Chapter 3: Structure of groups

Matthew Macauley

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

Math 4120, Modern Algebra

Definitions and notation

Recall the definition of a subgroup.

Definition

A subgroup of G is a subset $H \subseteq G$ that is also a group. We denote this by $H \leq G$.

Writing $C_2 \leq D_3$ means *there is a copy of C_2 sitting inside of D_3 as a subgroup*.

We must be careful, because there might be multiple copies:

$$C_2 \cong \langle f \rangle = \{1, f\} \leq D_3, \qquad C_2 \cong \langle rf \rangle = \{1, rf\} \leq D_3.$$

Some books will write things like

$$\mathbb{Z}_3 \leq D_3 \qquad \text{and} \qquad C_3 \leq S_3,$$

but we will try to avoid this, because $\mathbb{Z}_3 \not\subseteq D_3$ and $C_3 \not\subseteq S_3$. Instead, we can write

$$\mathbb{Z}_3 \cong \langle r \rangle \leq D_3 \qquad \text{and} \qquad C_3 \cong \langle (123) \rangle \leq S_3.$$

Remark

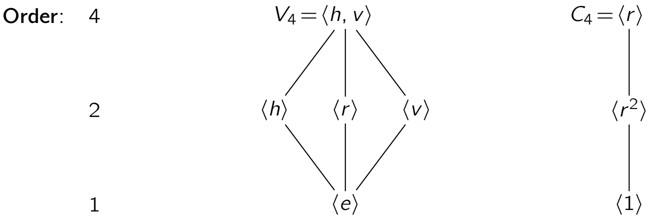
It is usually prefered to express a subgroup by its generator(s).

The two groups of order 4

Let's start by considering the subgroup of the two groups of order 4.

- Proper subgroups of V_4: $\langle h \rangle = \{e, h\}$, $\langle v \rangle = \{e, v\}$, $\langle r \rangle = \{e, r\}$, $\langle e \rangle = \{e\}$.
- Proper 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 these in a subgroup lattice:



The subgroup lattice of D_3

Let's construct the subgroup lattice of $G = D_3$.

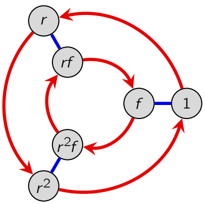
In any group G, every element $g \in D_3$ generates a cyclic subgroup, $\langle g \rangle \leq G$.

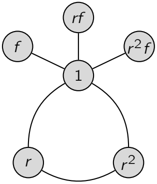
For small groups like D_3, these are the only proper subgroups.

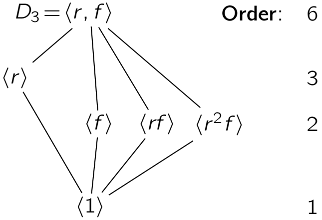
Here are the non-trivial proper subgroups of D_3:

$$\langle r \rangle = \{1, r, r^2\} = \langle r^2 \rangle, \quad \langle f \rangle = \{1, f\}, \quad \langle rf \rangle = \{1, rf\}, \quad \langle r^2 f \rangle = \{1, r^2 f\}, \quad \langle 1 \rangle = \{1\}.$$

Note that some subgroups are visually apparent in the Cayley diagram and/or cycle graph, whereas others aren't.







Intersections of subgroups

Proposition (HW)

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 (HW)

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*.

- Think of the LHS as the subgroup built "*from the bottom up*"
- Think of the RHS as the subgroup built "*from the top down*"

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

The defining property of lattices

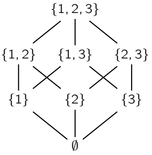
A lattice is a partially ordered set such that every pair of elements x, y has a unique:

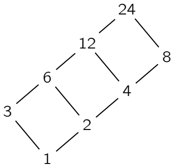
- supremum, or least upper bound, $x \vee y$
- infimum, or greatest lower bound, $x \wedge y$.

Examples that we're familiar with are subset lattices and divisor lattices.

$x \vee y = x \cup y$

$x \wedge y = x \cap y$



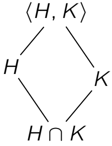


$x \vee y = \mathrm{lcm}(x, y)$

$x \wedge y = \gcd(x, y)$

The intersection $H \cap K$ of two subgroups is the largest subgroup contained in both of them.

Their union $H \cup K$ is not a subgroup (unless one contains the other). But it generates $\langle H, K \rangle$, the smallest subgroup containing both of them.



$H \vee K$: "*smallest subgroup above both H and K*"

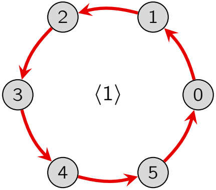
$H \wedge K$: "*largest subgroup below both H and K*"

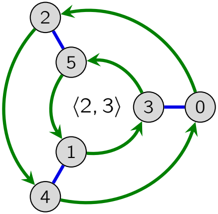
The subgroup lattice of $\mathbb{Z}_6$

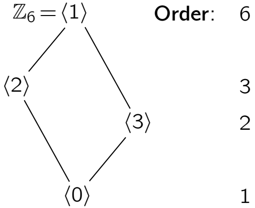
Consider the group $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Its subgroups are

$$\langle 0\rangle = \{0\}, \qquad \langle 1\rangle = \mathbb{Z}_6 = \langle 5\rangle, \qquad \langle 2\rangle = \{0,2,4\} = \langle 4\rangle, \qquad \langle 3\rangle = \{0,3\}.$$

Different choices of Cayley diagrams can highlight different subgroups.







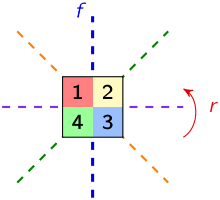
Tip

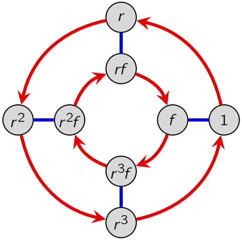
It will be *essential* to learn the subgroup lattices of our standard examples of groups.

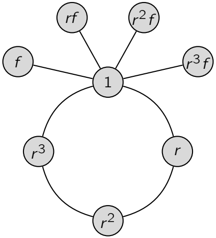
The subgroup lattice of D_4

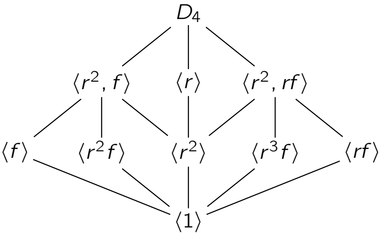
The subgroups of D_4 are:

- The entire group D_4, and the trivial group $\langle 1 \rangle$
- 4 subgroups generated by reflections: $\langle f \rangle$, $\langle rf \rangle$, $\langle r^2 f \rangle$, $\langle r^3 f \rangle$.
- 1 subgroup generated by a 180° rotation, $\langle r^2 \rangle \cong C_2$
- 1 subgroup generated by a 90° rotation, $\langle r \rangle \cong C_4$
- 2 subgroups isomorphic to V_4: $\langle r^2, f \rangle$, $\langle r^2, rf \rangle$.

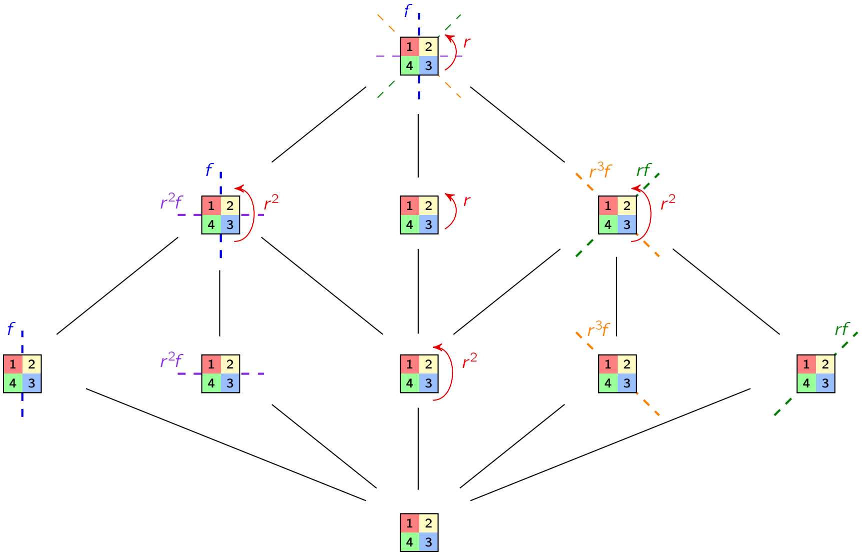








The subgroup lattice of D_4



The subgroup lattice of Q_8

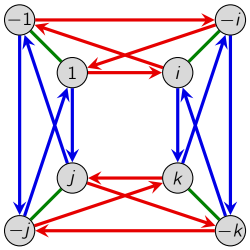
Let's determine all subgroups of the quaternion group

