Chapter 5: Actions of groups

Matthew Macauley

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

Math 8510, Abstract Algebra

Action graphs

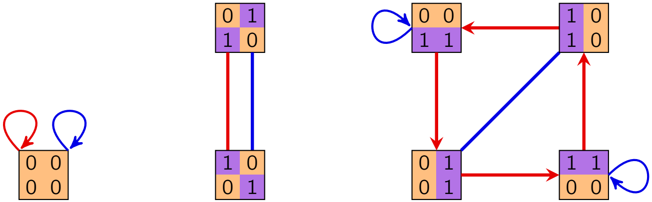
Technically, we started this class with group actions, and a bijective correspondence between "actions" (group elements) and "configurations" (set elements).

This need not always happen!

Suppose we have a size-7 set consisting of the following "binary squares."

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

The group $D_4 = \langle r, f \rangle$ "acts on S" as follows:



Every group action on a finite set defines an action graph, which generalizes Cayley graphs.

The "group switchboard" analogy

Suppose we have a "switchboard" for G, with every element $g \in G$ having a "button."

If $a \in G$, then pressing the a-button rearranges the objects in our set S. In fact, it is a permutation of S; call it $\phi(a)$.

If $b \in G$, then pressing the b-button rearranges the objects in S a different way. Call this permutation $\phi(b)$.

The element $ab \in G$ also has a button. We require that pressing the ab-button yields the same result as pressing the a-button, followed by the b-button. That is,

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

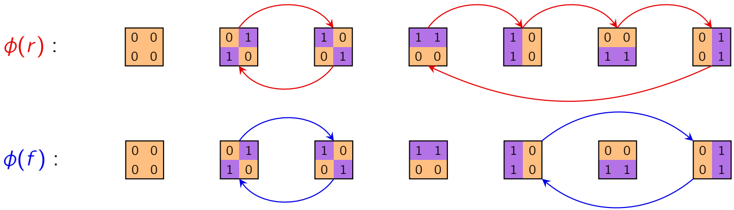
Let $\mathbf{Perm}(S)$ be the group of permutations of S.

Definition

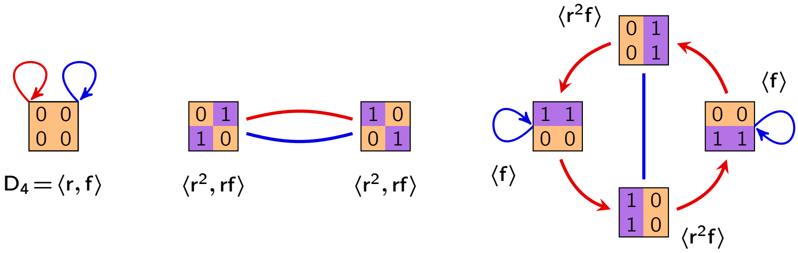
A group G acts on a set S if there is a homomorphism $\phi\colon G \to \mathbf{Perm}(S)$.

The "group switchboard" analogy

In our binary square example, pressing the r-button and f-button permutes S as follows:

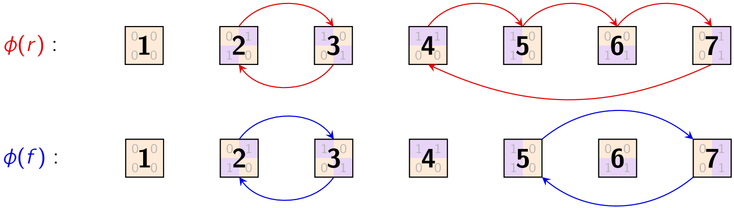


Observe how these permutations are encoded in the action graph. (Below each $s \in S$ is the subgroup that fixes it.)

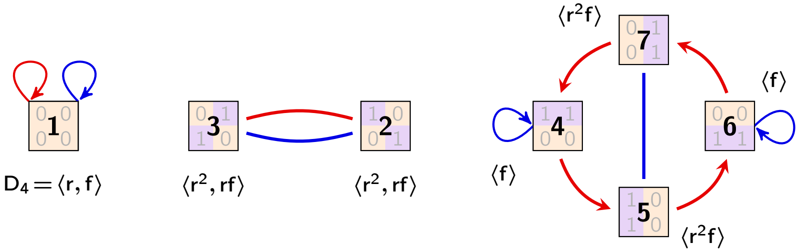


The “group switchboard” analogy

This action is an embedding $\phi\colon D_4 \hookrightarrow \mathrm{Perm}(S) \cong S_7$.



Notice that $\mathrm{Im}(\phi) = \big\langle (23)(4567), (23)(57) \big\rangle \cong D_4 \leq S_7$.



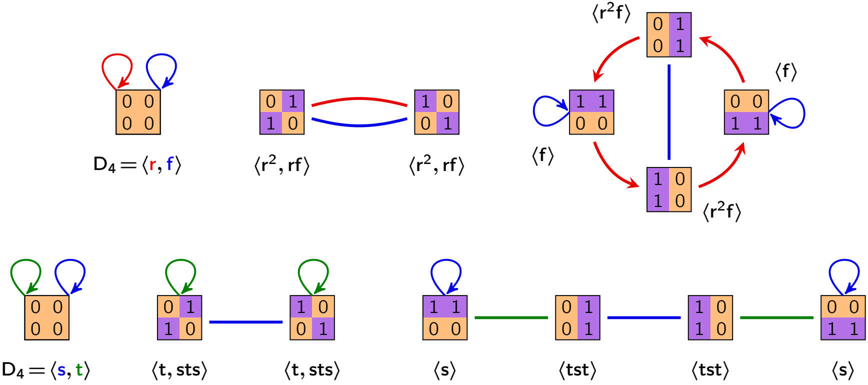
Action graphs vs. G-sets

Definition

A set S with a (right) action by G is called a (right) *G-set*.

Big idea

Action graphs are to G-sets, like how Cayley graphs are to groups.

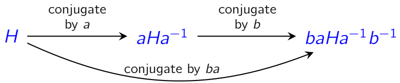


Left actions vs. right actions (an annoyance we can deal with)

As we've defined group actions, "*pressing the a-button followed by the b-button should be the same as pressing the ab-button*."

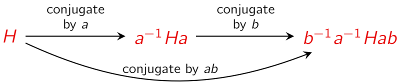
However, sometimes it appears like it's the same as "*pressing the ba-button*."

"Left group action"



$$\phi(a)\phi(b) = \phi(ba)$$

"Right group action"



$$\phi(a)\phi(b) = \phi(ab)$$

We'll call aHa^{-1} the left conjugate of H by a, and $a^{-1}Ha$ the right conjugate.

Some books forgo our "ϕ-notation" and use the following notation to distinguish left vs. right group actions:

$$g.(h.s) = (gh).s\,, \qquad\qquad (s.g).h = s.(gh).$$

We'll usually keep the ϕ, and write $\phi(g)\phi(h)s = \phi(gh)s$ and $s.\phi(g)\phi(h) = s.\phi(gh)$. As with groups, the "dot" will be optional.

Left actions vs. right actions (an annoyance we can deal with)

Alternative definition (other textbooks)

A right group action is a mapping

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

such that

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

A left group action can be defined similarly. Theorems for left actions have analogues for right actions.

Each left action has a related right action, and vice-versa. We will use right actions, and write

$$s.\phi(g)$$

for "*the element of S that the permutation $\phi(g)$ sends s to*," i.e., where pressing the g-button sends s.

If we have a left action, we'll write $\phi(g).s$.

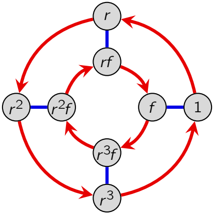
Action graphs generalize Cayley graphs

The group $G = D_4 = \langle r, f \rangle$ can on itself ($S = D_4$), or on its subgroups,

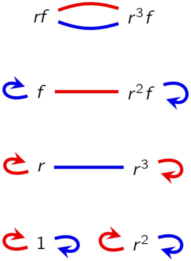
$$S = \big\{ D_4, \langle r \rangle, \langle r^2, f \rangle, \langle r^2, rf \rangle, \langle f \rangle, \langle rf \rangle, \langle r^2 f \rangle, \langle r^3 f \rangle, \langle r^2 \rangle, \langle 1 \rangle \big\}.$$

There are several ways to define the result of *"pressing the g-button on our switchboard"*.

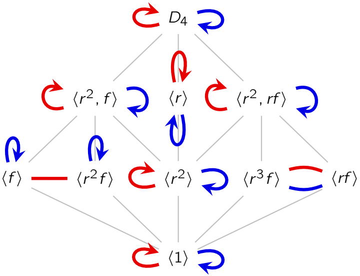
We say that: "*G acts on...*"



"*... itself by right-multiplication*"



"*... itself by conjugation*"



"*... its subgroups by conjugation*"

Remark

Every Cayley graph is the action graph of a particular group action.

Five features of every group action

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

There are several ways to classify them. For example:

- three are subsets of S
- two are subgroups of G.

Another way to classify them is by local vs. global:

- three are features of individual group or set elements (we'll write in *lowercase*)
- two are features of the homomorphism ϕ. (we'll write in *Uppercase*)

We will see parallels within and between these classes.

For example, two "local" features will be "dual" to each other, as will the global features.

Also, our global features can be expressed as intersections of our local features, either ranging over all $s \in S$, or over all $g \in G$.

We'll start by exploring the three local features.

Notation

Throughout, we'll denote identity elements by $1 \in G$ and $e \in \mathrm{Perm}(S)$.

Two local features: orbits and stabilizers

Suppose G acts on set S, and pick some $s \in S$. We can ask two questions about it:

(i) What other states (in S) are reachable from s? (We call this the orbit of s.)

(ii) What group elements (in G) fix s? (We call this the stabilizer of s.)

Definition

Suppose that G acts on a set S (on the right) via $\phi\colon G \to \mathrm{Perm}(S)$.

(i) The orbit of $s \in S$ is the set

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

(ii) The stabilizer of s in G is

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

In terms of the action graph

(i) The orbit of $s \in S$ is the connected component containing s.

(ii) The stabilizer of $s \in S$ are the group elements whose paths start and end at s; "loops."

The third local feature: fixators

Our last local feature is defined for each group element $g \in G$. A natural question is:

(iii) What *states* (in S) does g fix?

Definition

Suppose that G acts on a set S (on the right) via $\phi \colon G \to \mathrm{Perm}(S)$.

(iii) The fixator of $g \in G$ are the elements $s \in S$ fixed by g:

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

In terms of the action graph

(iii) The fixator of $g \in G$ are the nodes from which the g-paths are loops.

In terms of the "group switchboard analogy"

(i) The orbit of $s \in S$ are the elements in S the can be reached by pressing buttons.

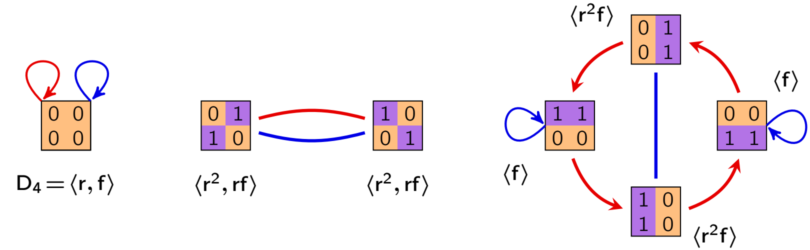
(ii) The stabilizer of $s \in S$ consists of the buttons that have no effect on s.

(iii) The fixator of $g \in G$ are the elements in S that don't move when we press the g-button.

Three local features: orbits, stabilizers, and fixators

The orbits of our running example are the 3 connected components.

Each node is labeled by its stabilizer.



The fixators are $\text{fix}(1) = S$, and

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

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

Local duality: stabilizers vs. fixators

Consider the following table, where a checkmark at (g, s) means g fixes s.

	$\begin{smallmatrix}0&0\\0&0\end{smallmatrix}$	$\begin{smallmatrix}0&1\\1&0\end{smallmatrix}$	$\begin{smallmatrix}1&0\\0&1\end{smallmatrix}$	$\begin{smallmatrix}0&0\\1&1\end{smallmatrix}$	$\begin{smallmatrix}0&1\\0&1\end{smallmatrix}$	$\begin{smallmatrix}1&1\\0&0\end{smallmatrix}$	$\begin{smallmatrix}1&0\\1&0\end{smallmatrix}$
1	✓	✓	✓	✓	✓	✓	✓
r	✓						
r^2	✓	✓	✓				
r^3	✓						
f	✓			✓		✓	
rf	✓	✓	✓				
r^2f	✓				✓		✓
r^3f	✓	✓	✓				

- the stablizers can be read off the columns: *group elements that fix $s \in S$*
- the fixators can be read off the rows: *set elements fixed by $g \in G$*.

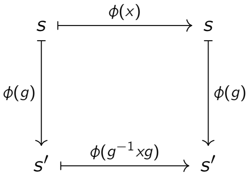
The stabilizer subgroup

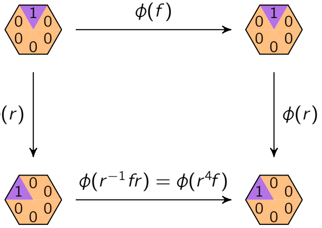
Proposition (HW exercise)

For any $s \in S$, the set $\mathbf{stab}(s)$ is a subgroup of G. Elements in the same orbit have conjugate stabilizers:

$$\mathbf{stab}(s.\phi(g)) = g^{-1}\,\mathbf{stab}(s)g, \quad \text{for all } g \in G \text{ and } s \in S.$$

In other words, if x stabilizes s, then $g^{-1}xg$ stabilizes $s.\phi(g)$.



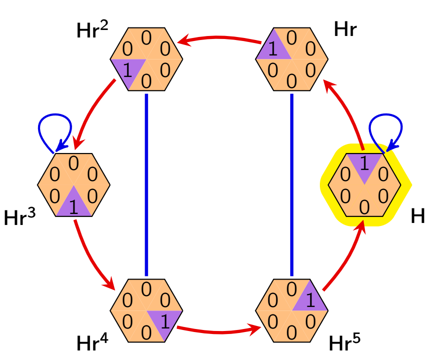


In other words, if x is a loop from s, and $s \xrightarrow{g} s'$, then $g^{-1}xg$ is a loop from s'.

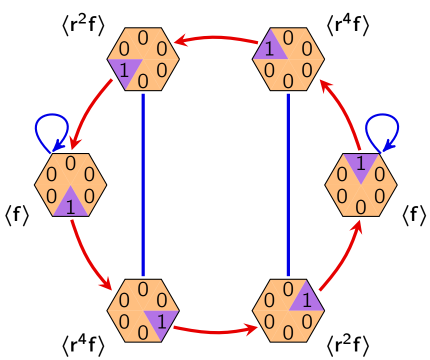
The stabilizer subgroup

Here is another example of an action, this time of $G = D_6$.

Let s be the highlighted hexagon, and $H = \textbf{stab}(s)$.



labeled by destinations



labeled by stabilizers

Two global features: fixed points and the kernel

Our last two features are properties of the action ϕ, rather than of specific elements.

The first definition is new, and the second is an familiar concept in this new setting.

Definition

Suppose that G acts on a set S via $\phi\colon G \to \mathrm{Perm}(S)$.

(iv) The kernel of the action is the set

$$\mathrm{Ker}(\phi) = \{k \in G \mid \phi(k) = e\} = \{k \in G \mid s.\phi(k) = s \text{ for all } s \in S\}.$$

(v) The fixed points of the action, denoted $\mathrm{Fix}(\phi)$, are the orbits of size 1:

$$\mathrm{Fix}(\phi) = \{s \in S \mid s.\phi(g) = s \text{ for all } g \in G\}.$$

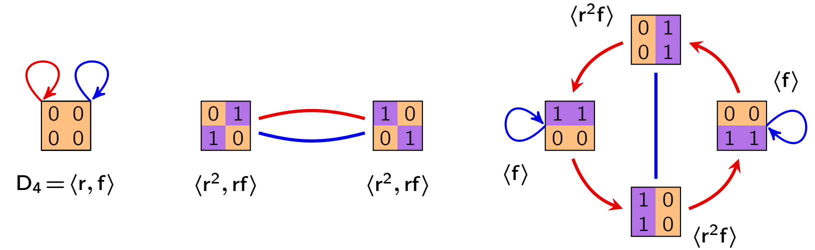
Proposition (global duality: fixed points vs. kernel)

Suppose that G acts on a set S via $\phi\colon G \to \mathrm{Perm}(S)$. Then

$$\mathrm{Ker}(\phi) = \bigcap_{s \in S} \mathrm{stab}(s), \qquad \text{and} \qquad \mathrm{Fix}(\phi) = \bigcap_{g \in G} \mathrm{fix}(g).$$

Let's also write $\mathrm{Orb}(\phi)$ for the set of orbits of ϕ.

Two global features: fixed points and the kernel



In terms of the action graph

(iv) The kernel of ϕ are the paths that are "loops from every $s \in S$."

(v) The fixed points of ϕ are the size-1 connected components.

In terms of the group switchboard analogy

(iv) The kernel of ϕ are the "broken buttons"; those $g \in G$ that have no effect on any s.

(v) The fixed points of ϕ are those $s \in S$ that are not moved by pressing any button.

