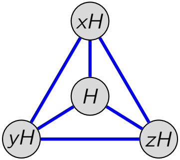
Let's revisit $N = \langle (12)(34), (13)(24) \rangle$ and $H = \langle (123) \rangle$ of A_4:





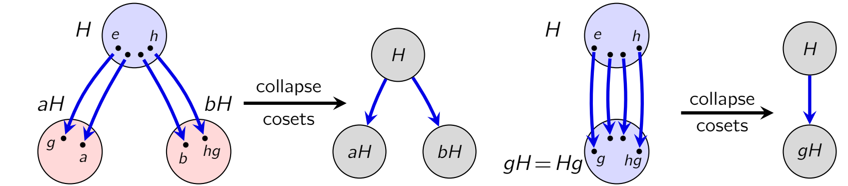
	N	aN	a^2N
N	N	aN	a^2N
aN	aN	a^2N	N
a^2N	a^2N	N	aN





When do the cosets of H form a group?

In the following: *the right coset Hg consists of the nodes at the "arrowtips"*.



Elements in the right coset Hg are in multiple left cosets — not a valid Cayley graph — Elements in Hg all stay in gH — valid Cayley graph

Key idea

If H is normal subgroup of G, then the quotient group G/H exists.

If H is not normal, then following the blue arrows from H is ambiguous.

In other words, it depends on our where we start within H.

What does it mean to "multiply" two cosets?

Proposition

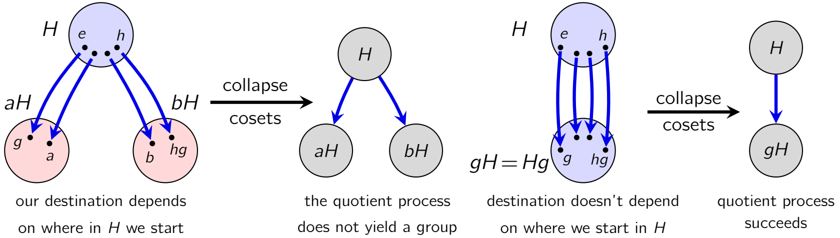
If $H \trianglelefteq G$, the set of left cosets G/H forms a group, with binary operation

$$aH \cdot bH := abH.$$

It's clear that G/H is closed under this operation, we just have to show that the operation is well-defined.

By that, we mean that it *does not depend on our choice of coset representative*:

$$\text{if } a_1H = a_2H \text{ and } b_1H = b_2H, \text{ then } a_1H \cdot b_1H = a_2H \cdot b_2H.$$



Quotient groups, algebraically

Lemma

When $H \trianglelefteq G$, the set of cosets G/H forms a group.

Proof

To show the binary operation is well-defined, suppose $a_1H = a_2H$ and $b_1H = b_2H$. Then

$$
\begin{aligned}
a_1H \cdot b_1H &= a_1b_1H && \text{(by definition)} \\
&= a_1(b_2H) && (b_1H = b_2H \text{ by assumption}) \\
&= (a_1H)b_2 && (b_2H = Hb_2 \text{ since } H \trianglelefteq G) \\
&= (a_2H)b_2 && (a_1H = a_2H \text{ by assumption}) \\
&= a_2b_2H && (b_2H = Hb_2 \text{ since } H \trianglelefteq G) \\
&= a_2H \cdot b_2H && \text{(by definition)}
\end{aligned}
$$

Thus, the binary operation on G/H is well-defined.

We'll leave checking the group axioms as an exercise. □