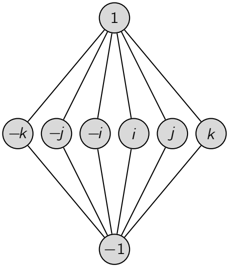
$$Q_8 = \left\langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \right\rangle.$$

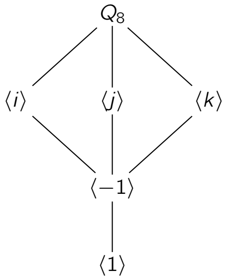
Every element generates a cyclic subgroup:

$$\langle 1 \rangle = \{1\}, \qquad \langle -1 \rangle = \{\pm 1\}, \qquad \langle i \rangle = \langle -i \rangle = \{\pm 1, \pm i\},$$

$$\langle j \rangle = \langle -j \rangle = \{\pm 1, \pm j\}, \qquad \langle k \rangle = \langle k \rangle = \{\pm 1, \pm k\}.$$







The subgroup lattice of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

We've seen the subgroup lattices of Two groups of order 8:

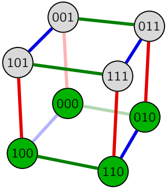
- D_4 has five elements of order 2, and 10 subgroups.
- Q_8 has one elemenet of order 2, and 6 subgroups.

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has seven *elements* of order 2.

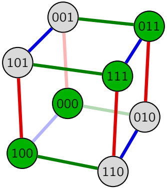
Rule of thumb

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

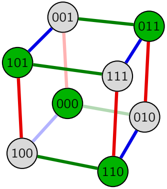
The following Cayley diagrams show three different subgroups of order 4 in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.



$\langle 100, 010 \rangle$



$\langle 100, 011 \rangle$



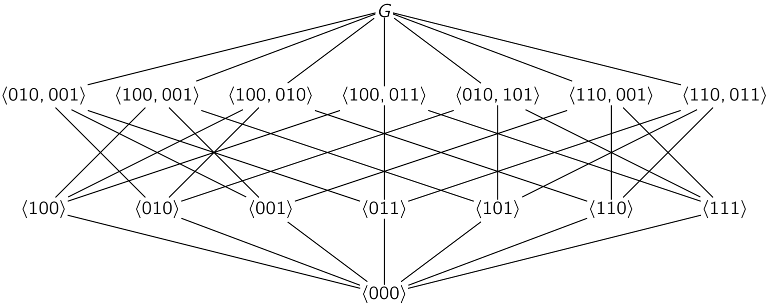
$\langle 110, 011 \rangle$

The subgroup lattice of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

All $\binom{7}{2} = 21$ pairs of non-identity element elements generate a subgroup isomorphic to V_4.

But this triple-counts all such subgroups. In summary, the subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ are:

- The subgroups G and $\{000\}$,
- 7 subgroups isomorphic to C_2,
- 7 subgroups isomorphic to V_4.



An observation

By now, we have seen enough examples to make a few observations about subgroups.

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

1. D_3 has subgroups of order 1, 2, 3, and 6.
2. C_6 has subgroups of order 1, 2, 3, and 6.
3. D_4 has subgroups of order 1, 2, 4, and 8.
4. Q_8 has subgroups of order 1, 2, 4, and 8.
5. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has subgroups of order 1, 2, 4, and 8.

Notice how in all five cases, the order of each subgroup divides $|G|$.

This is a fundamental property of subgroups, but we don't yet have the tools to prove it.

The missing piece is the concept of a coset, which we'll learn about soon.

A useful shortcut

Often, we'll need to verify that some $H \subseteq G$ is a subgroup. This requires checking

1. Identity: $e \in H$.
2. Inverses: If $h \in H$, then $h^{-1} \in H$.
3. Closure: If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.

There is a better way to check whether H is a subgroup.

One-step subgroup test

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

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

Proof

"$\Rightarrow$": Suppose $H \leq G$, and pick $h_1, h_2 \in H$. Then $h_2^{-1} \in H$, and by closure, $h_1 h_2^{-1} \in H$. ✓

"$\Leftarrow$": Suppose Eq. (1) holds, and take any $h \in H$.

- **Identity**: Take $x = y = h$. By Eq. (1), $xy^{-1} = hh^{-1} = e \in H$. ✓
- **Inverses**: Take $x = e$, $y = h$. By Eq. (1), $xy^{-1} = eh^{-1} = h^{-1} \in H$. ✓
- **Closure**: Take $x = h_1$ and $y = h_2^{-1}$. By Eq. (1),

$$xy^{-1} = h_1 (h_2^{-1})^{-1} = h_1 h_2 \in H. \quad ✓$$

Subgroups of cyclic groups

Proposition

Every subgroup of a cyclic group is cyclic.

Proof

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

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

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 $\ell > 0$.

Use the division algorithm to write $\ell = qk + r$, for some remainder where $0 \leq r < k$.

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

$$x^r = x^{\ell - qk} = x^\ell x^{qk} = x^\ell (x^k)^{-1} \in H.$$

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

Corollary

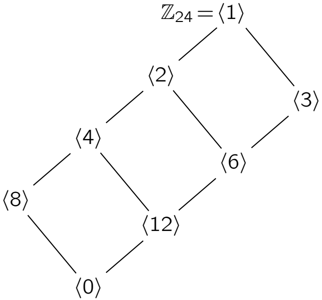
The subgroup of $G = \mathbb{Z}$ generated by $a_1, \ldots, a_k$ is $\langle \gcd(a_1, \ldots, a_k) \rangle \cong \mathbb{Z}$. $\square$

Subgroups of cyclic groups

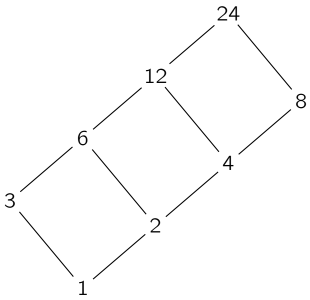
If d divides n, then $\langle d \rangle \leq \mathbb{Z}_n$ has order n/d. Moreover, all cyclic subgroups have this form.

Corollary

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



subgroup lattice

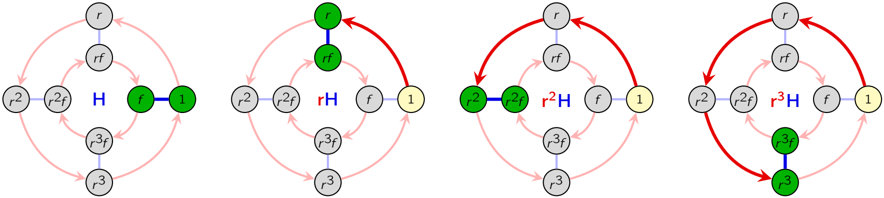


divisor lattice

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

The idea of cosets

By the regularity property of Cayley diagrams, identical copies of the fragment that corresponds to a subgroup appears throughout the diagram.



Of course, only one of these is actually a subgroup; the others don't contain the identity.

These are called left cosets of $H = \langle f \rangle$.

Informal definition

To find the left coset xH in a Cayley diagram, carry out the the following steps:

1. starting from the identity, follow a path to get to x
2. from x, follow all "H-paths".

Cosets, formally

Definition

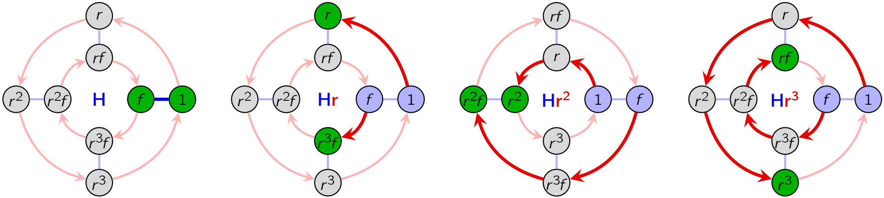
If $H \leq G$, then a left coset is a set

$$xH = \{xh \mid h \in H\},$$

for some fixed $x \in G$ called the representative. Similarly, we can define a right coset as

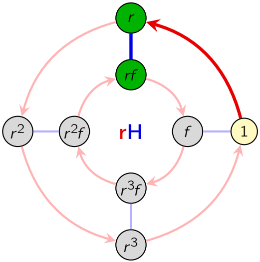
$$Hx = \{hx \mid h \in H\}.$$

Let's look at the right cosets of $H = \langle f \rangle$ in D_4.