Global duality: fixed points vs. kernel

Consider the following table, where a checkmark at (g, s) means g fixes s.

	$\begin{smallmatrix}0&0\\0&0\end{smallmatrix}$	$\begin{smallmatrix}0&1\\1&0\end{smallmatrix}$	$\begin{smallmatrix}1&0\\0&1\end{smallmatrix}$	$\begin{smallmatrix}0&0\\1&1\end{smallmatrix}$	$\begin{smallmatrix}0&1\\0&1\end{smallmatrix}$	$\begin{smallmatrix}1&1\\0&0\end{smallmatrix}$	$\begin{smallmatrix}1&0\\1&0\end{smallmatrix}$
1	✓	✓	✓	✓	✓	✓	✓
r	✓						
r^2	✓	✓	✓				
r^3	✓						
f	✓			✓		✓	
rf	✓	✓	✓				
r^2f	✓				✓		✓
r^3f	✓	✓	✓				

- the fixed points consist of columns with all checkmarks: *set elts fixed by everything*
- the kernel consists of the rows with all checkmarks: *group elements that fix everything*.

Two theorems on orbits, and their consequences

Our binary square example gives us key intutition about group actions.

Qualitative observations

- elements in larger orbits tend to have smaller stabilizers, and vice-versa
- action tables with more "checkmarks" tend to have more orbits.

Both of these qualitative observations can be formalized into quantitative theorems.

Theorems

1. **Orbit-stabilizer theorem**: the size of an orbit is the index of the stabilizer.
2. **Orbit-counting theorem**: the number of orbits is the average number of things fixed by a group element.

If we set up our actions correctly, the orbit-stabilizer theorem will imply:

- The size of the conjugacy class $\text{cl}_G(H)$ is the index of the normalizer of $H \leq G$
- The size of the conjugacy class $\text{cl}_G(x)$ is the index of the centralizer of $x \in G$

We can also determine the number of conjugacy classes from the orbit-counting theorem.

Our first theorem on orbits

Orbit-stabilizer theorem

For any group action $\phi\colon G \to \mathrm{Perm}(S)$, and any $s \in S$,

$$|\,\mathrm{orb}(s)| \cdot |\,\mathrm{stab}(s)| = |\,G\,|\,.$$

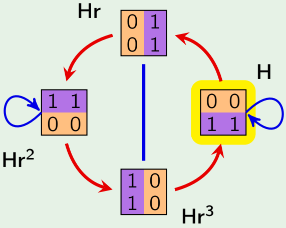
Equivalently, *the size of the orbit containing s is* $|\,\mathrm{orb}(s)| = [G : \mathrm{stab}(s)]$.

Proof

Goal: Exhibit a bijection between elements of $\mathrm{orb}(s)$, and right cosets of $\mathrm{stab}(s)$.

That is, "*two g-buttons send s to the same place iff they're in the same coset*".

r^3	fr^3	$\mathbf{Hr^3}$
r^2	fr^2	$\mathbf{Hr^2}$
r	fr	$\mathbf{Hr}$
1	f	$\mathbf{H = stab(s)}$



Note that $s.\phi(g) = s.\phi(k)$ iff g and k are in the same right coset of H in G.

The orbit-stabilizer theorem: $|\text{orb}(s)| \cdot |\text{stab}(s)| = |G|$

Proof (cont.)

Throughout, let $H = \text{stab}(s)$.

"$\Rightarrow$" *If two elements send s to the same place, then they are in the same coset.*

Suppose $g, k \in G$ both send s to the same element of S. This means:

$$\begin{aligned} s.\phi(g) = s.\phi(k) \quad &\Longrightarrow \quad s.\phi(g)\phi(k)^{-1} = s \\ &\Longrightarrow \quad s.\phi(g)\phi(k^{-1}) = s \\ &\Longrightarrow \quad s.\phi(gk^{-1}) = s \qquad \text{(i.e., } gk^{-1} \text{ stabilizes } s) \\ &\Longrightarrow \quad gk^{-1} \in H \qquad \text{(recall that } H = \text{stab}(s)) \\ &\Longrightarrow \quad Hgk^{-1} = H \\ &\Longrightarrow \quad Hg = Hk \end{aligned}$$

"$\Leftarrow$" *If two elements are in the same coset, then they send s to the same place.*

Take two elements $g, k \in G$ in the same right coset of H. This means $Hg = Hk$.

This is the last line of the proof of the forward direction, above. We can change each $\Longrightarrow$ into $\Longleftrightarrow$, and thus conclude that $s.\phi(g) = s.\phi(k)$. □

If we have instead, a left group action, the proof carries through but using left cosets.

Our second theorem on orbits

Orbit-counting theorem

Let a finite group G act on a set S via $\phi\colon G \to \mathsf{Perm}(S)$. Then

$$|\operatorname{Orb}(\phi)| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{fix}(g)|.$$

This says that the "*average number of checkmarks per row*" is the number of orbits:

	$\begin{smallmatrix}0&0\\0&0\end{smallmatrix}$	$\begin{smallmatrix}0&1\\1&0\end{smallmatrix}$	$\begin{smallmatrix}1&0\\0&1\end{smallmatrix}$	$\begin{smallmatrix}0&0\\1&1\end{smallmatrix}$	$\begin{smallmatrix}0&1\\0&1\end{smallmatrix}$	$\begin{smallmatrix}1&1\\0&0\end{smallmatrix}$	$\begin{smallmatrix}1&0\\1&0\end{smallmatrix}$
1	✓	✓	✓	✓	✓	✓	✓
r	✓						
r^2	✓	✓	✓				
r^3	✓						
f	✓			✓		✓	
rf	✓	✓	✓				
r^2f	✓				✓		✓
r^3f	✓	✓	✓				

Orbit-counting theorem: $|\operatorname{Orb}(\phi)| = \dfrac{1}{|G|}\sum_{g\in G}|\operatorname{fix}(g)|$.

Proof

Let's first count the number of checkmarks in the action table, three ways:

$$\underbrace{\sum_{g\in G}|\operatorname{fix}(g)|}_{\text{count by rows}} = \Big|\big\{(g,s)\in G\times S \mid s.\phi(g)=s\big\}\Big| = \underbrace{\sum_{s\in S}|\operatorname{stab}(s)|}_{\text{count by columns}}.$$

By the orbit-stabilizer theorem, we can replace each $|\operatorname{stab}(s)|$ with $|G|/|\operatorname{orb}(s)|$:

$$\sum_{s\in S}|\operatorname{stab}(s)| = \sum_{s\in S}\frac{|G|}{|\operatorname{orb}(s)|} = |G|\sum_{s\in S}\frac{1}{|\operatorname{orb}(s)|}.$$

Let's express this sum over all disjoint orbits $S=\mathcal{O}_1\cup\cdots\cup\mathcal{O}_k$ separately:

$$|G|\sum_{s\in S}\frac{1}{|\operatorname{orb}(s)|} = |G|\sum_{\mathcal{O}\in\operatorname{Orb}(\phi)}\Bigg(\underbrace{\sum_{s\in\mathcal{O}}\frac{1}{|\operatorname{orb}(s)|}}_{=1\quad (why?)}\Bigg) = |G|\sum_{\mathcal{O}\in\operatorname{Orb}(\phi)}1 = |G|\cdot|\operatorname{Orb}(\phi)|.$$

Equating this last term with the first term gives the desired result. ☐

Groups acting on elements, subgroups, and cosets

It is frequently of interest to analyze the action of a group G on its elements, subgroups, or cosets of some fixed $H \leq G$.

Often, the orbits, stabilizers, and fixed points of these actions are familiar algebraic objects.

A number of deep theorems have a slick proof via a clever group action.

Here are common examples of group actions:

- G acts on itself by right-multiplication (or left-multiplication).
- G acts on itself by conjugation.
- G acts on its subgroups by conjugation.
- G acts on the right-cosets of a fixed subgroup $H \leq G$ by right-multiplication.

For each of these, we'll characterize the orbits, stabilizers, fixators kernel, and fixed points.

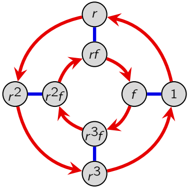
We'll encounter familiar objects such as conjugacy classes, normalizers, stabilizers, and normal subgroups, as some of our "five fundamental features".

Groups acting on themselves by right-multiplication

Assume $|G| > 2$. The group G acts on itself (that is, $S = G$) by **right-multiplication**:

$$\phi\colon G \longrightarrow \mathrm{Perm}(S)\,, \qquad \phi(g) = \text{the permutation that sends each } x \mapsto xg.$$

- there is only one orbit: $\mathrm{orb}(x) = G$, for all $x \in G$
- the stabilizer of each $x \in G$ is $\mathrm{stab}(x) = \langle 1 \rangle$
- the fixator of $g \neq 1$ is $\mathrm{fix}(g) = \emptyset$.
- there are no fixed points, and the kernel is trivial:



$$\mathrm{Fix}(\phi) = \bigcap_{g \in G} \mathrm{fix}(g) = \emptyset, \qquad \text{and} \qquad \mathrm{Ker}(\phi) = \bigcap_{s \in S} \mathrm{stab}(s) = \langle 1 \rangle.$$

Cayley's theorem

If $|G| = n$, then there is an embedding $G \hookrightarrow S_n$.

Proof

Let G act on itself by right multiplication. This defines a homomorphism

$$\phi\colon G \longrightarrow \mathrm{Perm}(S) \cong S_n.$$

Since $\mathrm{Ker}(\phi) = \langle 1 \rangle$, it is an embedding. $\square$

Groups acting on themselves by conjugation

Another way a group G can act on itself (that is, $S = G$) is by **conjugation**:

$$\phi\colon G \longrightarrow \text{Perm}(S), \qquad \phi(g) = \text{the permutation that sends each } x \mapsto g^{-1}xg.$$

- The orbit of $x \in G$ is its conjugacy class:

$$\text{orb}(x) = \{x.\phi(g) \mid g \in G\} = \{g^{-1}xg \mid g \in G\} = \text{cl}_G(x).$$

- The stabilizer of x is its centralizer:

$$\text{stab}(x) = \{g \in G \mid g^{-1}xg = x\} = \{g \in G \mid xg = gx\} := C_G(x)$$

- The fixator of $g \in G$ is also its centralizer, because

$$\text{fix}(g) = \{x \in S \mid x.\phi(g) = x\} = \{x \in G \mid g^{-1}xg = x\} = C_G(g).$$

- The fixed points and kernel are the center, because

$$\text{Fix}(\phi) = \bigcap_{g \in G} \text{fix}(g) = \bigcap_{g \in G} C_G(g) = Z(G) = \bigcap_{x \in G} C_G(x) = \bigcap_{x \in G} \text{stab}(x) = \text{Ker}(\phi).$$

Groups acting on themselves by conjugation

Let's apply our two theorems:

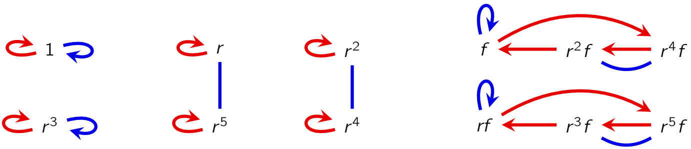
1. **Orbit-stabilizer theorem**. "*the size of an orbit is the index of the stabilizer*":

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

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

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

Let's revisit our old example of conjugacy classes in $D_6 = \langle r, f \rangle$:



Notice that the stabilizers are $\mathbf{stab}(r) = \mathbf{stab}(r^2) = \mathbf{stab}(r^4) = \mathbf{stab}(r^5) = \langle r \rangle$,

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

Groups acting on themselves by conjugation

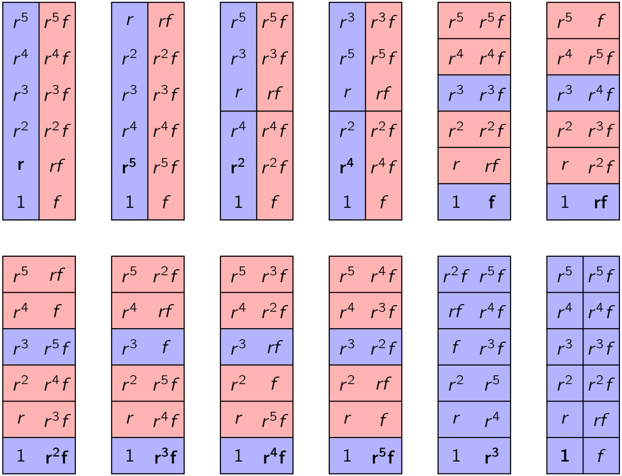
Here is the "*fixed point table*". Note that $\text{Ker}(\phi) = \text{Fix}(\phi) = \langle r^3 \rangle$.

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

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

Groups acting on themselves by conjugation

Here are the cosets of all 12 cyclic subgroups in D_6 (some coincide).



Do you see how to deduce from the orbit-counting theorem that there are 6 conjugacy classes?

Groups acting on subgroups by conjugation

Any group G acts on its set S of subgroups by **conjugation**:

$$\phi \colon G \longrightarrow \mathrm{Perm}(S)\,, \qquad \phi(g) = \text{the permutation that sends each } H \text{ to } g^{-1}Hg.$$

This is a **right action**, but there is an associated left action: $H \mapsto gHg^{-1}$.

Let $H \leq G$ be an element of S.

- The orbit of H consists of all conjugate subgroups:

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

- The stabilizer of H is the normalizer of H in G:

$$\mathrm{stab}(H) = \{g \in G \mid g^{-1}Hg = H\} = N_G(H).$$

- The fixator of g are the subgroups that g normalizes:

$$\mathrm{fix}(g) = \{H \mid g^{-1}Hg = H\} = \{H \mid g \in N_G(H)\},$$

- The fixed points of ϕ are precisely the normal subgroups of G:

$$\mathrm{Fix}(\phi) = \{H \leq G \mid g^{-1}Hg = H \text{ for all } g \in G\}.$$

- The kernel of this action is the set of elements that normalize every subgroup:

$$\mathrm{Ker}(\phi) = \{g \in G \mid g^{-1}Hg = H \text{ for all } H \leq G\} = \bigcap_{H \leq G} N_G(H).$$

Groups acting on subgroups by conjugation

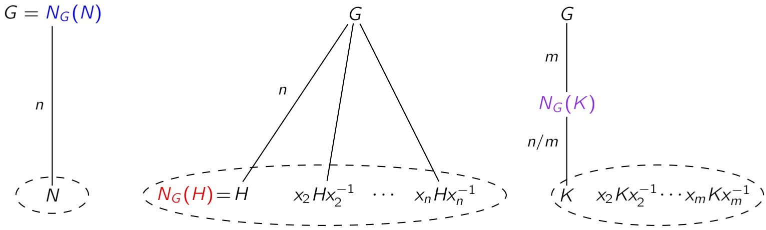
Let's apply our two theorems:

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

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

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

#conjugacy classes of subgroups of G = average size of a normalizer.

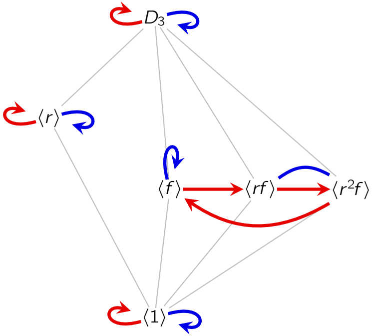


normal	*fully unnormal*	*moderately unnormal*
$\big\|\operatorname{cl}_G(N)\big\| = 1$	$\big\|\operatorname{cl}_G(H)\big\| = [G : H]$; as large as possible	$1 < \big\|\operatorname{cl}_G(K)\big\| < [G : K]$

Groups acting on subgroups by conjugation

Here is an example of $G = D_3$ acting on its subgroups.

$\tau(1) =$	$\langle 1 \rangle$	$\langle r \rangle$	$\langle f \rangle$	$\langle rf \rangle$	$\langle r^2 f \rangle$	D_3
$\tau(r) =$	$\langle 1 \rangle$	$\langle r \rangle$	$\langle f \rangle$	$\langle rf \rangle$	$\langle r^2 f \rangle$	D_3
$\tau(r^2) =$	$\langle 1 \rangle$	$\langle r \rangle$	$\langle f \rangle$	$\langle rf \rangle$	$\langle r^2 f \rangle$	D_3
$\tau(f) =$	$\langle 1 \rangle$	$\langle r \rangle$	$\langle f \rangle$	$\langle rf \rangle$	$\langle r^2 f \rangle$	D_3
$\tau(rf) =$	$\langle 1 \rangle$	$\langle r \rangle$	$\langle f \rangle$	$\langle rf \rangle$	$\langle r^2 f \rangle$	D_3
$\tau(r^2 f) =$	$\langle 1 \rangle$	$\langle r \rangle$	$\langle f \rangle$	$\langle rf \rangle$	$\langle r^2 f \rangle$	D_3



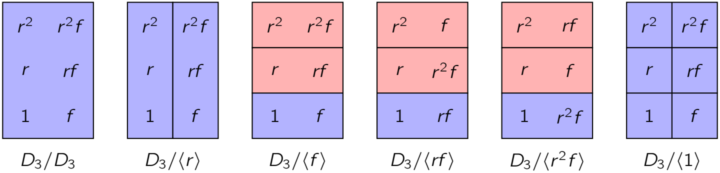
Observations

Do you see how to read stabilizers and fixed points off of the permutation diagram?

- $\mathrm{Ker}(\phi) = \langle 1 \rangle$ consists of the row(s) with only fixed points.
- $\mathrm{Fix}(\phi) = \{\langle 1 \rangle, \langle r \rangle, D_3\}$ consists of the column(s) with only fixed points.
- By the orbit-counting theorem, there are $|\mathrm{Orb}(\phi)| = 24/|D_3| = 4$ conjugacy classes.

Groups acting on subgroups by conjugation

Consider the partitions of D_3 by the left cosets of its six subgroups:



- fix(g) are the subgroups H for which "*g appears in a blue coset of H*"
- Ker(ϕ) are elements that "*only appear in blue cosets*"
- By the orbit-counting theorem, the subgroups fall into

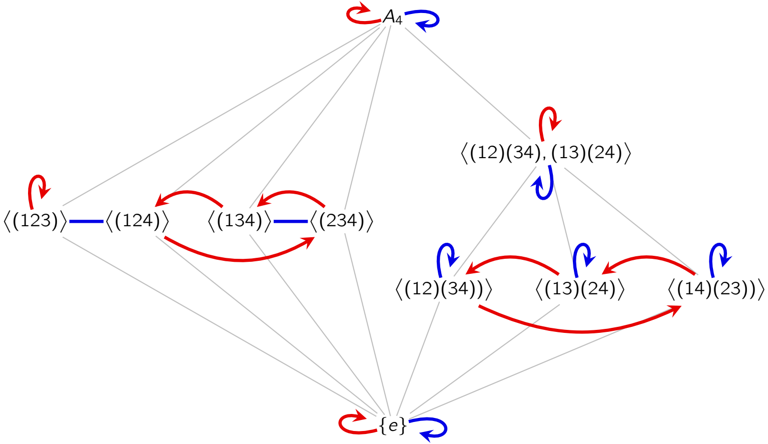
$$|\,\mathrm{Orb}(\phi)| = \text{average \# check marks per row} = \frac{\text{total \# of blue entries}}{|G|}$$

conjugacy classes.

Equivalently: *how many full "G-boxes" the blue cosets can be rearranged to fill up.*

Groups acting on subgroups by conjugation

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



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

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

Groups acting on subgroups by conjugation

Here is the "*fixed point table*" of the action of A_4 on its subgroups.

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

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

Groups acting on cosets of H by right-multiplication

Fix a subgroup $H \leq G$. Then G acts on its **right cosets** by **right-multiplication**:

$$\phi\colon G \longrightarrow \mathrm{Perm}(S)\,, \qquad \phi(g) = \text{the permutation that sends each } Hx \text{ to } Hxg.$$

Let Hx be an element of $S = H\backslash G$ (the right cosets of H).

- There is only one orbit. For example, given two cosets Hx and Hy,

$$\phi(x^{-1}y) \text{ sends } Hx \longmapsto Hx(x^{-1}y) = Hy.$$

- The stabilizer of Hx is the conjugate subgroup $x^{-1}Hx$:

$$\mathrm{stab}(Hx) = \{g \in G \mid Hxg = Hx\} = \{g \in G \mid Hxgx^{-1} = H\} = x^{-1}Hx.$$

- There doesn't seem to be a standard term for the fixator of g:

$$\mathrm{fix}(g) = \{Hx \mid Hxg = Hx\} = \{Hx \mid xgx^{-1} \in H\}.$$

- Assuming $H \neq G$, there are no fixed points of ϕ.
- The kernel of this action is the intersection of all conjugate subgroups of H:

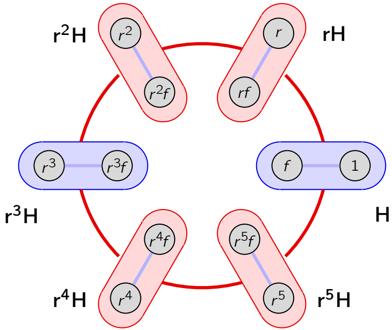
$$\mathrm{Ker}(\phi) = \bigcap_{x\in G} \mathrm{stab}(x) = \bigcap_{x\in G} x^{-1}Hx.$$

  Notice that $\langle 1\rangle \leq \mathrm{Ker}(\phi) \leq H$, and $\mathrm{Ker}(\phi) = H$ iff $H \trianglelefteq G$.

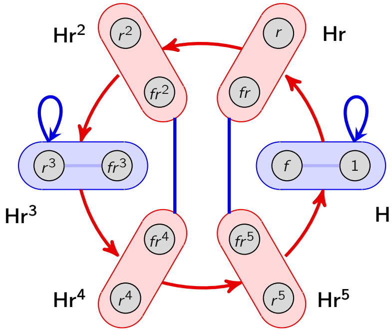
Groups acting on cosets of H by right-multiplication

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

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



not a valid action graph



action graph of ϕ

Subgroups of small index

Groups acting on cosets is a useful technique for establishing seemingly unrelated results.

Several of these involving showing that subgroups of "small index" are normal.

We've already seen that subgroups of index 2 are normal.

Of course, there are non-normal index-3 subgroups, like $\langle f \rangle \leq D_3$.

The following gives a sufficient condition for when index-3 subgroups are normal.

Proposition

If G has no subgroup of index 2, then any subgroup of index 3 is normal.

Proof

Let $H \leq G$ with $[G : H] = 3$.

Let G act on the cosets of H by multiplication, to get a nontrivial homomorphism

$$\phi \colon G \longrightarrow S_3.$$

$K := \mathrm{Ker}(\phi) \leq H$ is the largest normal subgroup of G contained in H. By the FHT,

$$G/K \cong \mathrm{Im}(\phi) \leq S_3.$$

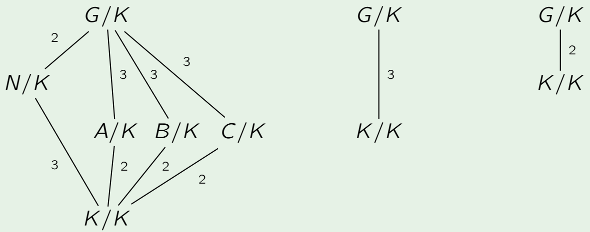
Subgroups of small index

Proof (contin.)

Thus, there are three cases for this quotient:

$$G/K \cong S_3, \qquad G/K \cong C_3, \qquad G/K \cong C_2.$$

Visually, this means that we have one of the following:



By the correspondence theorem, $K \leq H \lneq G$ implies $K/K \leq H/K \lneq G/K$.

Since G has no index-2 subgroup, only the middle case is possible (*Why?*).

This forces $K/K = H/K$, and so $K = H$ which is normal for multiple reasons. ☐

Subgroups of small index

Proposition

Suppose $H \leq G$ and $[G : H] = p$, the smallest prime dividing $|G|$. Then $H \trianglelefteq G$.

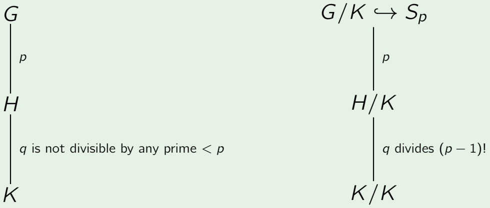
Proof

Let G act on the cosets of H by multiplication, to get a non-trivial homomorphism

$$\phi \colon G \longrightarrow S_p.$$

The kernel $K = \mathrm{Ker}(\phi)$, is the largest normal subgroup of G such that $K \leq H \lneq G$.

We'll show that $H = K$, or equivalently, that $[H : K] = 1$. By the correspondence theorem:



Do you see why $q = 1$? □

A summary of our four actions

Thus far, we have seen four important (right) actions of a group G, acting:

- on itself by right-multiplication
- on itself by conjugation.
- on its subgroups by conjugation.
- on the right-cosets of a fixed subgroup $H \leq G$ by multiplication.

set $S =$	G		subgroups of G	right cosets of H
operation	multiplication	conjugation	conjugation	right multiplication
orb(s)	G	$\mathrm{cl}_G(g)$	$\mathrm{cl}_G(H)$	all right cosets
stab(s)	$\langle 1 \rangle$	$C_G(g)$	$N_G(H)$	$x^{-1}Hx$
fix(g)	G or $\emptyset$	$C_G(g)$	$\{H \mid g \in N_G(H)\}$	
Ker(ϕ)	$\langle 1 \rangle$	$Z(G)$	$\bigcap_{H \leq G} N_G(H)$	largest norm. subgp. $N \leq H$
Fix(ϕ)	$\emptyset$	$Z(G)$	normal subgroups	none

Actions of automorphism groups

Let's revist the idea of automorophisms, but this time in a group action framework.

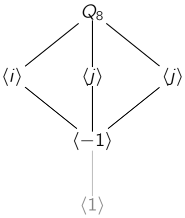
For any G, the automorphism group $\mathrm{Aut}(G)$ naturally acts on $S = G$ via a homomorphism

$$\phi\colon \mathrm{Aut}(G) \longrightarrow \mathrm{Perm}(S), \qquad \phi(\sigma) = \text{the permutation that sends each } g \mapsto \sigma(g).$$

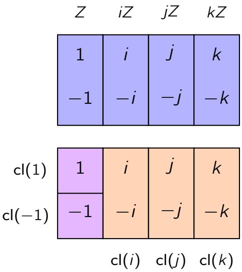
Let's see an example. Any $\sigma \in \mathrm{Aut}(Q_8)$ must send i to an element of order 4: $\pm i$, $\pm j$, $\pm k$.

This leaves 4 choices for $\sigma(j)$. Therefore, $|\,\mathrm{Aut}(Q_8)| \leq 24$.

The inner automorphism group is $\mathrm{Inn}(Q_8) = \{\,\mathrm{Id}, \varphi_i, \varphi_j, \varphi_k\}$.



$\mathrm{Inn}(Q_8) \cong Q_8/\langle -1 \rangle \cong V_4$



cosets of $Z(Q_8)$ are in bijection with inner automorphisms of Q_8

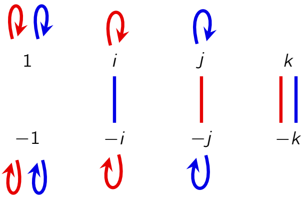
inner automorphisms of Q_8 permute elements within conjugacy classes

All permutations of $\{i, j, k\}$ define an outer automorphism, and so $\mathrm{Out}(Q_8) \cong S_3$.

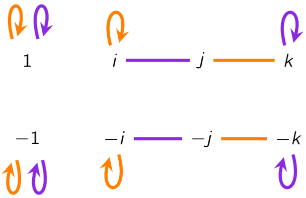
Automorphisms of Q_8

All three groups $\mathbf{Aut}(Q_8)$, $\mathbf{Inn}(Q_8)$, and $\mathbf{Out}(Q_8) \cong \mathbf{Aut}(Q_8)/\mathbf{Inn}(Q_8)$ act on $S = Q_8$.

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



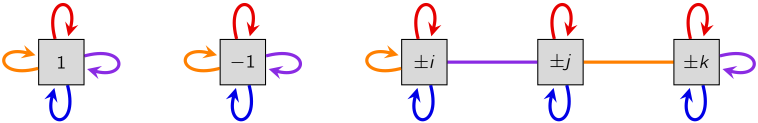
$\mathbf{Out}(Q_8) \cong S_3$



Overlaying these two graphs gives the action on $S = Q_8$ by

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

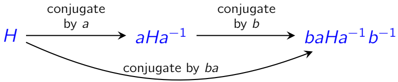
The group $\mathbf{Aut}(Q_8)$ also acts on the conjugacy classes:



Action equivalence

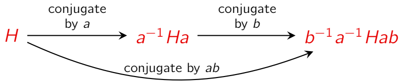
Let's recall the difference between left-conjugating and right conjugating:

"Left group action"



$$\phi(a)\phi(b) = \phi(ba)$$

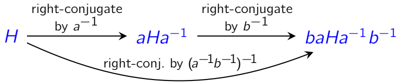
"Right group action"



$$\phi(a)\phi(b) = \phi(ab)$$

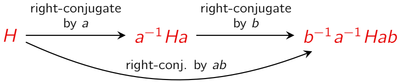
There's a better way to describe left actions than the faux-homomorphic $\phi(a)\phi(b) = \phi(ba)$.

"Left group action"



$$\phi(a^{-1})\phi(b^{-1}) = \phi(a^{-1}b^{-1}) = \phi((ba)^{-1})$$

"Right group action"



$$\phi(a)\phi(b) = \phi(ab)$$

Big idea

For every right action, there is an "equivalent" left-action where:

"pressing g-buttons, from L-to-R" $\Leftrightarrow$ "pressing g^{-1}-buttons, from R-to-L".

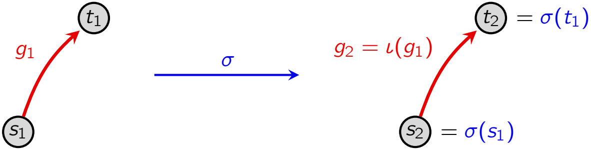
Action equivalence, informally

Action equivalence is more general. Consider two groups acting on sets, say via

$$\phi_1 \colon G_1 \longrightarrow \mathsf{Perm}(S_1), \qquad \text{and} \qquad \phi_2 \colon G_2 \longrightarrow \mathsf{Perm}(S_2).$$

If these are "equivalent", then we'll need

- a set bijection $\sigma \colon S_1 \longrightarrow S_2$
- a group isomorphism $\iota \colon G_1 \longrightarrow G_2$.



Informally, these actions are **equivalent** if:

1. pressing the g_1-button in the G_1-switchboard, followed by
2. applying $\sigma \colon S_1 \to S_2$ to get to the other graph

is the same as doing these steps in reverse order. That is,

1. applying $\sigma \colon S_1 \to S_2$ to get to the other graph, then
2. pressing the $\iota(g_1)$-button on the G_2-switchboard.

Action equivalence, formally

Definition

Two actions $\phi_1 \colon G_1 \longrightarrow \mathbf{Perm}(S_1)$ and $\phi_2 \colon G_2 \longrightarrow \mathbf{Perm}(S_2)$ are equivalent if there is an isomorphism $\iota \colon G_1 \to G_2$ and a bijection $\sigma \colon S_1 \to S_2$ such that

$$\sigma \circ \phi_1(g) = \phi_2(\iota(g)) \circ \sigma, \quad \text{for all } g \in G.$$

We say that the resulting action graphs are action equivalent.

This can be expressed with a commutative diagram:

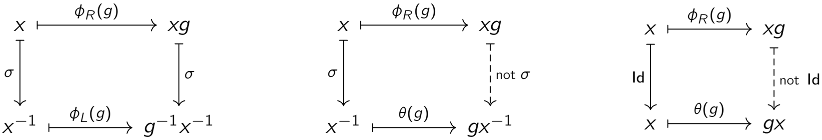
$$\begin{array}{ccc} S_1 & \xrightarrow{\ \phi_1(g)\ } & S_1 \\ {\scriptstyle\sigma}\big\downarrow & & \big\downarrow{\scriptstyle\sigma} \\ S_2 & \xrightarrow[\ \phi_2(\iota(g))\ ]{} & S_2 \end{array}$$

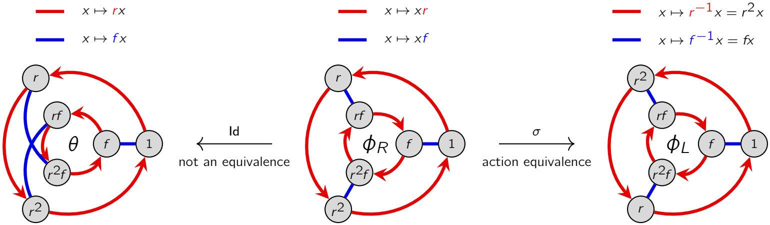
Action equivalence can be used to show that in our binary square example, we could have:

- defined $\phi(r)$ to rotate clockwise, and $\phi(f)$ to flip vertically
- used tiles with a and b, rather than 0 and 1
- read from right-to-left, rather than left-to-right, etc.

Every right action has an equivalent left action

G acting on...	right action	equivalent left action
itself by multiplication	$x \mapsto xg$	$x \mapsto g^{-1}x$
itself by conjugation	$x \mapsto g^{-1}xg$	$x \mapsto gxg^{-1}$
its subgroups by conjugation	$H \mapsto g^{-1}Hg$	$H \mapsto gHg^{-1}$
cosets by multiplication	$H \mapsto Hg$	$H \mapsto g^{-1}H$

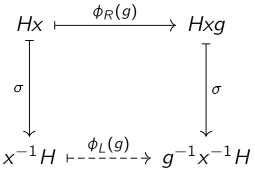


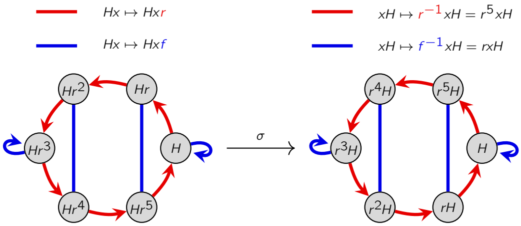


Every right action has an equivalent left action

G acting on...	right action	equivalent left action
itself by multiplication	$x \mapsto xg$	$x \mapsto g^{-1}x$
itself by conjugation	$x \mapsto g^{-1}xg$	$x \mapsto gxg^{-1}$
its subgroups by conjugation	$H \mapsto g^{-1}Hg$	$H \mapsto gHg^{-1}$
cosets by multiplication	$H \mapsto Hg$	$H \mapsto g^{-1}H$

Recall that $aH = bH$ implies $Ha^{-1} = Hb^{-1}$.