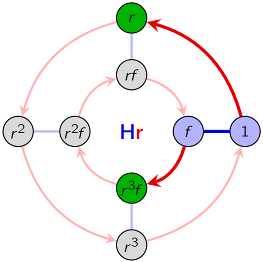


Left vs. right cosets

- 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.



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



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

Left cosets look like copies of the subgroup. Right cosets are usually scattered, because we adopted the convention that arrows in a Cayley diagram represent right multiplication.

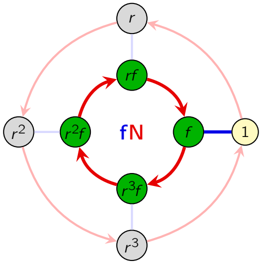
Key point

Left and right cosets are generally different.

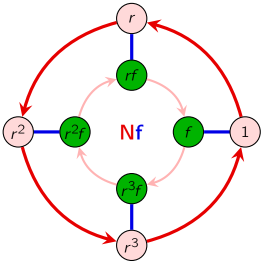
Left vs. right cosets

Let's look at the left and right cosets of a different subgroup, $N = \langle r \rangle$.

- The **left coset** fN in D_4: first go to f, then traverse all "N-paths".
- The **right coset** Nf in D_4: first traverse all N-paths, then traverse the f path.



$fN = f\{1, r, r^2, r^3\} = \{f, fr, fr^2, fr^3\}$



$Nf = \{1, r, r^2, r^3\}f = \{f, rf, r^2f, r^3f\}$

Remarks

- There are multiple representatives for the same coset:

$$fN = rfN = r^2fN = r^3fN, \qquad Nf = Nrf = Nr^2f = Nr^3f.$$

- For this subgroup, each left coset is a right coset. Such a subgroup is called normal.

Basic properties of cosets

The following results should be "visually clear" from the Cayley diagrams and regularity.

Proposition

Each (left) coset can have multiple representatives: if $b \in aH$, then $aH = bH$.

Proof

Since $b \in aH$, we can write $b = ah$, for some $h \in H$. That is, $h = a^{-1}b$ and $a = bh^{-1}$.

To show that $aH = bH$, we need to verify both $aH \subseteq bH$ and $aH \supseteq bH$.

"$\subseteq$": Take $ah_1 \in aH$. We need to write it as bh_2, for some $h_2 \in H$. By substitution,

$$ah_1 = (bh^{-1})h_1 = b(h^{-1}h_1) \in bH.$$

"$\supseteq$": Pick $bh_3 \in bH$. We need to write it as ah_4 for some $h_4 \in H$. By substitution,

$$bh_3 = (ah)h_3 = a(hh_3) \in aH.$$

Therefore, $aH = bH$, as claimed. $\square$

Corollary (boring but useful)

The equality $xH = H$ holds if and only if $x \in H$. (And analogously, for $Hx = H$.)

Basic properties of cosets

Proposition

For any subgroup $H \leq G$, the (left) cosets of H partition the group G.

Proof

We know that the element $g \in G$ lies in a (left) coset of H, namely gH. Uniqueness follows because if $g \in kH$, then $gH = kH$. □

Proposition

All (left) cosets of $H \leq G$ have the same size. □

Proof

It suffices to show that $|xH| = |H|$, for any $x \in H$.

Define a map

$$\varphi \colon H \longrightarrow xH, \qquad h \longmapsto xh.$$

It is elementary to show that this is a bijection. □

Lagrange's theorem

Remark

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

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

Let's compare these two partitions for the subgroup $H = \langle f \rangle$ of $G = D_4$.

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

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

Definition

The index of a subgroup H of 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 $|G| = [G : H] \cdot |H|$. $\square$

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	$z_1 K$	$z_2 K$	$z_3 K$	$\cdots$	$z_n K$
	$\vdots$	$\vdots$	$\vdots$	$\iddots$	$\vdots$
aH	$a_1 K$	$a_2 K$	$a_3 K$	$\cdots$	$a_n K$
H	K	$h_2 K$	$h_3 K$	$\cdots$	$h_n K$

Proof

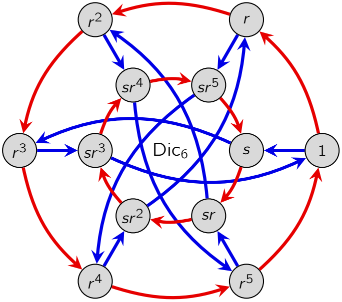
By Lagrange's theorem,

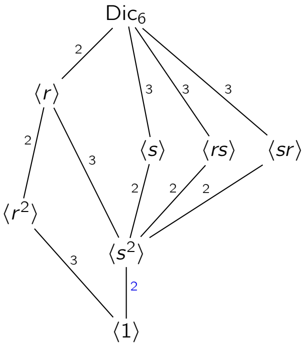
$$[G : H][H : K] = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = \frac{|G|}{|K|} = [G : K]. \qquad \square$$

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.

Cosets in additive groups

In any abelian group, left cosets and right cosets coincide, because

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

In abelian groups written additively, like $\mathbb{Z}_n$ and $\mathbb{Z}$, left cosets are written not as aH, but

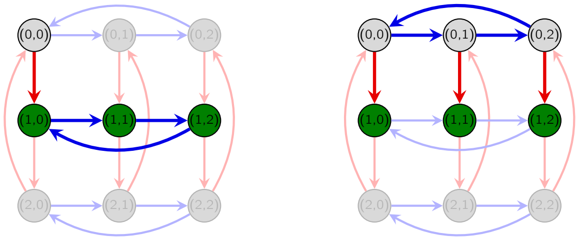
$$a + H = \{a + h \mid h \in H\}.$$

For example, let $G = \mathbb{Z}$. The cosets of the subgroup $H = 4\mathbb{Z} = \{4k \mid k \in \mathbb{Z}\}$ are

$$\begin{aligned} H &= \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\} = H \\ 1 + H &= \{\dots, -11, -7, -3, 1, 5, 9, 13, \dots\} = H + 1 \\ 2 + H &= \{\dots, -10, -6, -2, 2, 6, 10, 14, \dots\} = H + 2 \\ 3 + H &= \{\dots, -9, -5, -1, 3, 7, 11, 15, \dots\} = H + 3. \end{aligned}$$

Note that $3H$ would be interpreted to mean the subgroup $3(4\mathbb{Z}) = 12\mathbb{Z}$.

$(1,0) + \langle (0,1) \rangle$

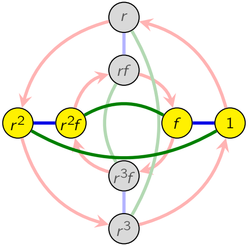


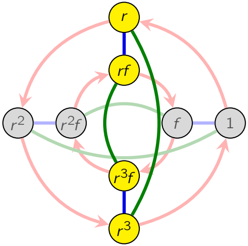
$\langle (0,1) \rangle + (1,0)$

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

Even though $xH = Hx$ does not imply $xh = hx$ for all $h \in H$, the converse holds.

Even in a nonabelian group, there may be elements that commute with everything.

Definition

The center of G is the set

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

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:

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

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

The center of a group

Proposition

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

Proof

- **Identity**: $eg = ge$ for all $g \in G$. ✓
- **Inverses**: Take $z \in Z(G)$. For any $g \in G$, we know that $zg = gz$.

  Multipy this on the left and right by z^{-1}:

  $$gz^{-1} = z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1} = z^{-1}g.$$

  Therefore, $z^{-1} \in Z(G)$. ✓
- **Closure**: Suppose $z_1, z_2 \in Z(G)$. Then for any $g \in G$,

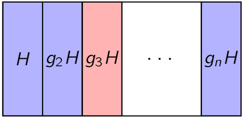
  $$(z_1 z_2)g = z_1(z_2 g) = z_1(g z_2) = (z_1 g)z_2 = (g z_1)z_2 = g(z_1 z_2).$$

  Therefore, $z_1 z_2 \in Z(G)$. ✓

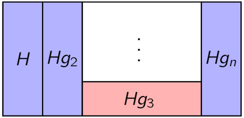
Normal subgroups and normalizers

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

- "Best case" scenario: all of them
- "Worst case" scenario: only H
- In general: somewhere between these two extremes

Definition

A subgroup H is a normal subgroup of G 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.