Since $aH = bH \not\Rightarrow Ha = Hb$, the the map $xH \mapsto Hx$ is not even well-defined.

Left and right actions of permutations

Recall the two "canonical" ways label a Cayley graph for $S_3 = \langle (12), (23) \rangle$ with the set

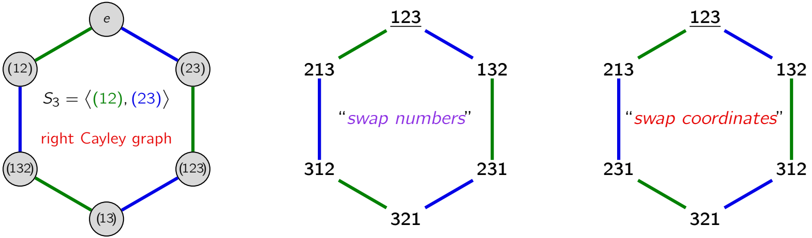
$$S = \{\mathbf{123}, \mathbf{132}, \mathbf{213}, \mathbf{231}, \mathbf{312}, \mathbf{321}\}.$$

In one, (ij) can be interpreted to mean

"*swap the numbers in the* i^{th} *and* j^{th} *coordinates*."

Alternatively, (ij) could mean

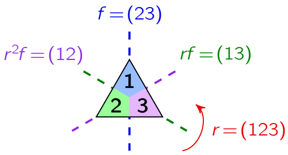
"*swap the numbers* i *and* j*, regardless of where they are*."



One of these is a left group action, and the other a right group action.

Left and right actions of permutations

Canonically associate elements of D_3 with S_3 via an isomorphism:



which acts on $S = \{\mathbf{123}, \mathbf{132}, \mathbf{213}, \mathbf{231}, \mathbf{312}, \mathbf{321}\}$

where

- "*pressing the r-button*" cyclically shifts the entries to the right,
- "*pressing the f-button*" transposes the last two entries (coordinates):

$$\pi(1)\pi(2)\pi(3) \overset{\phi(r)}{\longmapsto} \pi(3)\pi(1)\pi(2), \qquad \pi(1)\pi(2)\pi(3) \overset{\phi(f)}{\longmapsto} \pi(1)\pi(3)\pi(2).$$

This defines a *right action*, by the homomorphism

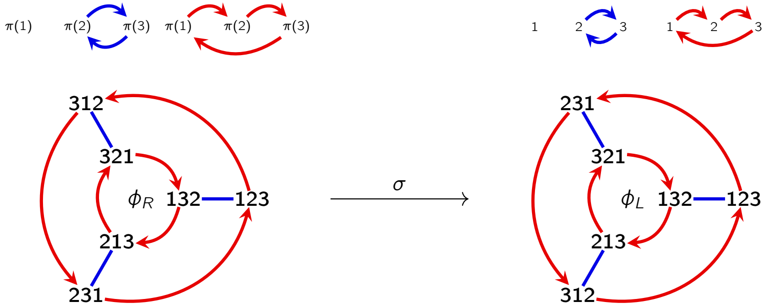
$$\phi_R \colon S_3 \longrightarrow \mathrm{Perm}(S), \qquad \phi_R(\tau) \colon \pi(1)\pi(2)\pi(3) \longmapsto \pi(\tau(1))\pi(\tau(2))\pi(\tau(3)).$$

The equivalent left action *permutes numbers*, rather than entries

$$\phi_L \colon S_3 \longrightarrow \mathrm{Perm}(S), \qquad \phi_L(\tau) \colon \pi(1)\pi(2)\pi(3) \longmapsto \tau^{-1}(\pi(1))\tau^{-1}(\pi(2))\tau^{-1}(\pi(3)).$$

Left and right actions of permutations

right action "*permutes positions*" left action "*permutes numbers*"



$$\pi(1)\pi(2)\pi(3) = \mathbf{312} \xmapsto{\ \phi_R(\tau)\ } \pi(\tau(1))\pi(\tau(2))\pi(\tau(3)) = \mathbf{321}$$

$$\downarrow \sigma \qquad\qquad\qquad\qquad \downarrow \sigma$$

$$\pi^{-1}(1)\pi^{-1}(2)\pi^{-1}(3) = \mathbf{231} \overset{\phi_L(\tau)}{\dashrightarrow} \tau^{-1}(\pi^{-1}(1))\tau^{-1}(\pi^{-1}(2))\tau^{-1}(\pi^{-1}(3)) = \mathbf{321}$$

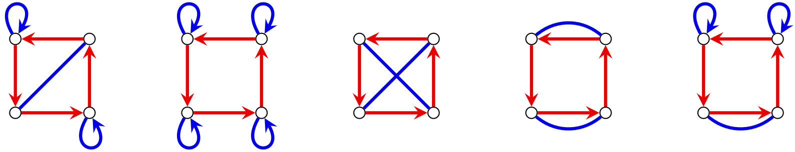
Classification of action graphs

Natural question

Given a group G, what are its possible action graphs?

Note that it suffices to consider individual orbits separately.

For example, which of the following can arise as an orbit of an action by $G = D_4$?



Definition

An action $\phi \colon G \to \mathrm{Perm}(S)$ is

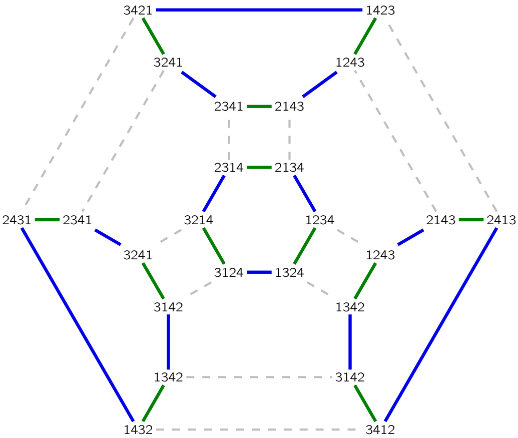
- transitive if it has only one orbit: ("*graph is connected*")
- free if $\mathrm{stab}(s) = \langle e \rangle$ for all $s \in S$. ("*uncollapsed – no nontrivial loops*")

In this language our question becomes: "*classify all transitive actions by G.*"

An example of a free action that is not transitive

The group $S_3 = \langle (12), (23) \rangle$ acts on permutations **1234**, via $\phi \colon S_3 \to \mathrm{Perm}(S)$, where

- $\phi((12))$ = the permutation that swaps the 1st and 2nd coordinates
- $\phi((23))$ = the permutation that swaps the 2nd and 3rd coordinates

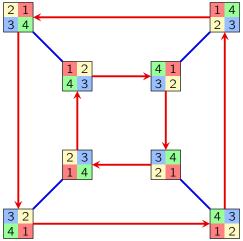


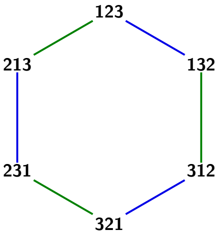
Simply transitive actions

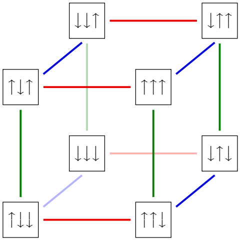
Definition

An action $\phi \colon G \to \mathrm{Perm}(S)$ is simply transitive if it is transitive and free.

Here are some simply transitive actions that we have seen.







What do you notice about these action graphs?

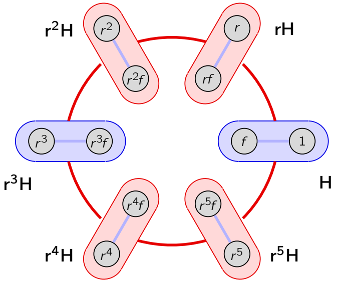
Proposition

Every simply transitive G-action is equivalent to G acting on itself by multiplication.

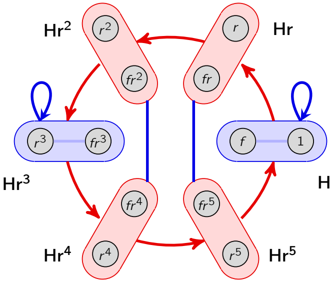
Transitive actions

All transtive actions can be constructed by collapsing Cayley graphs.

But what to collapse? Recall the bijection between nodes in orb(s) and cosets of stab(s).



collapse left cosets of H (not an action)



collapse right cosets of H (an action)

Proposition

Every transitive G-action is equivalent to G acting on a set of cosets by multplication.

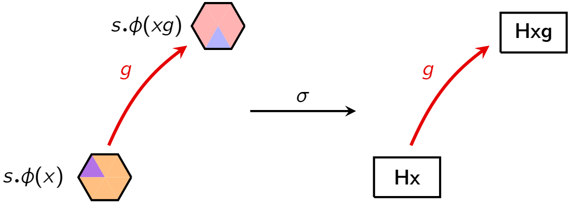
Transitive actions

Proposition

Every transitive G-action is equivalent to G acting on a set of cosets by multplication.

Proof sketch. Let $\iota\colon G \to G$ be the identity, fix $s \in S$, let $H = \mathrm{stab}(s)$, and define

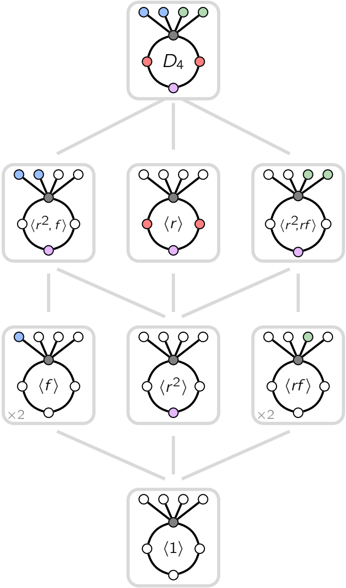
$$\sigma\colon S \longrightarrow H\backslash G, \qquad \sigma\colon s.\phi(x) \longmapsto Hx$$

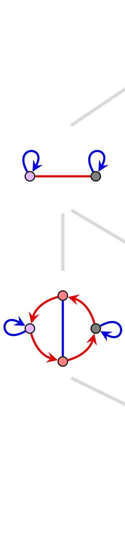


Show that σ is a well-defined bijection, and then the proof follows because:

$$\begin{array}{ccc} S & \xrightarrow{\phi(g)} & S \\ \sigma\downarrow & & \downarrow\sigma \\ H\backslash G & \xrightarrow[\psi(g)]{} & H\backslash G \end{array} \qquad \begin{array}{ccc} s.\phi(x) & \xrightarrow{\phi(g)} & s.\phi(xg) \\ \sigma\downarrow & & \downarrow\sigma \\ Hx & \xmapsto[\psi(g)]{} & Hxg \end{array}$$

The transitive actions of D_4: collapsing by right cosets

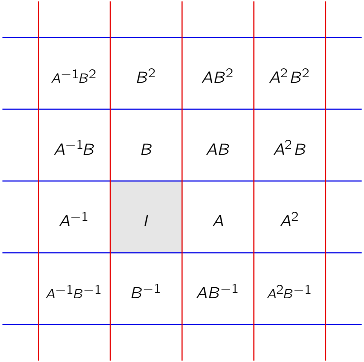


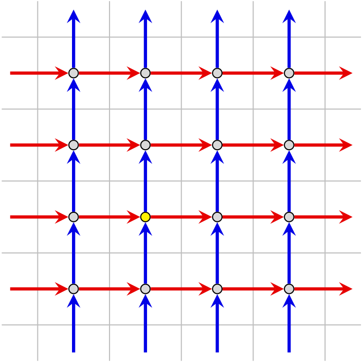


Simply transitive actions from finite reflection groups

One place where simply transitive actions arise is from tilings.

The group $\langle A, B \mid AB = BA \rangle \cong \mathbb{Z} \times \mathbb{Z}$ acts simply transitively on the unit squares in $\mathbb{Z}^2$.

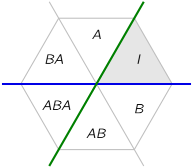




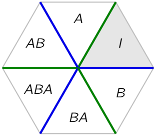
The shaded region is called a **fundamental chamber**.

Simply transitive actions from finite reflection groups

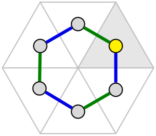
The dihedral group $D_3 = \langle A, B \mid A^2 = B^2 = (AB)^3 = 1 \rangle$ acts simply transitively on the six regions of a hexagon.



"*left action*"

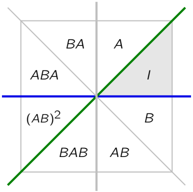


"*right action*"

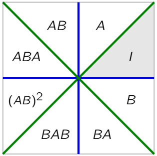


"*(right) Cayley graph*"

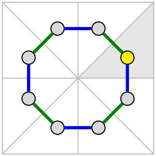
The dihedral group D_4 acts simply transitively on the eight regions of a square.



"*left action*"



"*right action*"

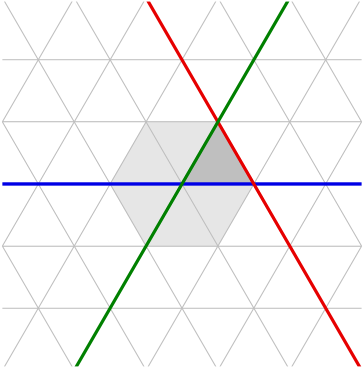


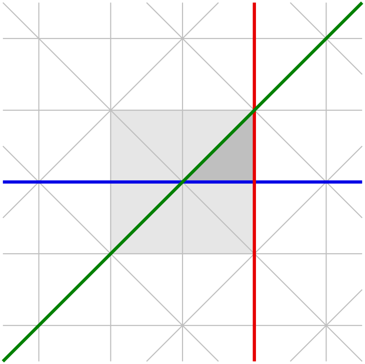
"*(right) Cayley graph*"

Simply transitive actions from finite reflection groups

In both previous examples, adding a third reflection generates a tiling of the plane.

The resulting affine groups, $\mathsf{Aff}(D_3)$ and $\mathsf{Aff}(D_4)$, act simply transitively on the chambers.

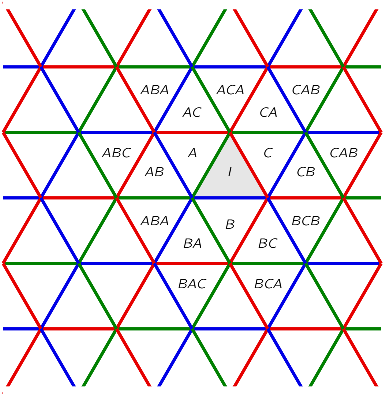


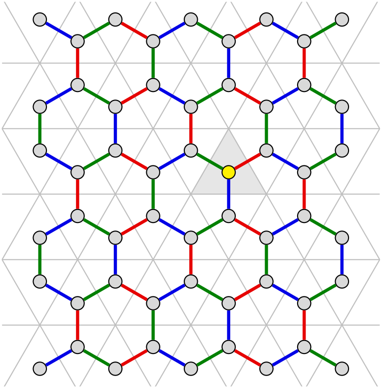


Simply transitive actions and affine Weyl groups

The group $\mathsf{Aff}(D_3)$ is better known as the affine Weyl group of type A_2.

It acts simply transitively on the chambers of the following tiling of $\mathbb{R}^2$.





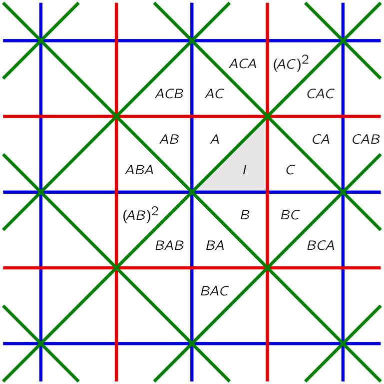
It has presentation

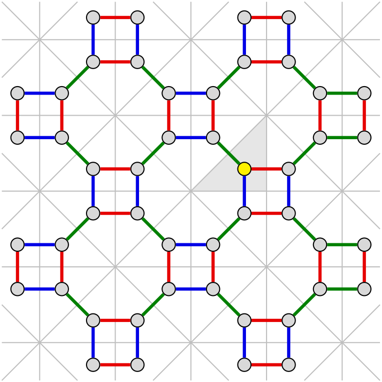
$$W(\tilde{A}_2) = \mathsf{Aff}(D_3) = \langle A, B \mid A^2 = B^2 = C^2 = (AB)^3 = (AC)^3 = (BC)^3 = 1 \rangle.$$

Simply transitive actions and affine Weyl groups

The group $\mathrm{Aff}(D_4)$ is better known as the affine Weyl group of type C_2.

It acts simply transitively on the chambers of the following tiling of $\mathbb{R}^2$.





It has presentation

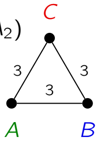
$$W(\tilde{C}_2) = \mathrm{Aff}(D_4) = \langle A, B \mid A^2 = B^2 = C^2 \mid (AB)^4 = (AC)^4 = (BC)^2 = 1 \rangle.$$

Weyl groups and Dynkin diagrams

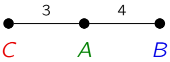
The presentations of the affine Weyl groups are encoded by Dynkin diagrams.

Nodes s_i are generators, and the labeled edges m_{ij} describe relations: $(s_i s_j)^{m_{ij}} = 1$.

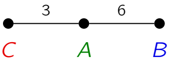
$\mathrm{Aff}(D_3) = W(\tilde{A}_2)$



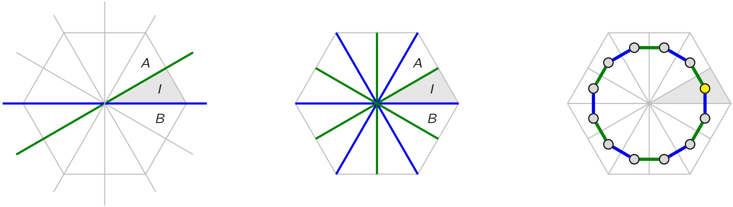
$\mathrm{Aff}(D_4) = W(\tilde{C}_2)$



$\mathrm{Aff}(D_6) = W(\tilde{G}_2)$



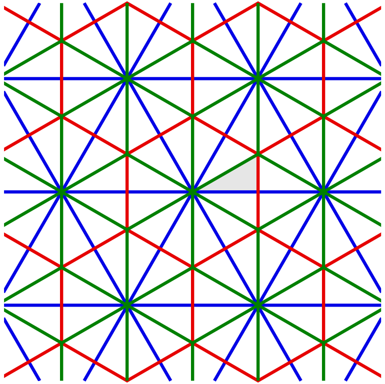
This last example is the affine version of $D_6 = \langle A, B \mid A^2 = B^2 = (AB)^6 = 1 \rangle$ acting simply transitively on the 12 regions of a hexagon.

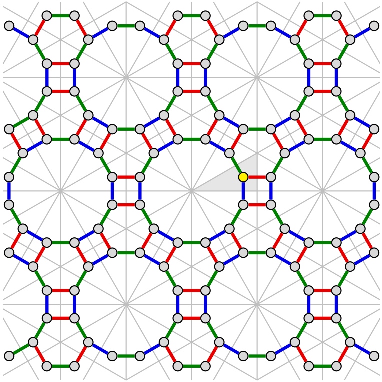


One last affine Weyl group

The group Aff(D_6) is better known as the the affine Weyl group of type G_2.

It acts simply transitively on the chambers of the following tiling of $\mathbb{R}^2$.





It has presentation

$$W(\tilde{G}_2) = \text{Aff}(D_6) = \langle A, B, C \mid A^2 = B^2 = C^2 = (AB)^6 = (AC)^3 = (BC)^2 = 1 \rangle.$$

Coxeter groups and tilings of hyperbolic space

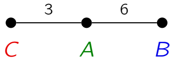
A Coxeter group is a group generated by "reflections", with presentation

$$W = \langle s_1, \dots, s_n \mid s_i^2 = 1,\ (s_i s_j)^{m_{ij}} = 1 \rangle.$$

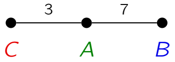
Like Weyl groups, this can be encoded by a Coxeter graph.

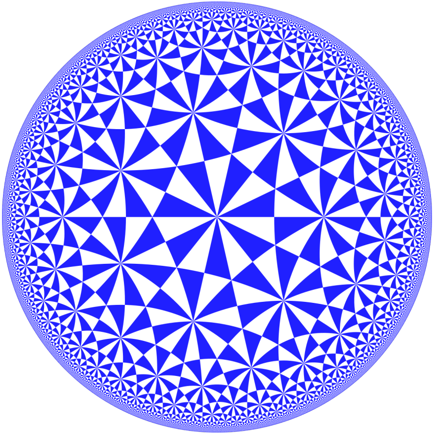
Some Coxeter groups act simply transitively on chambers of hyperbolic tilings.

$\mathrm{Aff}(D_6) = W(\tilde{G}_2)$



A hyperbolic Coxeter group





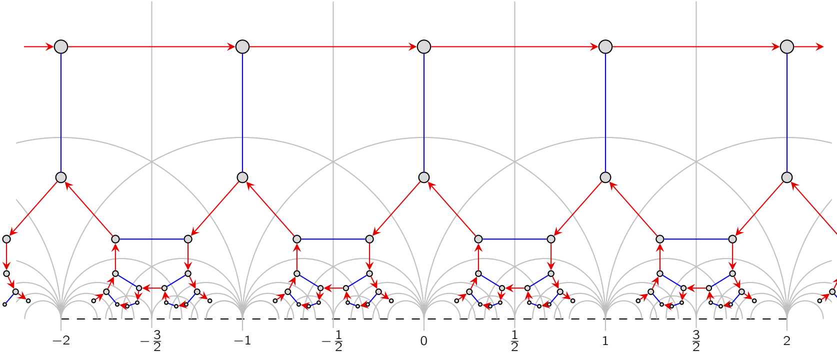
A simply transitive action of $PSL_2(\mathbb{Z})$

The projective special linear group

$$PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\langle -I \rangle, \qquad \text{where } SL_2(\mathbb{Z}) = \Bigg\langle \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{S}, \underbrace{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}}_{T} \Bigg\rangle$$

defines a tiling of hyperbolic ideal triangles in the upper half-plane via

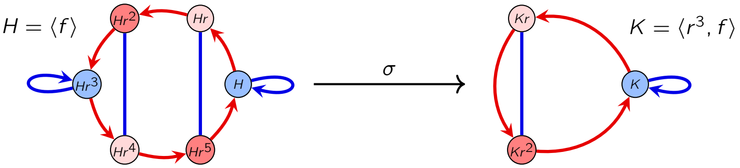
$$S \colon z \longmapsto \frac{0z-1}{z+0} = -\frac{1}{z}, \qquad \text{and} \qquad T \colon z \longmapsto \frac{z+1}{0z+1} = z+1.$$



Equivariance

Next, we'll study equivariance: structure-preserving maps between two different actions.

Consider this example of action graphs from $G = D_6$ acting on cosets:



This can be described by the following commutative diagram:

$$\begin{array}{ccc} H\backslash G & \xmapsto{\phi(g)} & H\backslash G \\ \sigma \big\downarrow & & \big\downarrow \sigma \\ K\backslash G & \xmapsto{\phi(g)} & K\backslash G \end{array} \qquad\qquad \begin{array}{ccc} Hx & \xmapsto{\phi(g)} & Hxg \\ \sigma \big\downarrow & & \big\downarrow \sigma \\ Kx & \xmapsto{\phi(g)} & Kxg \end{array}$$

Key idea

We say that "*the map σ commutes with the action of the group*."

Equivariant maps and bijections

Key idea

(Action) equivalence is to equivariance, as (group) isomorphisms are to homomorphisms.

Definition

Suppose G acts on S_i via $\phi_i \colon G \to \mathbf{Perm}(S_i)$ for $i = 1, 2$. A **G-equivariant map** is a surjection $\sigma \colon S_1 \to S_2$ such that $\sigma \circ \phi_1(g) = \phi_2(g) \circ \sigma$, for all $g \in G$:

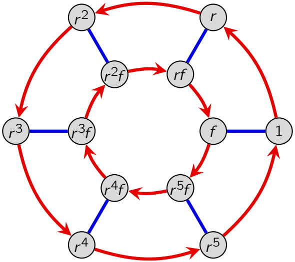
$$\begin{array}{ccc} S_1 & \xrightarrow{\ \phi_1(g)\ } & S_1 \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ S_2 & \xrightarrow{\ \phi_2(g)\ } & S_2 \end{array} \qquad\qquad \begin{array}{ccc} s_1 & \xmapsto{\ \phi_1(g)\ } & s_1.\phi_1(g) \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ s_2 & \xmapsto{\ \phi_2(g)\ } & s_2.\phi_2(g) \end{array}$$

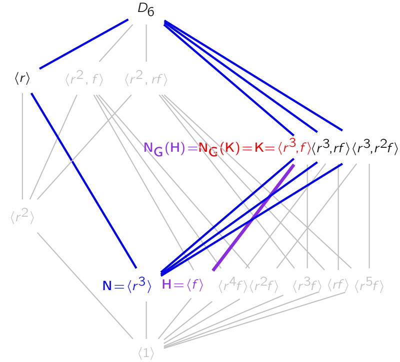
If $S := S_1 = S_2$, then G-equivariant maps are called G-equivariant bijections.

They define a group, $\mathbf{Aut}_G(S)$. We'll usually study $\mathbf{Aut}(G)(H\backslash G)$, for some $H \leq G$.

These can be thought of as action graph symmetries. (*not* "rewirings"!)

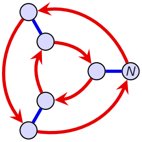
Equivariant bijections





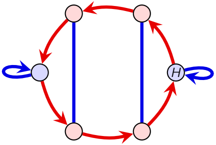
What do you notice about normalizers vs. symmetries of the actions graphs?

$N=\langle r^3\rangle$; *normal*



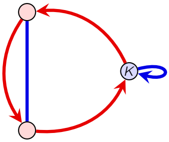
$\text{Aut}_G(N\backslash G)\cong D_3\cong N_G(N)/N$

$H=\langle f\rangle$; *moderately unnormal*



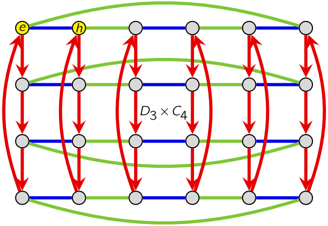
$\text{Aut}_G(H\backslash G)\cong C_2\cong N_G(H)/H$

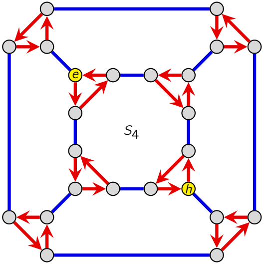
$K=\langle r^3,f\rangle$; *fully unnormal*

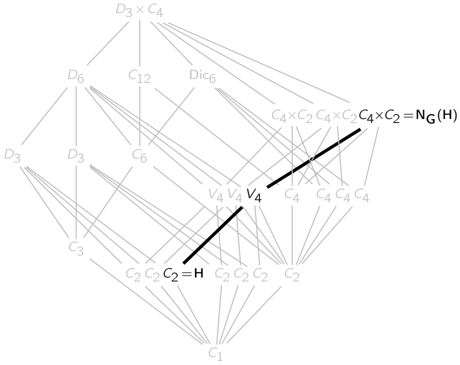


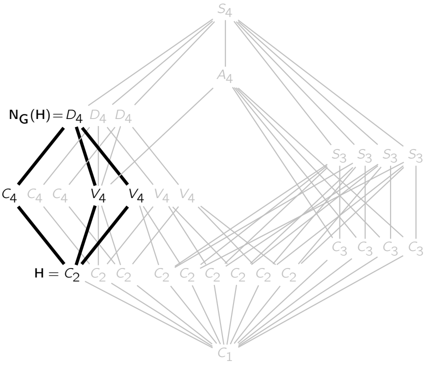
$\text{Aut}_G(K\backslash G)\cong \langle 1\rangle\cong N_G(K)/K$

Equivariant bijections

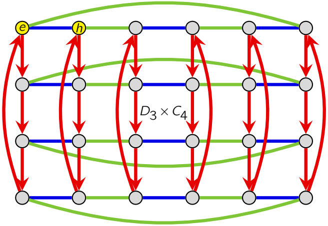


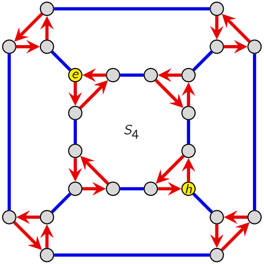






Equivariant bijections



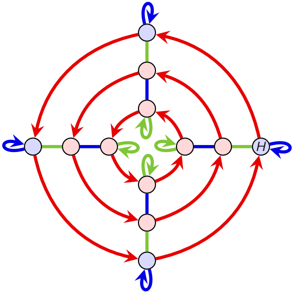


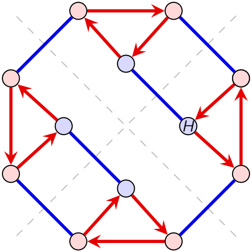
$H = \langle (f,1) \rangle \leq D_3 \times C_4 = G$

$\mathrm{Aut}_G(H \backslash G) \cong N_G(H)/H \cong C_4$

$H = \langle ((12)(34)) \rangle \leq S_4 = G$

$\mathrm{Aut}_G(H \backslash G) \cong N_G(H)/H \cong V_4$





Equivariant bijections: the main result

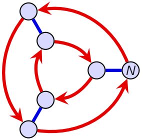
Theorem

If G acts on the set $S = H\backslash G$ of right cosets of $H \leq G$, then

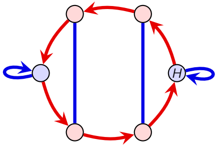
$$\mathrm{Aut}_G(H\backslash G) \cong N_G(H)/H.$$

Here's how the proof will go, given $\sigma \in \mathrm{Aut}_G(H\backslash G)$:

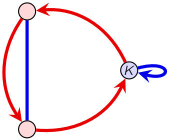
1. **Lemma 1**: $\sigma\colon Hg \mapsto Hxg$, for some fixed $x \in G$ (i.e., $\sigma = \phi(x)$).
2. **Lemma 2**: $\phi(x) \in \mathrm{Aut}_G(H\backslash G)$ iff $x \in N_G(H)$. That is, $\sigma\colon Hg \mapsto xHg$.
3. **FHT**: Two $\phi(x) = \phi(x')$ iff x, x' are in the same coset of H.



$\mathrm{Aut}_G(N\backslash G) \cong N_G(N)/N \cong D_3$



$\mathrm{Aut}_G(H\backslash G) \cong N_G(H)/H \cong C_2$



$\mathrm{Aut}_G(K\backslash G) \cong N_G(K)/K \cong \langle 1\rangle$

Equivariant bijections

Lemma 1

Let $\sigma \in \mathrm{Aut}_G(H\backslash G)$. Then σ is determined by the image of H:

$$\text{if } \sigma\colon H \mapsto Hx, \quad \text{then} \quad \sigma\colon Hg \mapsto Hxg, \text{ for all } g \in G.$$

Proof

Since σ is G-equivariant, it commutes with each $\phi(g) \in \mathrm{Perm}(H\backslash G)$.

That is, the following diagram commutes:

$$\begin{array}{ccc} H\backslash G & \xmapsto{\ \phi(g)\ } & H\backslash G \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ H\backslash G & \xmapsto{\ \phi(g)\ } & H\backslash G \end{array} \qquad\qquad \begin{array}{ccc} H & \xmapsto{\ \phi(g)\ } & Hg \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ Hx & \xmapsto{\ \phi(g)\ } & Hxg \end{array}$$

It follows that $\sigma\colon Hg \mapsto Hxg$, as claimed. □

Equivariant bijections

Lemma 2

The bijection of right cosets

$$\phi(x)\colon H\backslash G \longrightarrow H\backslash G, \qquad \phi(x)\colon Hg \longmapsto Hgx$$

is G-equivariant iff $x \in N_G(H)$.

Proof

"$\Rightarrow$": Suppose $\phi(x) \in \mathrm{Aut}_G(H\backslash G)$, and take $h \in H$. We have:

$$\begin{array}{ccc} H\backslash G & \xrightarrow{\ \phi(h)\ } & H\backslash G \\ {\scriptstyle \phi(x)}\downarrow & & \downarrow{\scriptstyle \phi(x)} \\ H\backslash G & \xrightarrow{\ \phi(h)\ } & H\backslash G \end{array} \qquad\qquad \begin{array}{ccc} H & \xmapsto{\ \phi(h)\ } & H \\ {\scriptstyle \phi(x)}\downarrow & & \downarrow{\scriptstyle \phi(x)} \\ Hx & \xmapsto{\ \phi(h)\ } & Hxh = Hx \end{array}$$

That is, for every $h \in H$,

$$H = Hxhx^{-1} \quad \Leftrightarrow \quad xhx^{-1} \in H \quad \Leftrightarrow \quad x \in N_G(H). \qquad \checkmark$$

Equivariant bijections

Lemma 2

The bijection of right cosets

$$\phi(x)\colon H\backslash G \longrightarrow H\backslash G, \qquad \phi(x)\colon Hg \longmapsto Hgx$$

is G-equivariant iff $x \in N_G(H)$.

Proof

"$\Leftarrow$": Suppose $x \in N_G(H)$, and pick $g \in G$.

We need to show that $\phi(x)$ and $\phi(g)$ in $\mathrm{Perm}(H\backslash G)$ commute.

By Lemma 1: $\phi(x)\colon Hg \mapsto Hxg = xHg$.