Examples of normal sugroups

We've seen cases where we know a subgroup will be normal without having to check.

1. The subgroup $H = G$ is always normal. The only left coset is also the only right coset:
$$eG = G = Ge.$$
2. The subgroup $H = \{e\}$ is always normal. The left and right cosets are singletons sets:
$$gH = \{g\} = Hg.$$
3. Subgroups H of index 2 are normal. The two cosets (left or right) are H and $G \setminus H$.
4. Subgroups of *abelian groups* are always normal, because for any $H \leq G$,
$$aH = \big\{ah \mid h \in H\big\} = \big\{ha \mid h \in H\big\} = Ha.$$
5. Subgroups $H \leq Z(G)$ are always normal, for the same reason as above.

Normalizers are subgroups

Theorem

For any $H \leq G$, we have $N_G(H) \leq G$.

Proof

- **Identity**: $eH = He$. ✓
- **Inverses**: Suppose $gH = Hg$. Multiply on the left and right by g^{-1}:
$$Hg^{-1} = g^{-1}(gH)g^{-1} = g^{-1}(Hg)g^{-1} = g^{-1}H. \quad ✓$$
- **Closure**: Suppose $g_1 H = Hg_1$ and $g_2 H = Hg_2$. Then
$$(g_1 g_2)H = g_1(g_2 H) = g_1(Hg_2) = (g_1 H)g_2 = (Hg_1)g_2 = H(g_1 g_2). \quad ✓$$

Corollary

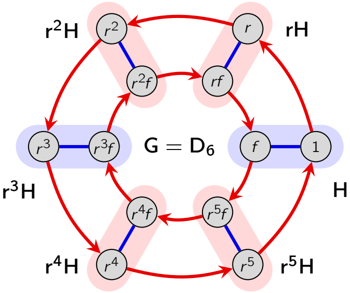
Every subgroup is normal in its normalizer:
$$H \trianglelefteq N_G(H) \leq G.$$

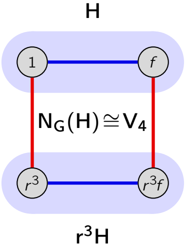
Proof

By definition, $gH = Hg$ for all $g \in N_G(H)$. Therefore, $H \trianglelefteq N_G(H)$. $\square$

How to spot the normalizer in a Cayley diagram

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.





We can get from H to rH multiple ways: via r or r^5.

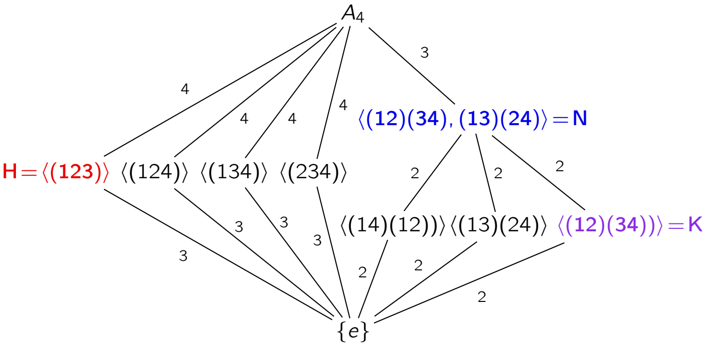
The *only* way to get from H to r^3H is via the path r^3.

Remark

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

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

The subgroup lattice of A_4



Going forward, we will consider the following three subgroups of A_4:

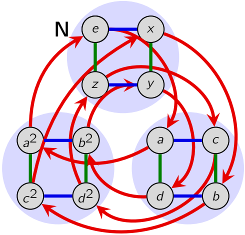
$$\begin{aligned} N &= \big\langle (12)(34), (13)(24) \big\rangle = \big\{e,\ (12)(34),\ (13)(24),\ (14)(23)\big\} \\ H &= \big\langle (123) \big\rangle = \big\{e,\ (123),\ (132)\big\} \\ K &= \big\langle (12)(34) \big\rangle = \big\{e,\ (12)(34)\big\}. \end{aligned}$$

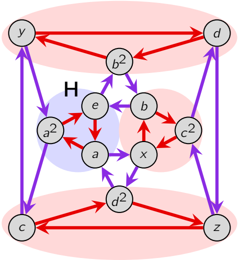
For each one, its normalizer lies between it and A_4 (inclusive) on the subgroup lattice.

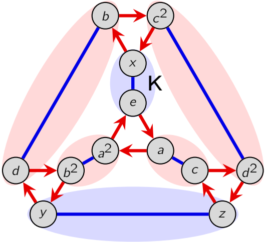
Three subgroups of A_4

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.

Conjugate subgroups

For a fixed element $g \in G$, the set

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

is called the conjugate of H by g.

Observation 1

For any $g \in G$, the conjugate gHg^{-1} is a subgroup of G.

Proof

1. **Identity**: $e = geg^{-1}$. ✓
2. **Closure**: $(gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1}$. ✓
3. **Inverses**: $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. ✓

Observation 2

$gh_1g^{-1} = gh_2g^{-1}$ if and only if $h_1 = h_2$. $\square$

Later, we'll prove that H and gHg^{-1} are isomorphic subgroups.

How to check if a subgroup is normal

If $gH = Hg$, then right-multiplying both sides by g^{-1} yields $gHg^{-1} = H$.

This gives us a new way to check whether a subgroup H is normal in 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").

Sometimes, one of these methods is *much* easier than the others!

For example, all it takes to show that H is not normal is finding *one element* $h \in H$ for which $ghg^{-1} \notin H$ for some $g \in G$.

As another example, if we happen to know that G has a unique subgroup of size $|H|$, then H *must* be normal. (Why?)

The conjugacy class of a subgroup

Proposition

Conjugation is an equivalence relation on the set of subgroups of G.

Proof

We need to show that conjugacy is reflexive, symmetric, and transitive.

- **Reflexive**: $eHe^{-1} = H$. ✓
- **Symmetric**: Suppose H is conjugate to K, by $aHa^{-1} = K$. Then K is conjugate to H:

$$a^{-1}Ka = a^{-1}(aHa^{-1})a = H. \quad \checkmark$$

- **Transitive**: Suppose $aHa^{-1} = K$ and $bKb^{-1} = L$. Then H is conjugate to L:

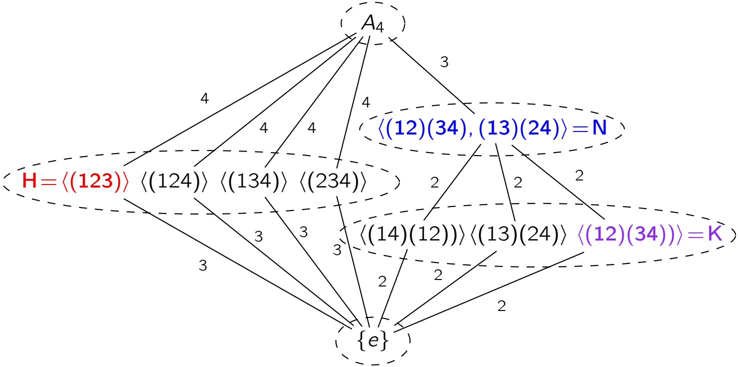
$$(ba)H(ba)^{-1} = b(aHa^{-1})b^{-1} = bKb^{-1} = L. \quad \checkmark$$

Definition

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

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

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

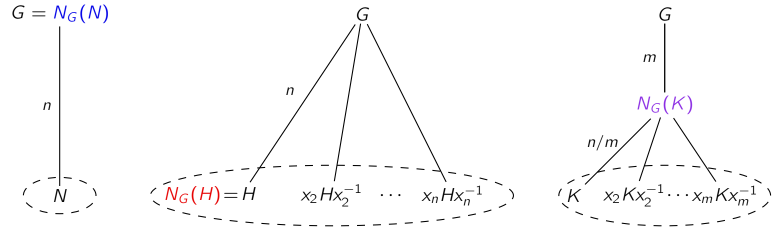
Though we do not yet have the tools to prove such a result, we will state it here.

Theorem

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

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

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



normal — $\big|\operatorname{cl}_G(N)\big| = 1$

fully unnormal — $\big|\operatorname{cl}_G(H)\big| = [G : H]$; as large as possible

moderately unnormal — $1 < \big|\operatorname{cl}_G(K)\big| < [G : K]$

Normal subgroups of order 2

Often, we can determine the normal subgroups and conjugacy classes simply from inspecting the subgroup lattice.