The operations of left-multiplying by x, and right-multiplying by g commute. ✓

$$\begin{array}{ccc} H\backslash G & \xmapsto{\ \phi(g)\ } & H\backslash G \\ {\scriptstyle \phi(x)}\big\downarrow & & \big\downarrow{\scriptstyle \phi(x)} \\ H\backslash G & \xmapsto{\ \phi(g)\ } & H\backslash G \end{array} \qquad\qquad \begin{array}{ccc} H & \xmapsto{\ \phi(g)\ } & Hg \\ {\scriptstyle \phi(x)}\big\downarrow & & \big\downarrow{\scriptstyle \phi(x)} \\ Hx & \xmapsto{\ \phi(g)\ } & Hxg = xHg \end{array}$$

Equivariant bijections: the main result

Theorem

If G acts on the set $S = H\backslash G$ of right cosets of $H \leq G$, then

$$\mathrm{Aut}_G(H\backslash G) \cong N_G(H)/H.$$

Proof

We'll apply the FHT to the map

$$\phi\colon N_G(H) \longrightarrow \mathrm{Aut}_G(H\backslash G), \qquad x \longmapsto \phi(x) \in \mathrm{Perm}(H\backslash G),$$

where $\phi(x)\colon Hg \longmapsto Hgx$.

Homomorphism: this is the restriction of the action $\phi\colon G \to \mathrm{Perm}(H\backslash G)$ to $N_G(H)$. ✓

Onto: Immediate from Lemma 2. ✓

$\mathrm{Ker}(\phi) = H$. "$\subseteq$": Set $g = 1$ in the following:

$$x \in \mathrm{Ker}(\phi) \quad \Leftrightarrow \quad Hg = Hgx,\ \forall\, g \in G \quad \Leftrightarrow \quad H = Hgxg^{-1},\ \forall\, g \in G.$$

"$\supseteq$": If $h \in H$, then $\phi(h)\colon Hg \mapsto hHg = Hg$. ✓

The result now follows from the FHT. □

A creative application of a group action

Cauchy's theorem

If p is a prime dividing $|G|$, then G has an element (and hence a subgroup) of order p.

Proof

Let P be the set of ordered p-tuples of elements from G whose product is e:

$$(x_1, x_2, \dots, x_p) \in P \quad \text{iff} \quad x_1 x_2 \cdots x_p = e\,.$$

Observe that $|P| = |G|^{p-1}$. (We can choose $x_1, \dots, x_{p-1}$ freely; then x_p is forced.)

The group $\mathbb{Z}_p$ acts on P by cyclic shift:

$$\phi \colon \mathbb{Z}_p \longrightarrow \text{Perm}(P), \qquad (x_1, x_2, \dots, x_p) \xrightarrow{\phi(1)} (x_2, x_3 \dots, x_p, x_1)\,.$$

The set P is partitioned into orbits, each of size $|\,\mathbf{orb}(s)| = [\mathbb{Z}_p : \mathbf{stab}(s)] = 1$ or p.

The only way that the orbit of $(x_1, x_2, \dots, x_p)$ can have size 1 is if $x_1 = \cdots = x_p$.

Clearly, $(e, \dots, e) \in P$ is a fixed point.

The $|G|^{p-1} - 1$ other elements in P sit in orbits of size 1 or p.

Since $p \nmid |G|^{p-1} - 1$, there must be other orbits of size 1. Thus, some $(x, \dots, x) \in P$, with $x \neq e$ satisfies $x^p = e$. $\square$

p-groups and the Sylow theorems

Definition

A *p-group* is a group whose order is a power of a prime p. A p-group that is a subgroup of a group G is a *p-subgroup* of G.

Notational convention

Throughout, G will be a group of order $|G| = p^n \cdot m$, with $p \nmid m$. That is, p^n is the *highest power* of p dividing $|G|$.

There are three Sylow theorems, and loosely speaking, they describe the following about a group's p-subgroups:

1. **Existence**: In every group, p-subgroups of all possible sizes exist.
2. **Relationship**: All maximal p-subgroups are conjugate.
3. **Number**: Strong restrictions on the number of p-subgroups a group can have.

Together, these place strong restrictions on the structure of a group G with a fixed order.

p-groups

Before we introduce the Sylow theorems, we need to better understand p-groups.

Recall that a p-group is any group of order p^n. Examples, of 2-groups that we've seen include C_1, C_4, V_4, D_4 and Q_8, C_8, $C_4 \times C_2$, D_8, SD_8, Q_{16}, SA_8, $\mathrm{Pauli}_1, \dots$

p-group Lemma

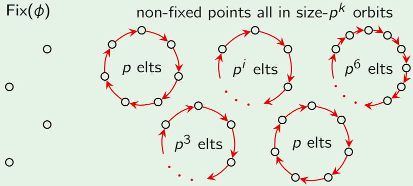
If a p-group G acts on a set S via $\phi \colon G \to \mathrm{Perm}(S)$, then

$$|\,\mathrm{Fix}(\phi)| \equiv_p |S|.$$

Proof (sketch)

Suppose $|G| = p^n$.

By the orbit-stabilizer theorem, the only possible orbit sizes are $1, p, p^2, \dots, p^n$.



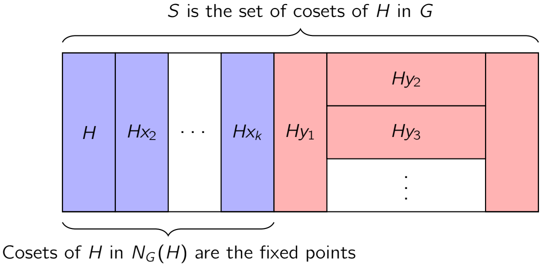
Normalizer lemma, Part 1

If H is a p-subgroup of G, then

$$[N_G(H) \colon H] \equiv_p [G \colon H] \, .$$

Approach:

- Let H (not G!) act on the (right) cosets of H by (right) multiplication.



- Apply our lemma: $|\operatorname{Fix}(\phi)| \equiv_p |S|$.

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

$$[N_G(H)\colon H] \equiv_p [G\colon H]\,.$$

Proof

Let $S = H\backslash G = \{Hx \mid x \in G\}$. The group H acts on S by **right-multiplication**, via $\phi\colon H \to \mathsf{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } Hx \text{ to } Hxh.$$

The fixed points of ϕ are the cosets Hx in the normalizer $N_G(H)$:

$$\begin{aligned} Hxh = Hx, \quad \forall h \in H \qquad &\Longleftrightarrow \qquad Hxhx^{-1} = H, \quad \forall h \in H \\ &\Longleftrightarrow \qquad xhx^{-1} \in H, \quad \forall h \in H \\ &\Longleftrightarrow \qquad x \in N_G(H)\,. \end{aligned}$$

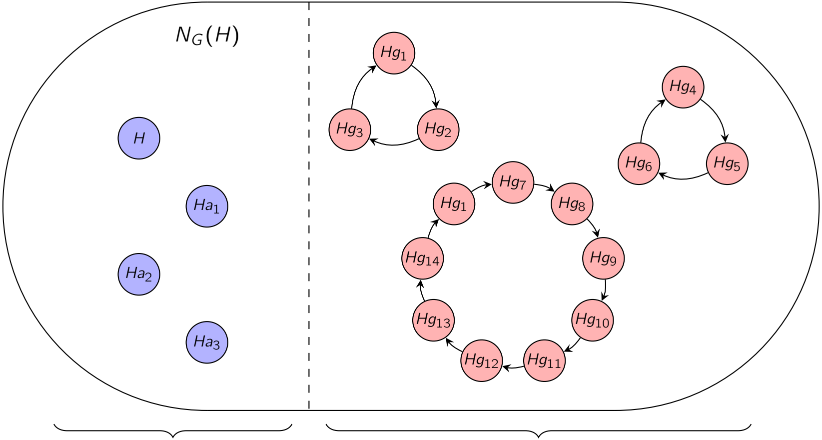
Therefore, $|\,\mathrm{Fix}(\phi)| = [N_G(H)\colon H]$, and $|S| = [G : H]$. By our p-group Lemma,

$$|\,\mathrm{Fix}(\phi)| \equiv_p |S| \quad \Longrightarrow \quad [N_G(H)\colon H] \equiv_p [G\colon H]\,. \qquad \square$$

p-groups

Here is a picture of the action of the p-subgroup H on the set $S = H\backslash G$, from the proof of the normalizer lemma.

$S = H\backslash G =$ set of right cosets of H in G



The fixed points are precisely the cosets in $N_G(H)$

Orbits of size > 1 are of various sizes dividing $|H|$, but all lie outside $N_G(H)$

p-subgroups

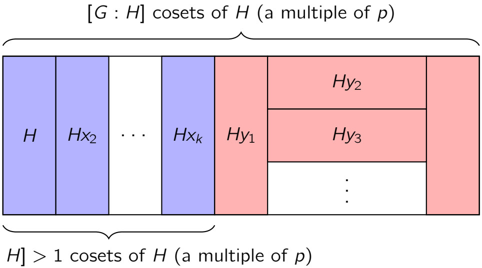
Recall that $H \leq N_G(H)$ (always), and H is fully unnormal if $H = N_G(H)$.

Normalizer lemma, Part 2

Suppose $|G| = p^n m$, and $H \leq G$ with $|H| = p^i < p^n$. Then $H \lneq N_G(H)$, and the index $[N_G(H) : H]$ is a multiple of p.

H is not "*fully unnormal*":

$H \lneq N_G(H) \leq G$



Important corollaries

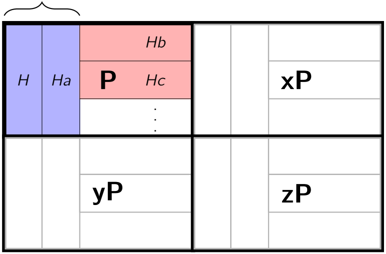
- p-groups cannot have any fully unnormal subgroups (i.e., $H \lneq N_G(H)$).
- In *any* finite group, the only fully unnormal p-subgroups are maximal.

Normalizers of p-subgroups

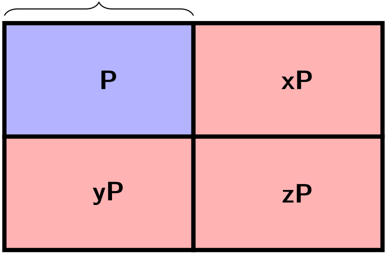
Let H be properly contained in a maximal p-subgroup $P \lneq G$.

- The normalizer of H *must* grow in P (and hence in G)
- The normalizer of P *need not* grow in G.

$H \lneq N_P(H) \leq N_G(H)$



it may happen that $P = N_G(P)$



Proof of the normalizer lemma

Normalizer lemma, Part 2

Suppose $|G| = p^n m$, and $H \leq G$ with $|H| = p^i < p^n$. Then $H \lneq N_G(H)$, and the index $[N_G(H) : H]$ is a multiple of p.

Proof

Since $H \trianglelefteq N_G(H)$, we can create the quotient map

$$q \colon N_G(H) \longrightarrow N_G(H)/H\,, \qquad\qquad q \colon g \longmapsto gH\,.$$

The size of the quotient group is $[N_G(H) \colon H]$, the number of cosets of H in $N_G(H)$.

By the normalizer lemma Part 1, $[N_G(H) \colon H] \equiv_p [G \colon H]$. By Lagrange's theorem,

$$[N_G(H) \colon H] \equiv_p [G \colon H] = \frac{|G|}{|H|} = \frac{p^n m}{p^i} = p^{n-i} m \equiv_p 0\,.$$

Therefore, $[N_G(H) \colon H]$ is a multiple of p, so $N_G(H)$ must be strictly larger than H. □

The Sylow theorems

Recall the following question that we asked earlier in this course.

Open-ended question

What group structural properties are possible, what are impossible, and how does this depend on $|G|$?

One approach is to decompose large groups into "building block subgroups." For example:

> *given a group of order* $72 = 2^3 \cdot 3^2$, *what can we say about its* 2*-subgroups and* 3*-subgroups?.*

This is the idea behind the Sylow theorems, developed by Norwegian mathematician Peter Sylow (1832–1918).

The Sylow theorems address the following questions of a finite group G:

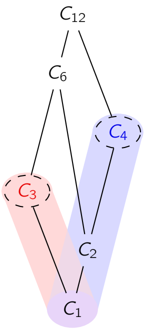
1. How big are its p-subgroups?
2. How are the p-subgroups related?
3. How many p-subgroups are there?
4. Are any of them normal?

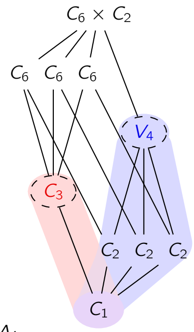
An example: groups of order 12

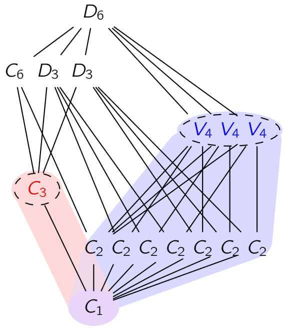
The Sylow theorems can be used to classify all groups of order 12.

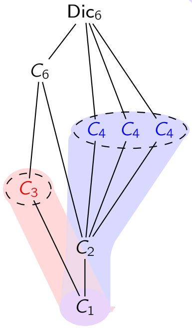
We've already seen them all.

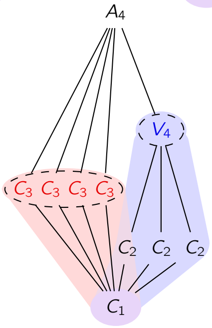
What patterns do you notice about the 2-groups and 3-groups, that might generalize to all p-subgroups?











The Sylow theorems

Notational convention

Througout, G will be a group of order $|G| = p^n \cdot m$, with $p \nmid m$.

That is, p^n is the *highest power* of p dividing $|G|$.

A subgroup of order p^n is called a Sylow p-subgroup.

Let $\text{Syl}(G)$ denote the set of Sylow subgroups, and $n_p := \big|\text{Syl}(G)\big|$.

There are three Sylow theorems, and loosely speaking, they describe the following about a group's p-subgroups:

1. **Existence**: In every group, p-subgroups of all possible sizes exist, and they're "*nested*".
2. **Relationship**: All maximal p-subgroups are conjugate.
3. **Number**: There are strong restrictions on n_p, the number of Sylow p-subgroups.

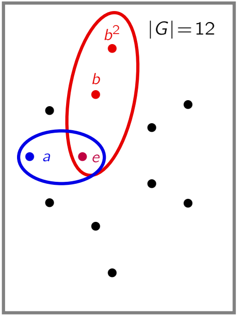
Together, these place strong restrictions on the structure of a group G with a fixed order.

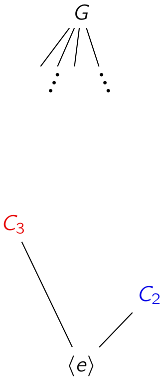
Our unknown group of order 12

Throughout, we will have a running example, a "mystery group" G of order $12 = 2^2 \cdot 3$.

We already know a little bit about G. By Cauchy's theorem, it must have:

- an element a of order 2, and
- an element b of order 3.





Using *only* the fact that $|G| = 12$, we will unconver as much about its structure as we can.

The 1^{st} Sylow theorem: existence of p-subgroups

First Sylow theorem

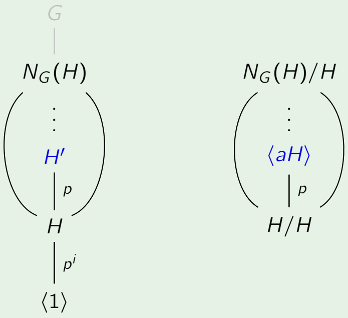
G has a subgroup of order p^k, for each p^k dividing $|G|$.

Also, every non-Sylow p-subgroup sits inside a larger p-subgroup.

Proof

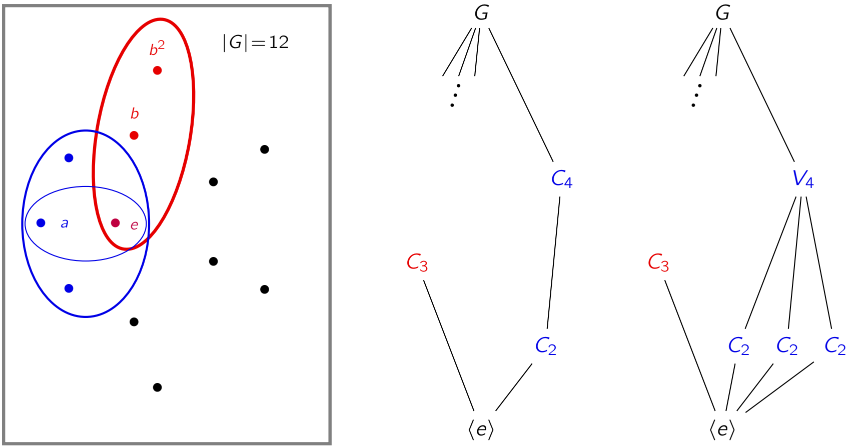
Take any $H \leq G$ with $|H| = p^i < p^n$. We know $H \trianglelefteq N_G(H)$ and p divides $|N_G(H)/H|$.

Find an element aH of order p. The union of cosets in $\langle aH \rangle$ is a subgroup of order p^{i+1}.



Our unknown group of order 12

By the first Sylow theorem, $\langle a \rangle$ is contained in a subgroup of order 4, which could be V_4 or C_4, or possibly both.