We'll make frequent use of the following straightforward result.

Lemma

An subgroup H of order 2 is normal if and only if it is contained in $Z(G)$.

Proof

Let $H = \{e, h\}$.

"$\Rightarrow$": Suppose $H \trianglelefteq G$. Then for all $x \in G$,

$$xH = x\{e, h\} = \{x, xh\}, \quad \text{and} \quad Hx = \{e, h\}x = \{x, hx\}.$$

Since $xH = Hx$, we must have $xh = hx$, and hence $H \leq Z(G)$. ✓

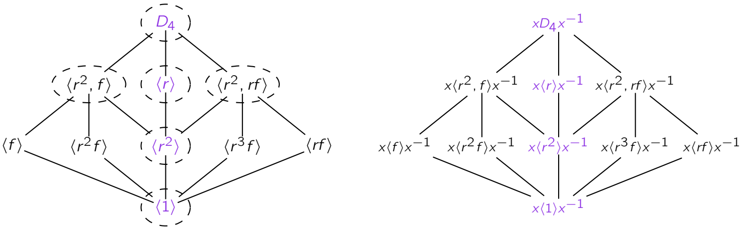
"$\Leftarrow$": Suppose $H \leq Z(G)$. Then for all $x \in G$,

$$xH = x\{e, h\} = \{x, xh\} = \{x, hx\} = \{e, h\}x = Hx.$$

Therefore, $H \trianglelefteq G$. ✓

Determining the conjugacy classes from the subgroup lattice

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



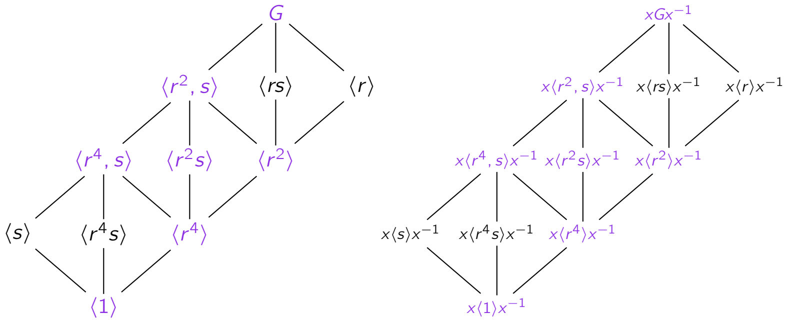
Subgroups at a unique "lattice neighborhood" are called unicorns, and must be normal.

Conclusions

- G and $\langle 1\rangle$ are always normal.
- The index-2 subgroups $\langle r^2, f\rangle$, $\langle r\rangle$, and $\langle r^2, rf\rangle$ must be normal.
- $\langle r^2\rangle = x\langle r^2\rangle x^{-1}$ is a unicorn (it's the only size-2 subgroup contained in three order-4 subgroups), and thus must be normal.
- $\langle f\rangle$ cannot be normal because $f \notin Z(D_4)$. Also, each conjugate subgroup must be contained in $\langle r^2, f\rangle$. Therefore, $\mathrm{cl}_{D_4}(\langle f\rangle)$ must have size 2, and likewise for $\mathrm{cl}_{D_4}(\langle rf\rangle)$.
- *We just determined all conjugacy classes simply from the subgroup lattice!*

A mystery group of order 16

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



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.

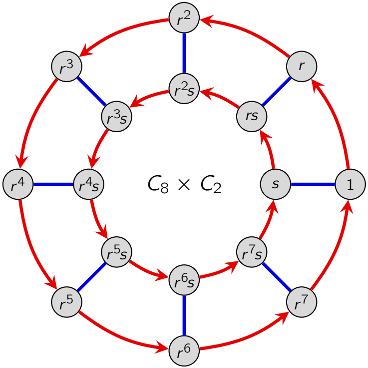
This doesn't necessarily mean that both of these are actually possible...

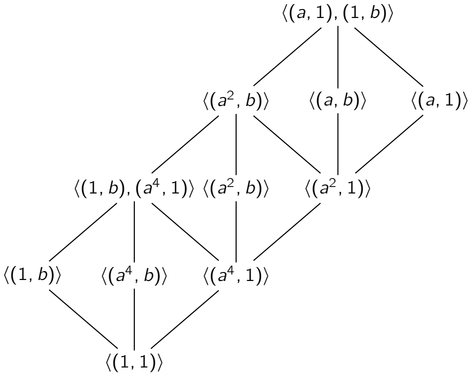
A mystery group of order 16

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

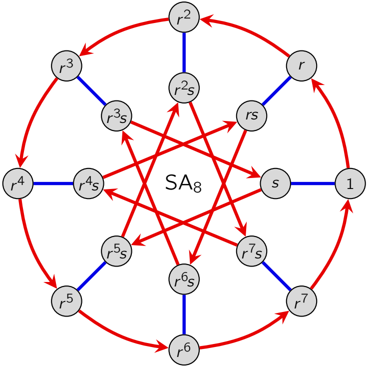


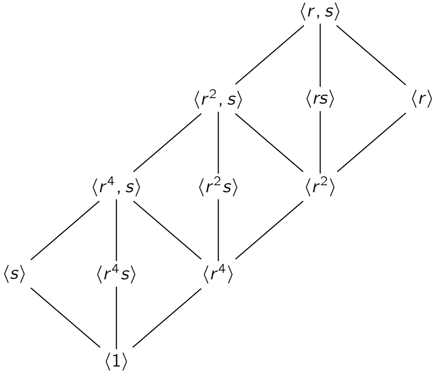


A mystery group of order 16

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

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





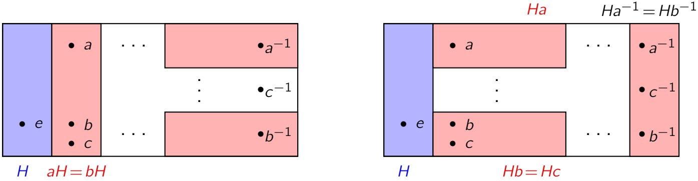
Conjugate subgroups, algebraically

We understand how to compare gH and Hg both algebraically and in a Cayley diagram.

But to understand H vs. gHg^{-1}, we need to compare gH to Hg^{-1}.

Proposition

If $aH = bH$, then $Ha^{-1} = Hb^{-1}$.



Proof

Using $x \in H \Leftrightarrow xH = H = Hx$, we deduce that

$$aH = bH \quad \Leftrightarrow \quad b^{-1}aH = H \quad \Leftrightarrow \quad H = Hb^{-1}a \quad \Leftrightarrow \quad Ha^{-1} = Hb^{-1}. \qquad \square$$

(Note that we're taking $x = b^{-1}a$ above.) $\square$

Conjugate subgroups, algebraically

We just showed that $aH = bH$ implies $Ha^{-1} = Hb^{-1}$.

Corollary

If $aH = bH$, then $aHa^{-1} = bHb^{-1}$.

Proof

Since $aH = bH$ we know that $Ha^{-1} = Hb^{-1}$, and so

$$aHa^{-1} = (aH)a^{-1} = (bH)a^{-1} = b(Ha^{-1}) = bHb^{-1}. \qquad \square$$

Corollary

For any subgroup $H \leq G$ of finite index, there are at most $[G : H]$ conjugates of H. $\square$

In summary, we have

$$\left|\operatorname{cl}_G(H)\right| = [G : N_G(H)] \leq [G : H].$$

We proved the inequality, but the inequality remains unproven. (We'll need group actions.)

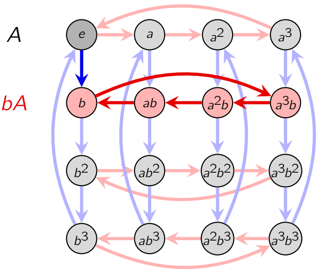
Conjugate subgroups, visually

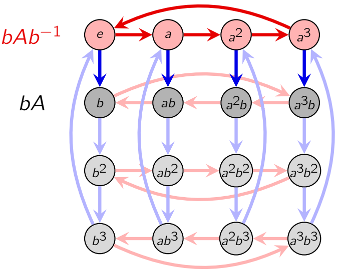
Remark

To identify the conjugate subgroup gHg^{-1} in the Cayley diagram, do the following:

1. Identify the left coset gH,
2. From each node in gH, traverse the g^{-1}-path.

Here is an example of this for the normal subgroup $A = \langle a \rangle$ of $G = C_4 \rtimes C_4$.