The 2^{nd} Sylow theorem: relationship among p-subgroups

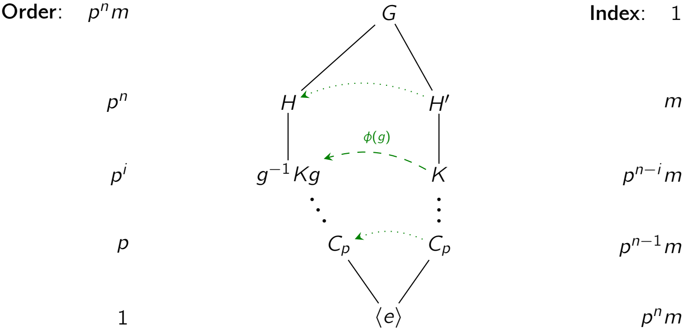
Second Sylow theorem

Any two Sylow p-subgroups are conjugate (and hence isomorphic).

We'll actually prove a stronger version, which easily implies the 2nd Sylow theorem.

Strong second Sylow theorem

Let $H \in \text{Syl}(G)$, and $K \le G$ any p-subgroup. Then K is conjugate to a subgroup of H.



The 2nd Sylow theorem: All Sylow p-subgroups are conjugate

Strong second Sylow theorem

Let H be a Sylow p-subgroup, and $K \leq G$ any p-subgroup. Then K is conjugate to some subgroup of H.

Proof

Let $S = H\backslash G = \{Hg \mid g \in G\}$, the set of right cosets of H.

The group K acts on S by **right-multiplication**, via $\phi \colon K \to \mathrm{Perm}(S)$, where

$$\phi(k) = \text{the permutation sending each } Hg \text{ to } Hgk.$$

A fixed point of ϕ is a coset $Hg \in S$ such that

$$\begin{aligned} Hgk = Hg\,, \quad \forall k \in K \qquad &\Longleftrightarrow \qquad Hgkg^{-1} = H\,, \quad \forall k \in K \\ &\Longleftrightarrow \qquad gkg^{-1} \in H\,, \quad \forall k \in K \\ &\Longleftrightarrow \qquad gKg^{-1} \subseteq H. \end{aligned}$$

Thus, *if we can show that ϕ has a fixed point Hg, we're done!*

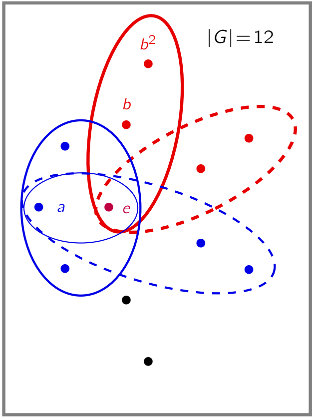
All we need to do is show that $|\,\mathrm{Fix}(\phi)| \not\equiv_p 0$. By the p-group Lemma,

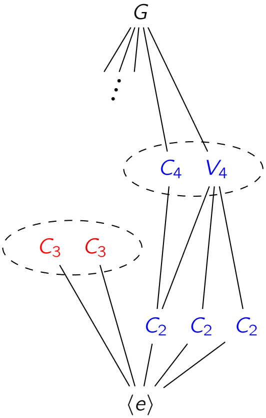
$$|\,\mathrm{Fix}(\phi)| \equiv_p |S| = [G : H] = m \not\equiv_p 0. \qquad \square$$

Our unknown group of order 12

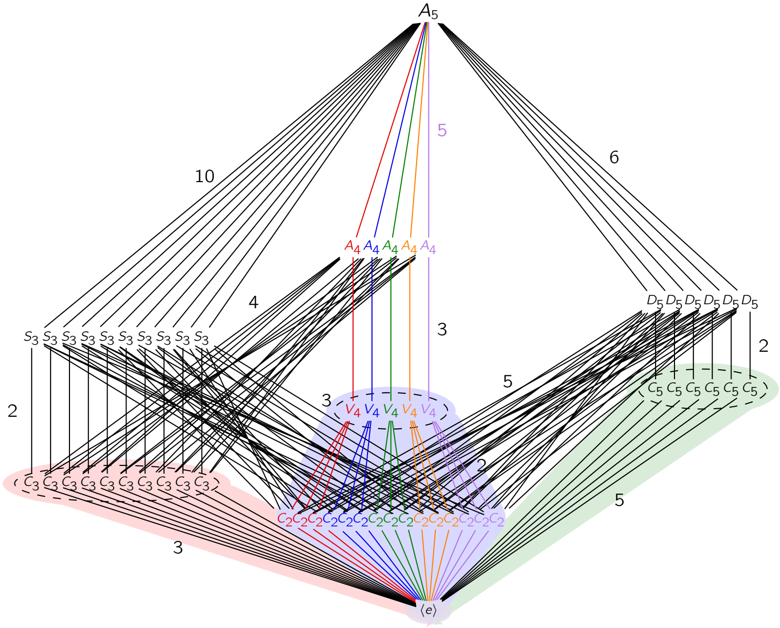
By the second Sylow theorem, all Sylow p-subgroups are conjugate, and hence isomorphic.

This eliminates the following subgroup lattice of a group of order 12.





Example: A_5 has no nontrivial proper normal subgroups



The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

Proposition

Let P be a non-normal Sylow p-subgroup of G. Then its normalizer is fully unnormal.

Proof

We'll verify the equivalent statement of $N_G(N_G(P)) = N_G(P)$.

Note that P is a normal Sylow p-subgroup of $N_G(P)$.

By the 2nd Sylow theorem, P is the unique Sylow p-subgroup of $N_G(P)$.

Take an element x that normalizes $N_G(P)$ (i.e., $x \in N_G(N_G(P))$. We'll show that it also normalizes P. By definition, $xN_G(P)x^{-1} = N_G(P)$, and so

$$P \leq N_G(P) \qquad \Longrightarrow \qquad xPx^{-1} \leq xN_G(P)x^{-1} = N_G(P).$$

But xPx^{-1} is also a Sylow p-subgroup of $N_G(P)$, and by uniqueness, $xPx^{-1} = P$. $\square$

The 3rd Sylow theorem: number of p-subgroups

Third Sylow theorem

Let n_p be the number of Sylow p-subgroups of G. Then

$$n_p \text{ divides } |G| \qquad \text{and} \qquad n_p \equiv_p 1\,.$$

(Note that together, these imply that $n_p \mid m$, where $|G| = p^n \cdot m$.)

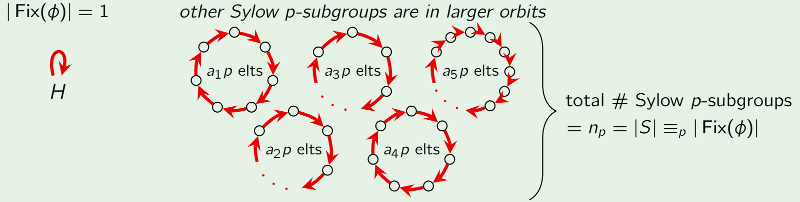
Proof

Take $H \in \mathrm{Syl}(G)$. By the 2nd Sylow theorem, $n_p = |\,\mathrm{cl}_G(H)| = [G : N_G(H)] \,\big|\, |G|$. ✓

The subgroup H acts on $S = \mathrm{Syl}_p(G)$ by conjugation, via $\phi \colon G \to \mathrm{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } K \text{ to } h^{-1}Kh.$$

Goal: *show that H is the unique fixed point*.



The 3rd Sylow theorem: number of p-subgroups

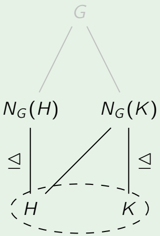
Proof (cont.)

Goal: *show that H is the unique fixed point*.

Let $K \in \mathrm{Fix}(\phi)$. Then $K \leq G$ is a Sylow p-subgroup satisfying

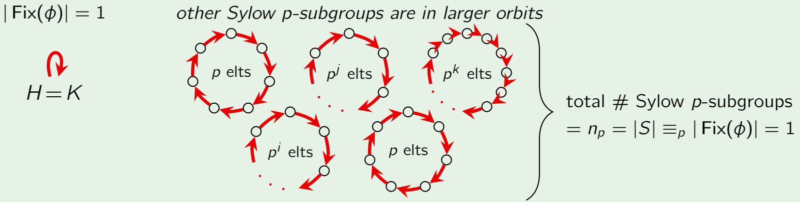
$$h^{-1}Kh = K\,, \quad \forall h \in H \quad \iff \quad H \leq N_G(K) \leq G\,.$$

- H and K are p-Sylow in G, and in $N_G(K)$.
- H and K are conjugate in $N_G(K)$. (2nd Sylow thm.)
- $K \trianglelefteq N_G(K)$, thus is only conjugate to itself in $N_G(K)$.



Thus, $K = H$. That is, $\mathrm{Fix}(\phi) = \{H\}$.

By the p-group Lemma, $n_p := |S| \equiv_p |\mathrm{Fix}(\phi)| = 1$. $\square$



Summary of the proofs of the Sylow theorems

For the 1st Sylow theorem, we started with $H = \{e\}$, and inductively created larger subgroups of size $p, p^2, \dots, p^n$.

For the $2^{\rm nd}$ and $3^{\rm rd}$ Sylow theorems, we used a clever group action and then applied one or both of the following:

(i) *orbit-stabilizer theorem*. If G acts on S, then $|\mathrm{orb}(s)|\cdot|\mathrm{stab}(s)| = |G|$.

(ii) *p-group lemma*. If a p-group acts on S, then $|S| \equiv_p |\mathrm{Fix}(\phi)|$.

To summarize, we used:

S2 The action of $K \in \mathrm{Syl}_p(G)$ on $S = H\backslash G$ by right multiplication for some other $H \in \mathrm{Syl}_p(G)$.

S3a The action of G on $S = \mathrm{Syl}_p(G)$, by conjugation.

S3b The action of $H \in \mathrm{Syl}_p(G)$ on $S = \mathrm{Syl}_p(G)$, by conjugation.

Our mystery group order 12

By the 3rd Sylow theorem, every group G of order $12 = 2^2 \cdot 3$ must have:

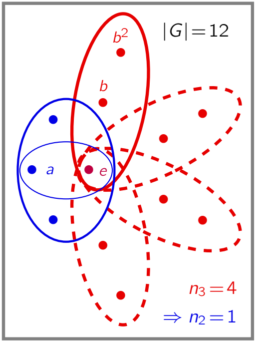
- n_3 Sylow 3-subgroups, each of order 3.

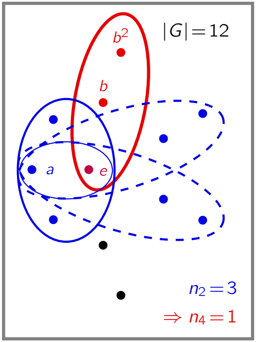
$$n_3 \mid 4, \qquad n_3 \equiv 1 \pmod 3 \qquad \Longrightarrow \qquad n_3 = 1 \text{ or } 4.$$

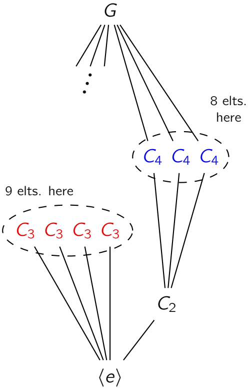
- n_2 Sylow 2-subgroups of order $2^2 = 4$.

$$n_2 \mid 3, \qquad n_2 \equiv 1 \pmod 2 \qquad \Longrightarrow \qquad n_2 = 1 \text{ or } 3.$$

But both are not possible! (There aren't enough elements.)





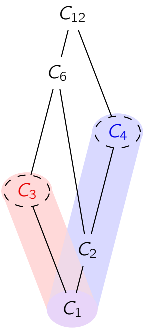


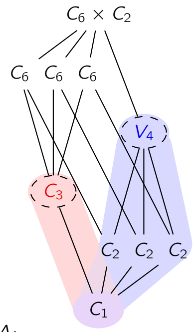
The five groups of order 12

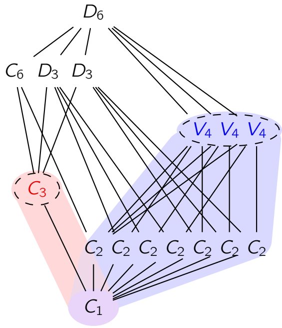
With a litte work and the Sylow theorems, we can classify all groups of order 12.

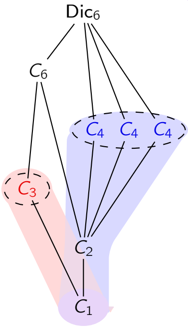
We've already seen them all. Here are their subgroup lattices.

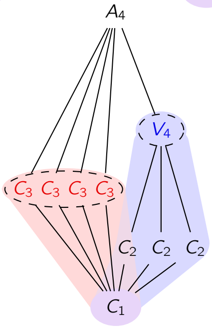
Note that *all* of these decompose as a direct or semidirect product of Sylow subgroups.











Simple groups and the Sylow theorems

Definition

A group G is simple if its only normal subgroups are G and $\langle e \rangle$.

Simple groups are to groups what primes are to integers, and are essential to understand.

The Sylow theorems are very useful for establishing statements like:

"There are no simple groups of order k (for some k)."

Since all Sylow p-subgroups are conjugate, the following result is immediate.

Remark

A Sylow p-subgroup is normal in G iff it's the unique Sylow p-subgroup (that is, if $n_p = 1$).

Thus, if we can show that $n_p = 1$ for some p dividing $|G|$, then G cannot be simple.

For some $|G|$, this is harder than for others, and sometimes it's not possible.

Tip

When trying to show that $n_p = 1$, it's usually helpful to analyze the largest primes first.

An easy example

We'll see three examples of showing that groups of a certain size cannot be simple, in successive order of difficulty.

Proposition

There are no simple groups of order 84.

Proof

Since $|G| = 84 = 2^2 \cdot 3 \cdot 7$, the third Sylow theorem tells us:

- n_7 divides $2^2 \cdot 3 = 12$ (so $n_7 \in \{1, 2, 3, 4, 6, 12\}$)
- $n_7 \equiv_7 1$.

The only possibility is that $n_7 = 1$, so the Sylow 7-subgroup must be normal. □

Observe why it is beneficial to use the largest prime first:

- n_3 divides $2^2 \cdot 7 = 28$ and $n_3 \equiv_3 1$. Thus $n_3 \in \{1, \not{2}, 4, 7, \not{14}, 28\}$.
- n_2 divides $3 \cdot 7 = 21$ and $n_2 \equiv_2 1$. Thus $n_2 \in \{1, 3, 7, 21\}$.

A harder example

Proposition

There are no simple groups of order 351.

Proof

Since $|G| = 351 = 3^3 \cdot 13$, the third Sylow theorem tells us:

- n_{13} divides $3^3 = 27$ (so $n_{13} \in \{1, 3, 9, 27\}$)
- $n_{13} \equiv_{13} 1$.

The only possibilies are $n_{13} = 1$ or 27.

A Sylow 13-subgroup P has order 13, and a Sylow 3-subgroup Q has order $3^3 = 27$. Therefore, $P \cap Q = \{e\}$.

Suppose $n_{13} = 27$. Every Sylow 13-subgroup contains 12 non-identity elements, and so G must contain $27 \cdot 12 = 324$ elements of order 13.

This leaves $351 - 324 = 27$ elements in G not of order 13. Thus, G contains only one Sylow 3-subgroup (i.e., $n_3 = 1$) and so G cannot be simple. □

The hardest example

Proposition

There are no simple groups of order $24 = 2^3 \cdot 3$.

From the 3rd Sylow theorem, we can only conclude that $n_2 \in \{1, 3\}$ and $n_3 = \{1, 4\}$.

Let H be a Sylow 2-subgroup, which has relatively "small" index: $[G : H] = 3$.

Lemma

If G has a subgroup of index $[G : H] = n$, and $|G|$ does not divide $n!$, then G is not simple.

Proof

Let G act on the **right cosets** of H (i.e., $S = H \backslash G$) by **right-multiplication**:

$$\phi \colon G \longrightarrow \mathrm{Perm}(S) \cong S_n\,, \qquad \phi(g) = \text{the permutation that sends each } Hx \text{ to } Hxg.$$

Recall that $\mathrm{Ker}(\phi) \trianglelefteq G$, and is the intersection of all conjugate subgroups of H:

$$\langle e \rangle \leq \mathrm{Ker}(\phi) = \bigcap_{x \in G} x^{-1} H x \lneq G$$

If $\mathrm{Ker}(\phi) = \langle e \rangle$ then $\phi \colon G \hookrightarrow S_n$ is an embedding, which is impossible because $|G| \nmid n!$. □

Finite abelian groups

Lemma 1

Let $|G| = p^n$. Then G is cyclic iff it has a unique subgroup of order p^k for each $k = 0, 1, \ldots, n$.

Proof

If $G \cong C_{p^n} = \langle r \rangle$, then $\langle r^d \rangle$ is the unique subgroup of order p^n/d.

Conversely, suppose G has a subgroup of order p^k for each $k = 0, 1, \ldots, n$, and let $|H| = p^{n-1}$.

By the first Sylow theorem, H has a subgroup of each order p^k as well, for $k = 0, 1, \ldots, n-1$.

Therefore, it must contain the unique subgroup of G of each of these orders, and hence, every proper subgroup of G.

Now, take any $g \notin H$. The cyclic subgroup $\langle g \rangle$ of G cannot be any of the subgroups of H, so it must be G. $\square$

Finite abelian groups

Lemma 2

If G is an abelian p-group with a unique subgroup of order p, then G is cyclic.

Proof

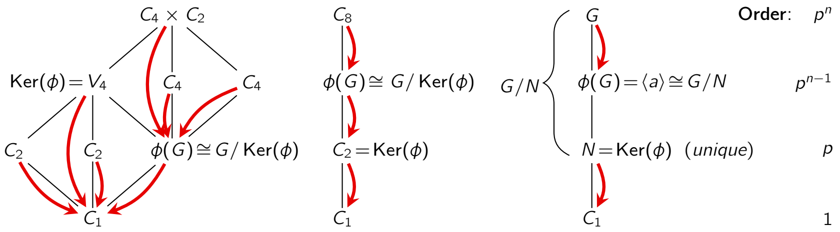
Induct on n, where $|G| = p^n$. The base case is trivial.

Suppose it holds for all p-groups of order up to p^{n-1}. Consider the homomorphism

$$\phi\colon G \longrightarrow G, \qquad \phi(x) = x^p.$$

The kernel is the unique subgroup $N \leq G$ of order p.

By Cauchy's theorem, every nontrivial subgroup of G must contain N.



Finite abelian groups

Lemma 2

If G is an abelian p-group with a unique subgroup of order p, then G is cyclic.

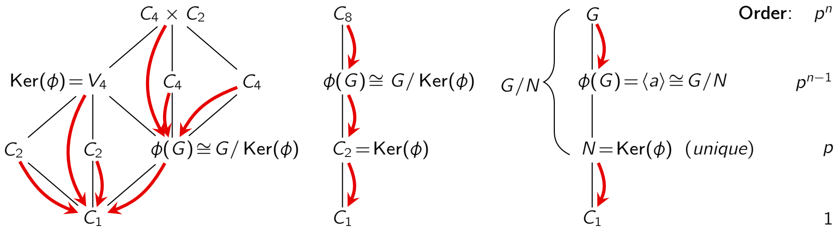
Proof (contin.)

By the FHT, $\phi(G) \cong G/N$ has order p^{n-1}.

However, $\phi(G) \leq G$, so it has a unique subgroup of order p.

By induction, $\phi(G) \cong G/N$ is cyclic, so it has a unique order-p^k subgroup H/N, for each $k \leq n-1$.

By the correspondence theorem, H is the unique subgroup of G of order p^{k-1}. □



Finite abelian groups

Lemma 3

Let G be a finite abelian p-group, and $A \leq G$ a maximal cyclic subgroup. Then $G = A \times H$ for some subgroup H.

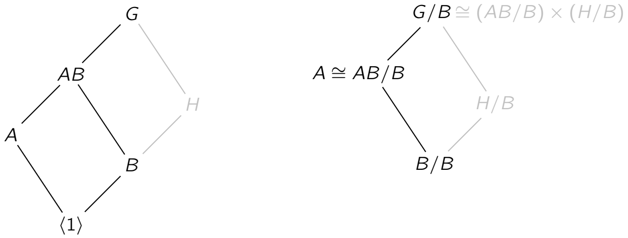
Proof

Induct on n, where $|G| = p^n$. The base case is trivial.

Let $A = \langle a \rangle$ for $|a| = p^k$, and assume the result holds for p-groups of order $< |G| = p^n$.

By the Lemma, there is a subgroup $B \leq G$ of order p, not contained in A.

By the diamond theorem: $AB/B \cong A/(A \cap B) \cong A$.



Finite abelian groups

Lemma 3

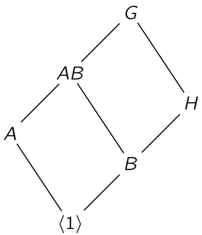
Let G be a finite abelian p-group, and $A \leq G$ a maximal cyclic subgroup. Then $G = A \times H$ for some subgroup H.

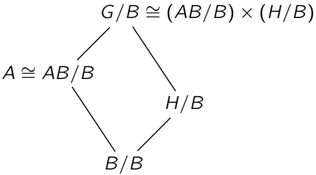
Proof (contin.)

No quotient of G can have a cyclic subgroup of order larger than $|A| = p^k$ (because $|H/N| = |\langle bH\rangle| = p^\ell > p^k$ in would force $|\langle b\rangle| > p^k$).

Therefore, $AB/B \cong A$ is a maximal cyclic subgroup of G/B.

By induction, there is some $H/B \leq G/B$ for which $G/B \cong AB/B \times H/B$.





Finite abelian groups

Lemma 3

Let G be a finite abelian p-group, and $A \leq G$ a maximal cyclic subgroup. Then $G = A \times H$ for some subgroup H.

Proof (contin.)

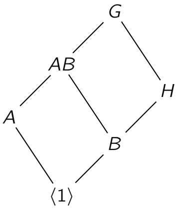
It suffices to show that A and H are lattice complements in G.

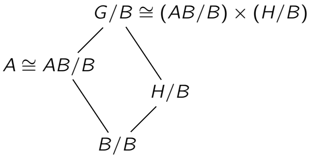
Generate G: Since $B \leq H$, we have $BH = H$ and $AB \subseteq AH$, and hence

$$G = (AB)H = A(BH) = AH.$$

Intersect trivially: Using $A \subseteq AB$ and basic set theory:

$$A \cap H \;\subseteq\; A \cap H \cap AB \;= A \cap (H \cap AB) \;=\; A \cap B \;=\; \langle 1 \rangle.$$





Finite abelian groups

Lemma 4

Every finite abelian group is a direct product of its Sylow p-groups.

Proof

Induct on the number of primes dividing $|G|$. □

Fundamental theorem of finite abelian groups

Every finite abelian group is a direct product of cyclic groups.

Proof

By Lemma 4, it suffices to consider the case of $|G| = p^n$. We'll induct on n.

The cases of $n = 0$ and $n = 1$ are trivial. Assume the result holds for all groups of order $p^1, \dots, p^{n-1}$.

If G is not cyclic, let A be a maximal cyclic subgroup.

Write $G = A \times H$ using Lemma 3, and apply the induction hypothesis. □

Conjugacy classes in A_n

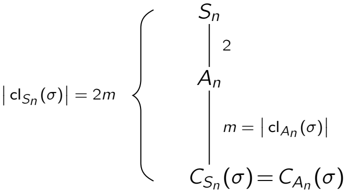
Elements in S_n are conjugate iff they have the same cycle type.

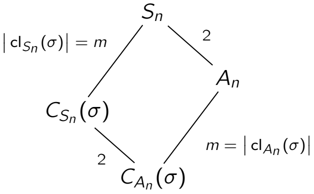
However, 8 of the 12 elements in A_4 are 3-cycles. These cannot all be conjugate.

Take $\sigma \in A_n$. *The size of its conjugacy class is the index of its centralizer.*

There are two cases to consider:

1. $C_{S_n}(\sigma)$ is a subgroup of A_n, or equivalently, $C_{A_n}(\sigma) = C_{S_n}(\sigma)$
2. $C_{S_n}(\sigma)$ is not a subgroup of A_n, or equivalently, $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$.





Key idea

Upon restricting to $A_n \leq S_n$, the conjugacy class of σ is either preserved or splits in two.

Simplicity of A_5

For example, S_5 has 7 conjugacy classes: $\text{cl}_{S_5}(e) = \{e\}$, and

$$\text{cl}_{S_5}((12)),\quad \text{cl}_{S_5}((123)),\quad \text{cl}_{S_5}((1234)),\quad \text{cl}_{S_5}((12345)),\quad \text{cl}_{S_5}((12)(34)),\quad \text{cl}_{S_5}((12)(345)).$$

To find the conjugacy classes of A_5, first disregard the odd permutations. Note that:

- $C_{S_5}(e) = S_5$
- $C_{S_5}((12)(34))$ and $C_{S_5}((123))$ both contain some $(ij) \notin A_5$
- $C_{S_5}((12345)) \leq A_5$

Therefore, the size-24 conjugacy class containing (12345) splits in A_5.

$$\left|\text{cl}_{S_5}((123))\right| = 20,\quad \left|\text{cl}_{S_5}((12345))\right| = 12,\quad \left|\text{cl}_{S_5}((13524))\right| = 12,\quad \left|\text{cl}_{S_5}((12)(34))\right| = 15.$$

Proposition

The alternating group A_5 is simple.

Proof

Any normal subgroup of A_5 must have order 2, 3, 4, 5, 6, 12, 15, ~~20~~, or ~~30~~.

It's also the union of conjugacy classes: $\{e\}$ and other(s) of sizes 12, 12, 15, and 20.

Other than A_5 and $\langle e \rangle$, this is impossible. □

A few basic properties of the alternating group A_n

Lemma

(i) A_n is generated by 3-cycles, if $n \geq 3$.

(ii) all 3-cycles are conjugate to (123), if $n \geq 5$.

Proof

(i) Since $A_3 = \langle (123) \rangle$, take $n \geq 4$.

A_n is generated by products of pairs of transpositions.

- **Type 1**. Disjoint transpositions:

$$(ab)(cd) = (acd)(acb).$$

- **Type 2**. Overlapping transpositions:

$$(ab)(bc) = (acb).$$ ✓

(ii) Take any 3-cycle (abc), and write

$$(abc) = \sigma(123)\sigma^{-1}, \qquad \sigma \in S_n.$$

If $\sigma \in A_n$, we're done. Otherwise, conjugate (123) by $\sigma \cdot (45) \in A_n$. ✓

Simplicity of A_n

Theorem

The alternating group A_n is simple, for all $n \geq 5$.

Proof

Consider a nontrivial proper normal subgroup $N \trianglelefteq G$.

All we have to do is show that N contains a 3-cycle. (Why?)

Pick any nontrivial $\sigma \in N$, and write it as a product of disjoint cycles.

There are several cases to consider separately. We'll either

(i) construct a 3-cycle from σ, or

(ii) construct an element in a previous case.

Case 1. σ contains a k-cycle $(a_1 a_2 \cdots a_k)$ for $k \geq 4$.

Then N contains a 3-cycle:

$$\underbrace{(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1}}_{\in N} \cdot \sigma^{-1} = (a_1 a_2 a_3)(a_1 a_2 \cdots a_k)(a_3 a_2 a_1)(a_k \cdots a_2 a_1) = (a_2 a_3 a_k) \in N. \quad \checkmark$$

In the remaining cases, *we can assume that σ is a product of 2- and 3-cycles*.

Simplicity of A_n

Theorem

The alternating group A_n is simple, for all $n \geq 5$.

Proof (contin.)

Case 2. σ has at least two 3-cycles; $\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6) \cdots$.

If we conjugate σ by $(a_1 a_2 a_4)$, we can also ignore the other (commuting) cycles in σ.

$$\underbrace{(a_1 a_2 a_4)\sigma(a_1 a_2 a_4)^{-1}}_{\in N} \cdot \sigma^{-1} = (a_1 a_2 a_4)[(a_1 a_2 a_3)(a_4 a_5 a_6) \cdots](a_4 a_2 a_1)[\cdots(a_6 a_5 a_4)(a_3 a_2 a_1)]$$
$$= (a_1 a_2 a_4 a_3 a_6) \in N.$$

We are now back in Case 1. ✓

Case 3. σ has only one 3-cycle; $\sigma = (a_1 a_2 a_3)(a_4 a_5)(a_6 a_7) \cdots\cdots$.

Then $\sigma^2 = (a_1 a_3 a_2) \in N$, and so $\sigma \in N$. ✓

We've exhausted the cases where σ contains a 3-cycle.

In the remaining cases, *we can assume that σ is a product of pairs of 2-cycles*.

Simplicity of A_n

Theorem

The alternating group A_5 is simple, for all $n \geq 5$.

Proof (contin.)

Case 4. σ is a product of 2-cycles; $\sigma = (a_1 a_2)(a_3 a_4) \cdots$.

If we conjugate σ by $(a_1 a_2 a_3)$, we can ignore the other (commuting) 2-cycles in σ.

$$\underbrace{(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1}}_{\in N} \cdot \sigma^{-1} = (a_1 a_2 a_3)(a_1 a_2)(a_3 a_4)(a_3 a_2 a_1)(a_1 a_2)(a_3 a_4)$$

$$= (a_1 a_4)(a_2 a_3) \in N.$$

Now, letting $\pi = (a_1 a_4 a_5)$,

$$\underbrace{(a_1 a_4)(a_2 a_3)\pi[(a_1 a_4)(a_2 a_3)]^{-1}}_{\in N} \cdot \pi^{-1} = (a_1 a_4)(a_2 a_3)(a_1 a_4 a_5)(a_1 a_4)(a_2 a_3)(a_5 a_4 a_1)$$

$$= (a_1 a_4 a_5) \in N. \qquad \checkmark$$

and this completes the proof. $\square$

Classification of finite simple groups

Theorem (2004)

Every finite simple group is isomorphic to one of the following groups:

- A cyclic group $\mathbb{Z}_p$, with p prime;
- An alternating group A_n, with $n \geq 5$;
- A Lie-type Chevalley group: $\mathrm{PSL}(n, q)$, $\mathrm{PSU}(n, q)$, $\mathrm{PsP}(2n, p)$, and $P\Omega^{\epsilon}(n, q)$;
- A Lie-type group (twisted Chevalley group or the Tits group): $D_4(q)$, $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, ${}^2F_4(2^n)'$, $G_2(q)$, ${}^2G_2(3^n)$, ${}^2B(2^n)$;
- One of 26 exceptional "sporadic groups."

The two largest sporadic groups are the:

- "baby monster group" B, which has order

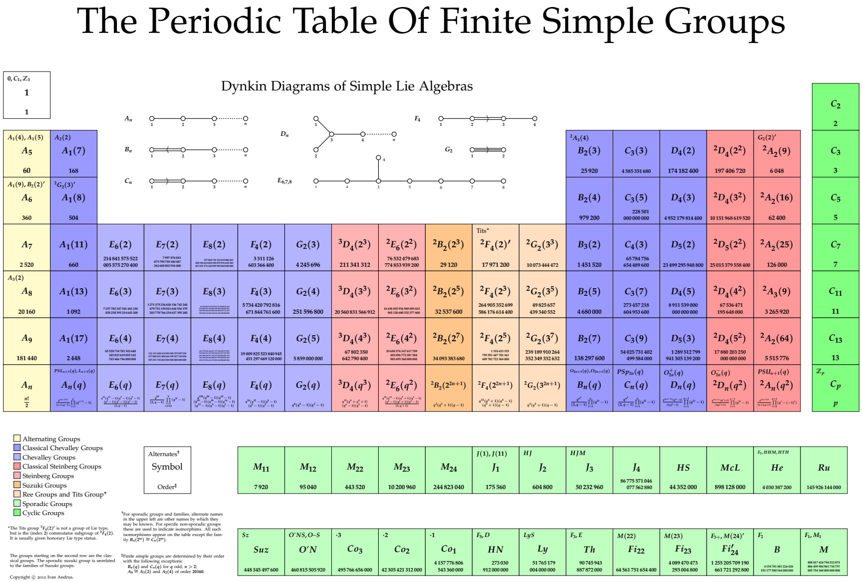
$$|B| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \approx 4.15 \times 10^{33};$$

- "monster group" M, which has order

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8.08 \times 10^{53}.$$

The proof of this classification theorem is spread across $\approx$15,000 pages in $\approx$500 journal articles by over 100 authors, published between 1955 and 2004.

Image by *Ivan Andrus*, 2012



Finite Simple Group (of Order Two), by The Klein Four$^{\text{TM}}$

Musical Fruitcake

View More by This Artist

Klein Four

Open iTunes to preview, buy, and download music.

View in iTunes

$9.99

Genres: Pop, Music
Released: Dec 05, 2005
℗ 2005 Klein Four

Customer Ratings

★★★★½ 13 Ratings

	Name	Artist	Time	Price	
1	Power of One	Klein Four	5:16	$0.99	View In iTunes ▸
2	Finite Simple Group (of Order Two)	Klein Four	3:00	$0.99	View In iTunes ▸
3	Three-Body Problem	Klein Four	3:17	$0.99	View In iTunes ▸
4	Just the Four of Us	Klein Four	4:19	$0.99	View In iTunes ▸
5	Lemma	Klein Four	3:43	$0.99	View In iTunes ▸
6	Calculating	Klein Four	4:09	$0.99	View In iTunes ▸
7	XX Potential	Klein Four	3:42	$0.99	View In iTunes ▸
8	Confuse Me	Klein Four	3:41	$0.99	View In iTunes ▸
9	Universal	Klein Four	4:13	$0.99	View In iTunes ▸
10	Contradiction	Klein Four	3:48	$0.99	View In iTunes ▸
11	Mathematics Paradise	Klein Four	3:51	$0.99	View In iTunes ▸
12	Stefanie (The Ballad of Galois)	Klein Four	4:51	$0.99	View In iTunes ▸
13	Musical Fruitcake (Pass it Around)	Klein Four	2:50	$0.99	View In iTunes ▸
14	Abandon Soap	Klein Four	2:17	$0.99	View In iTunes ▸

14 Songs