Let's check that $b^2Ab^{-2} = A$ and $b^3Ab^{-3} = A$, which means that $A \trianglelefteq G$.

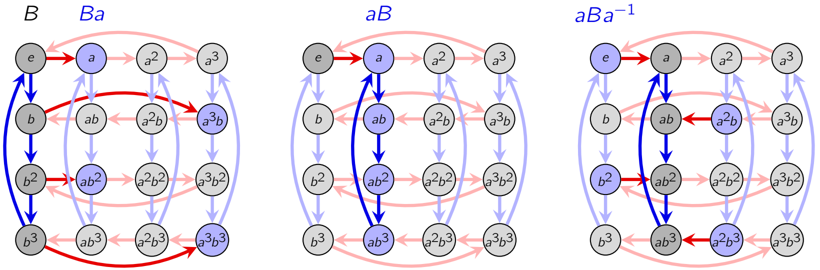
Conjugate subgroups, visually

Remark

To identify the conjugate subgroup gHg^{-1} in the Cayley diagram, do the following:

1. Identify the left coset gH,
2. From each node in gH, traverse the g^{-1}-path.

Let's carry out the same steps with the nonnormal subgroup $A = \langle B \rangle$ of $G = C_4 \rtimes C_4$.



It follows immediately that B is not normal. Let's find all conjuguate subgroups...

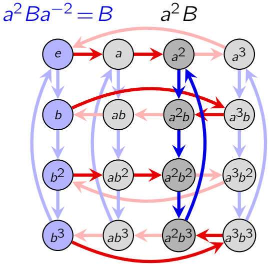
Conjugate subgroups, visually

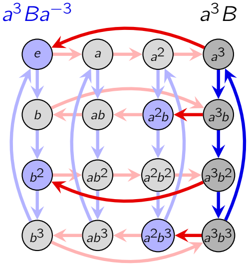
Remark

To identify the conjugate subgroup gHg^{-1} in the Cayley diagram, do the following:

1. Identify the left coset gH,
2. From each node in gH, traverse the g^{-1}-path.

Let's carry out the same steps with the nonnormal subgroup $A = \langle B \rangle$ of $G = C_4 \rtimes C_4$.





We conclude that $\mathrm{cl}_G(B) = \{B, aBa^{-1}\}$.

It follows that $[G : N_G(B)] = 2$, i.e., $|N_G(B)| = 8$. By inspection, $N_G(B) = B \cup a^2B$.

The product of two subgroups

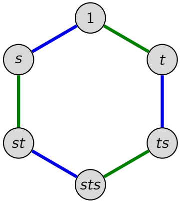
We have seen a number of definitions that involves product of elements and subgroups:

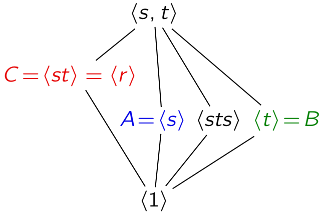
- Left cosets: $xH = \{xh \mid h \in H\}$
- Right cosets: $Hx = \{hx \mid h \in H\}$
- Conjugate subgroups: $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$.

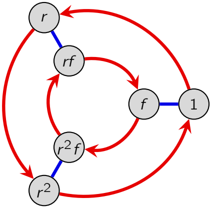
We can also define the product of two subgroups $A, B \leq G$:

$$AB = \{ab \mid a \in A,\ b \in B\}.$$

Let's investigate when this is a subgroup.







Notice that

$$AB = \{1, s, t, st\} \not\leq D_3, \qquad AC = \{1, r, r^2, f, fr, fr^2\} = D_3.$$

When is AB a subgroup?

Observation

If $AB = \{ab \mid a \in A,\ b \in B\}$ is a subgroup, then it must be "above" A and B in the lattice.

For closure to hold in AB, we need $(a_1 b_1)(a_2 b_2) \in AB$. It suffices to have $b_1 a_2 \in AB$.

Remark

If $A \leq N_G(B)$, "*A normalizes B*", i.e.,

$$\{ab \mid b \in B\} = aB = Ba = \{b'a \mid b' \in B\},$$

then every $ab \in AB$ can be written as some $b'a \in BA$.

Suppose A normalizes B. Then

$$(a_1 b_1)(a_2 b_2) = a_1 (b_1 a_2) b_2 = a_1 (a_2 b_1') b_2 \in AB.$$

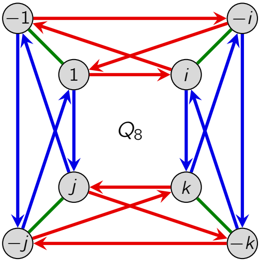
Proposition

If $A, B \leq G$ and one normalizes the other, then AB is a subgroup of G.

In particular, if at least one of them is normal, then $AB \leq G$. $\square$

Quotients

We have already encountered the concept a quotient of a group by a subgroup:



	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

$Q_8/\langle -1\rangle \cong V_4$

	± 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

We now know enough algebra to be able to formalize this.

Key idea

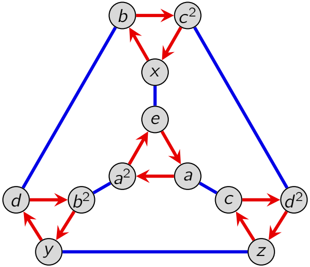
The quotient of G by a subgroup H exists when the (left) cosets of H form a group.

Goals:

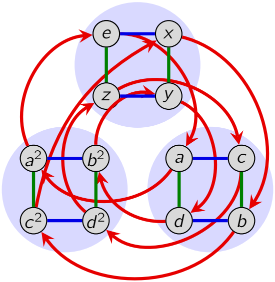
- Characterize *when* a quotient exists.
- Learn *how* to formalize this algebraically (without Cayley diagrams or tables).

Quotients

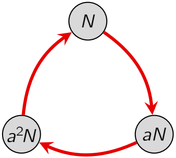
Here is an example of where the quotient works:



$A_4 = \langle (123), (12)(34) \rangle$



Organize the diagram by the left cosets of $N = \langle (12)(34), (14)(23) \rangle$



Collapse cosets into single nodes

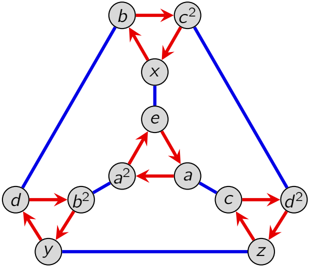
We denote the resulting group by $G/N = \{N,\ aN,\ a^2N\} \cong C_3$. Since it's a group, there is a binary operation on the set of cosets of N.

Questions

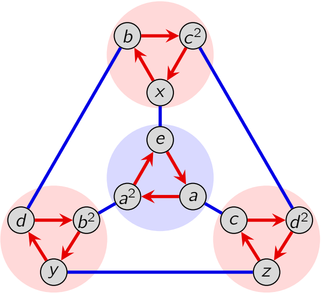
- Do you see *how* to define this binary operation?
- Do you see *why* this works for this particular $N \leq G$?
- Can you think of examples where this "quotient process" would fail, and why?

Quotients

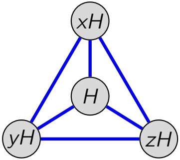
Here is an example of where the quotient fails:



$A_4 = \langle {\color{red}(123)}, {\color{blue}(12)(34)} \rangle$



Organize the diagram by the left cosets of $A = \langle (123) \rangle$.



Collapse cosets into single nodes

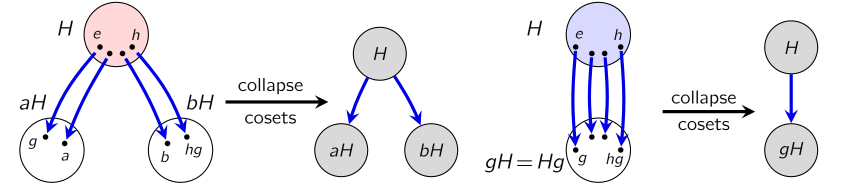
We can still write $G/H := \{H,\ xN,\ yH,\ zH\}$ for the set of (left) cosets of H in G.

However, the resulting diagram is not the Cayley diagram of a group.

In other words, something goes wrong if we try to define a binary operaton on G/H.

When and why the quotient process works

To get some intuition, let's consider collapsing the left cosets of a subgroup $H \leq G$.



Elements $g, hg \in Hg$ are in multiple left cosets of H

not a valid Cayley diagram

Elements in Hg all stay in gH

valid Cayley diagram

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.

We still need to formalize this and prove it algebraically.

What does it mean to "multiply" two cosets?

Quotient theorem

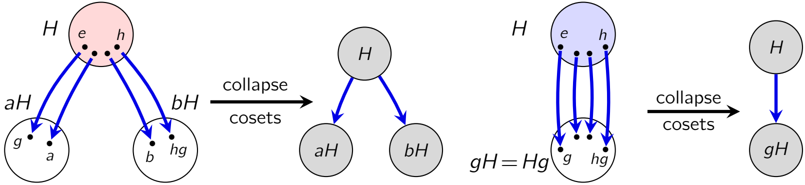
If $H \trianglelefteq G$, the set of cosets G/H forms a group, with binary operation

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

It is clear that G/H is closed under this operation.

We have to show that this operation is well-defined.

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



our destination depends on where in H we start

the quotient process does not yield a group

destination doesn't depend on where we start in H

quotient process succeeds

Quotient groups, algebraically

Lemma

Let $H \trianglelefteq G$. Multiplication of cosets is well-defined:

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

Proof

Suppose that $H \trianglelefteq G$, $a_1H = a_2H$ 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. $\square$

Quotient groups, algebraically

Quotient theorem (restated)

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

Proof

There is a well-defined binary operation on the set of left (equivalently, right) cosets: $aH \cdot bH = abH$.

We need to verify the three remaining properties of a group:

Identity. The coset $H = eH$ is the identity because for any coset $aH \in G/H$,

$$aH \cdot H = aeH = aH = eaH = H \cdot aH. \qquad \checkmark$$

Inverses. Given a coset aH, its inverse is $a^{-1}H$, because

$$aH \cdot a^{-1}H = eH = a^{-1}H \cdot aH. \qquad \checkmark$$

Closure. This is immediate, because $aH \cdot bH = abH$ is another coset in G/H. $\checkmark$

Quotient groups, algebraically

We just learned that if $H \trianglelefteq G$, then we can define a binary operation on cosets by

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

and *this works*.

Here's another reason why this makes sense.

Given any subgroup $H \leq G$, normal or not, define the product of left cosets:

$$xHyH = \big\{xh_1 yh_2 \mid h_1, h_2 \in H\big\}.$$

Exercise

If H is normal, then the set $xHyH$ is equal to the left cosets

$$xyH = \big\{xyh \mid h \in H\big\}.$$

To show that $xHyH = xyH$, it suffices to verify that $\subseteq$ and $\supseteq$ both hold. That is:

- every element of the form $xh_1 yh_2$ can be written as xyh for some $h \in H$.
- every element of the form xyh can be written as $xh_1 yh_2$ for some $h_1, h_2 \in H$.

Note that one containment is trivial. This will be left for homework.

Quotients of additive abelian groups

The subgroups of $G = \mathbb{Z}$ all have the form $n\mathbb{Z}$. Consider the subgroup

$$12\mathbb{Z} = \langle 12 \rangle = \{\dots, -24, -12, 0, 12, 24, \dots\} \trianglelefteq \mathbb{Z}.$$

The elements of the quotient group $\mathbb{Z}/\langle 12 \rangle$ are the cosets

$$0 + \langle 12 \rangle, \quad 1 + \langle 12 \rangle, \quad 2 + \langle 12 \rangle \quad , \; \dots \; , \quad 10 + \langle 12 \rangle, \quad 11 + \langle 12 \rangle.$$

Number theorists call these sets congruence classes modulo 12.

We say that two numbers are congruent modulo 12 if they are in the same coset.

Recall how to add cosets in the quotient group:

$$(a + \langle 12 \rangle) + (b + \langle 12 \rangle) := (a + b) + \langle 12 \rangle,$$

i.e., "(the coset containing a) + (the coset containing b) = the coset containing $a + b$."

For example, there are two ways to add 21 and 16 modulo 12:

- $(21 \pmod{12}) + (16 \pmod{12}) = 9 + 4 \pmod{12} = 1 \pmod{12}$.
- reduce $21 + 16 = 37$ modulo 12

It is not hard to see that $\mathbb{Z}/\langle 12 \rangle \cong \mathbb{Z}_{12}$.

We'll understand why when we see the isomorphism theorems.

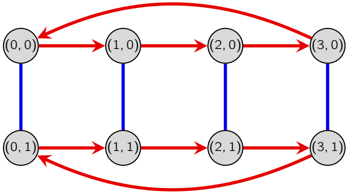
Quotient groups, algebraically

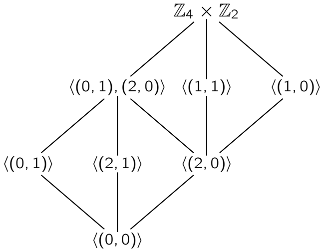
Remark

Do you think the following should be true or false, for subgroups H and K?

1. Does $H \cong K$ imply $G/H \cong G/K$?
2. Does $G/H \cong G/K$ imply $H \cong K$?
3. Does $H \cong K$ and $G_1/H \cong G_2/K$ imply $G_1 \cong G_2$?

All are false. Counterexamples for all of these can be found using the group $G = \mathbb{Z}_4 \times \mathbb{Z}_2$:





Conjugate elements

We've seen how conjugation defines an equivalence relation on the set of subgroups of G.

The equivalence class containing $H \leq G$ is its conjugacy class, denoted $\mathrm{cl}_G(H)$.

We can also conjugate elements. Given $x \in G$, we may ask:

"*which elements can be written as gxg^{-1} for some $g \in G$?*"

Definition

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

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

Proposition

The conjugacy class of $x \in G$ has size 1 if and only if $x \in Z(G)$.

Proof

Suppose $|\,\mathrm{cl}_G(x)| = 1$. This means that

$$\mathrm{cl}_G(x) = \{x\} \iff gxg^{-1} = x, \ \ \forall g \in G \iff gx = xg, \ \ \forall g \in G \iff x \in Z(G). \qquad \square$$

Conjugate elements

Lemma (exercise)

Conjugacy of elements is an equivalence relation.

Proof sketch

The following three properties need to be verified.

- **Reflexive**: Each $x \in G$ is conjugate to itself.
- **Symmetric**: If x is conjugate to y, then y is conjugate to x.
- **Transitive**: If x is conjugate to y, and y is conjugate to z, then x is conjugate to z.

As with any equivalence relation, the set is partitioned into equivalence classes.

The "class equation"

For any finite group G,

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

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

Conjugate elements

Proposition

Every normal subgroup is the union of conjugacy classes.

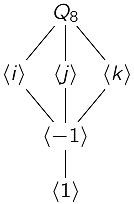
Proof

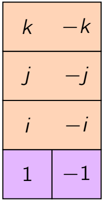
Suppose $n \in N \trianglelefteq G$. Then $gng^{-1} \in gNg^{-1} = N$, thus if $n \in N$, its entire conjugacy class $\text{cl}_G(n)$ is contained in N as well. $\square$

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

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

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





We completely determined the conjugacy classes without actually computing anything!

Conjugation preserves structure

Think back to linear algebra. Matrices A and B are similar (=conjugate) if $A = PBP^{-1}$.

Conjugate matrices have the same eigenvalues, eigenvectors, and determinant.

In fact, they represent the same linear map, but under a change of basis.

Central theme in mathematics

Two things that are conjugate have the same structure.

Let's start with a basic property preserved by conjugation.

Proposition

Conjugate elements in a group have the same order.

Proof

Consider x and $y = gxg^{-1}$. Suppose $|x| = n$, then

$$(gxg^{-1})^n = (gxg^{-1})(gxg^{-1}) \cdots (gxg^{-1}) = gx^n g^{-1} = geg^{-1} = e.$$

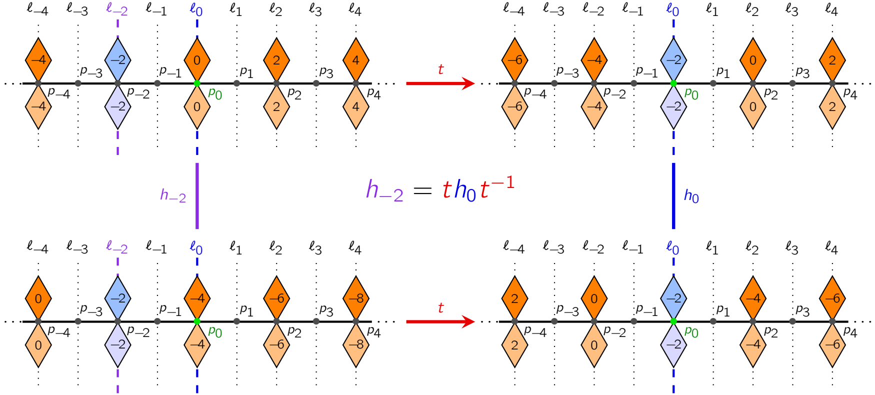
Therefore, $|x| \geq |gxg^{-1}| = |y|$. Reversing roles of x and y gives $|y| \geq |x|$. $\square$

Conjugation preserves structure

To understand what we mean by conjugation preserves structure, let's revisit 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.

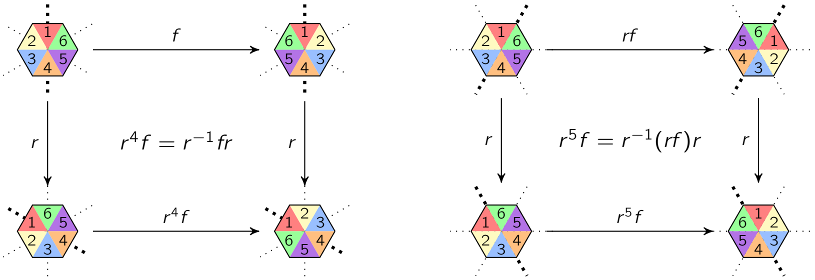
Conjugacy classes in D_n

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?

Next, let's verify the conjugacy classes algebraically.

Conjugacy classes in D_6

Let's find the conjugacy classes of D_6 algebraically.

The center is $Z(D_6) = \{e, r^3\}$; these are the *only* elements in size-1 conjugacy classes.

The only two elements of order 6 are r and r^5; so we must have $\mathrm{cl}_{D_6}(r) = \{r, r^5\}$.

The only two elements of order 3 are r^2 and r^4; so we must have $\mathrm{cl}_{D_6}(r^2) = \{r^2, r^4\}$.

For a reflection $r^i f$, we need to consider two cases; conjugating by r^j and by $r^j f$:

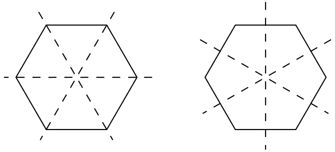
- $r^j(r^i f)r^{-j} = r^j r^i r^j f = r^{i+2j} f$
- $(r^j f)(r^i f)(r^j f)^{-1} = (r^j f)(r^i f) f r^{-j} = r^j f r^{i-j} = r^j r^{j-i} f = r^{2j-i} f.$

Thus, $r^i f$ and $r^k f$ are conjugate iff i and k have the same parity.

The Class Equation, visually:
Partition of D_6 by its
conjugacy classes

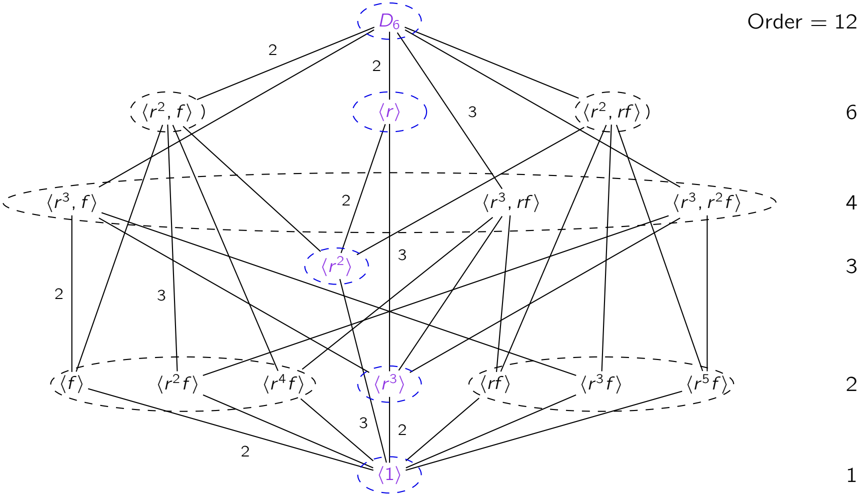
1	r	r^2	f	$r^2 f$	$r^4 f$
r^3	r^5	r^4	rf	$r^3 f$	$r^5 f$

If n is even, there are two conjugacy classes of reflections: those that fix two corners, and those that fix none.



The subgroup lattice of D_6

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



Cycle type and conjugacy in the symmetric group

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.

We can write the cycle type of a permutation $\sigma \in S_n$ as a list $c_1, c_2, \ldots, c_n$, where c_i is the number of cycles of length i in σ.

Here is an example of some elements in S_9 and their cycle types.

- $(1\ 8)\,(5)\,(2\ 3)\,(4\ 9\ 6\ 7)$ has cycle type 1,2,0,1.
- $(1\ 8\ 4\ 2\ 3\ 4\ 9\ 6\ 7)$ has cycle type 0,0,0,0,0,0,0,0,1.
- $e = (1)(2)(3)(4)(5)(6)(7)(8)(9)$ has cycle type 9.

Theorem

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

Big idea

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

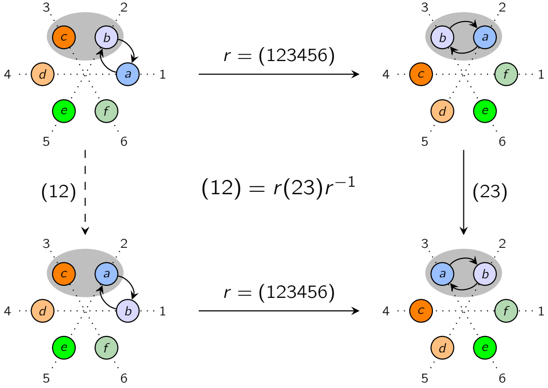
Conjugation preserves structure in the symmetric group

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:



swap positions
2 *and* 3

Centralizers

Definition

The centralizer of a set $X \subseteq G$ is the set of elements that commute with everything in X:

$$C_G(X) = \{g \in G \mid xg = xg, \text{ for all } g \in G\}.$$

It is easy to show that $C_G(X)$ is a subgroup, and that $C_G(H) \trianglelefteq N_G(H)$ if $H \leq G$. (HW).

If $X = \{x\}$, then we'll write $C_G(x)$. Clearly, $C_G(x)$ contains at least $\langle x \rangle$.

Definition

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

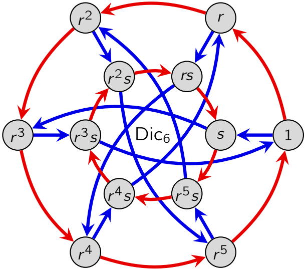
$$\mathrm{Deg}_G^C(x) := \frac{|C_G(x)|}{|G|} = \frac{1}{[G : C_G(x)]}.$$

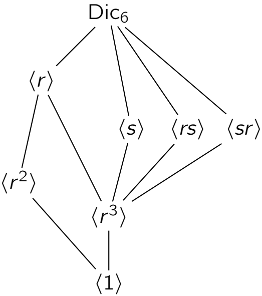
- If $\mathrm{Deg}_G^C(H) = 1$, then H is central.
- If $\mathrm{Deg}_G^C(H) = \frac{1}{n}$, we'll say H is fully uncentral.
- If $\frac{1}{n} < \mathrm{Deg}_G^C(H) < 1$, we'll say H is moderately uncentral.

Big idea

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

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 elements

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

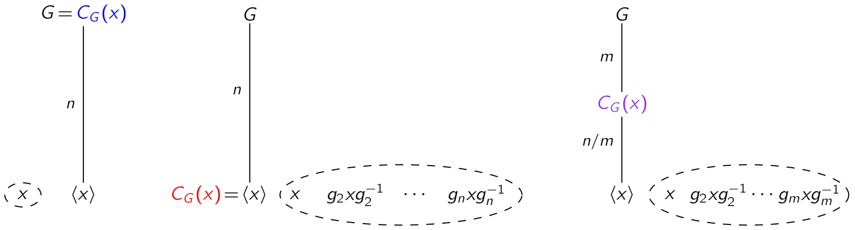
Theorem

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

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

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

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

fully uncentral

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

moderately uncentral

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