Section 5: Groups acting on sets

Matthew Macauley

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

Math 4120, Modern Algebra

Overview

Intuitively, a group action occurs when a group G "naturally permutes" a set S *of states*.

For example:

- The "Rubik's cube group" consists of the 4.3×10^{19} actions that *permutated* the 4.3×10^{19} configurations of the cube.
- The group D_4 consists of the 8 symmetries of the square. These symmetries are *actions* that *permuted* the 8 configurations of the square.

Group actions help us understand the interplay between the actual group of actions and sets of objects that they "rearrange."

There are many other examples of groups that "act on" sets of objects. We will see examples when the group and the set have different sizes.

There is a rich theory of group actions, and it can be used to prove many deep results in group theory.

Actions vs. configurations

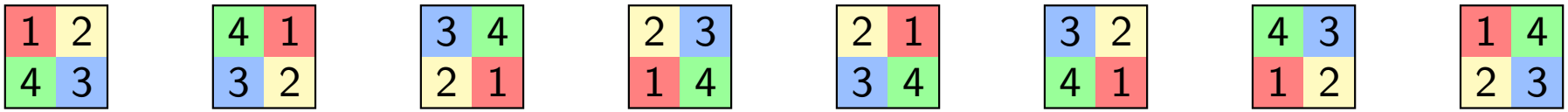
The group D_4 can be thought of as the 8 symmetries of the square:

There is a subtle but *important* distinction to make, between the actual 8 symmetries of the square, and the 8 configurations.

For example, the 8 symmetries (alternatively, "actions") can be thought of as

$$e, \quad r, \quad r^2, \quad r^3, \quad f, \quad rf, \quad r^2 f, \quad r^3 f\,.$$

The 8 configurations (or *states*) of the square are the following:

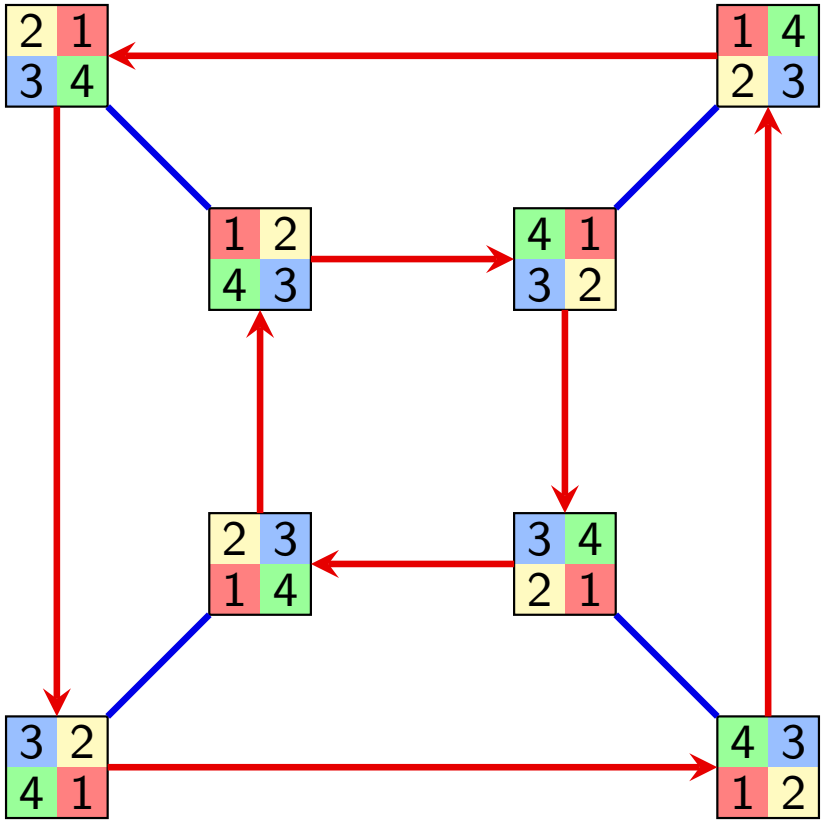


When we were just learning about groups, we made an action diagram.

- The vertices correspond to the states.
- The edges correspond to generators.
- The paths corresponded to actions (group elements).

Actions diagrams

Here is the action diagram of the group $D_4 = \langle r, f \rangle$:



In the beginning of this course, we picked a configuration to be the "solved state," and this gave us a *bijection* between configurations and actions (group elements).

The resulting diagram was a Cayley diagram. In this section, we'll skip this step.

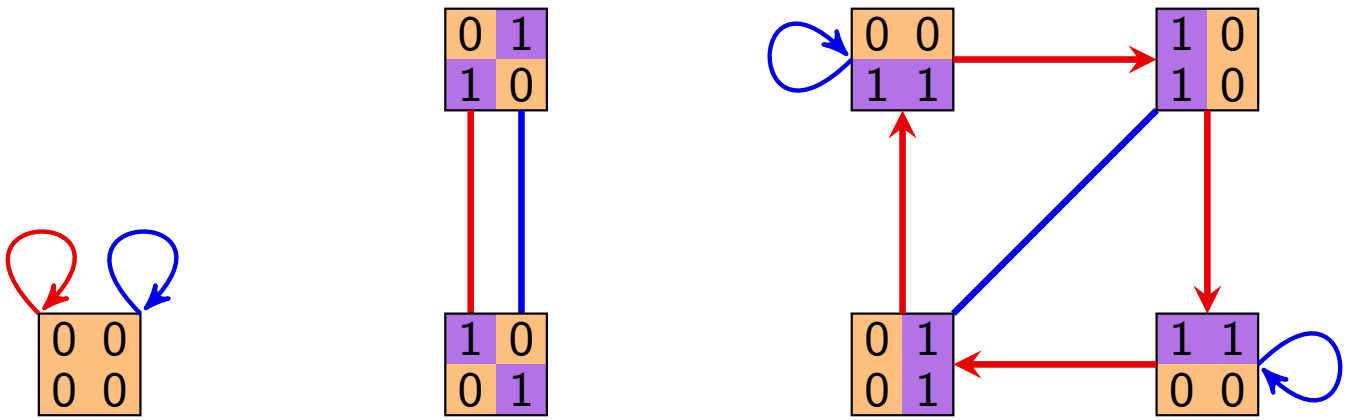
Actions diagrams

In all of the examples we saw in the beginning of the course, we had a bijective correspondence between actions and states. *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:



The action diagram above has some properties of Cayley diagrams, but there are some fundamental differences as well.

A "group switchboard"

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,

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

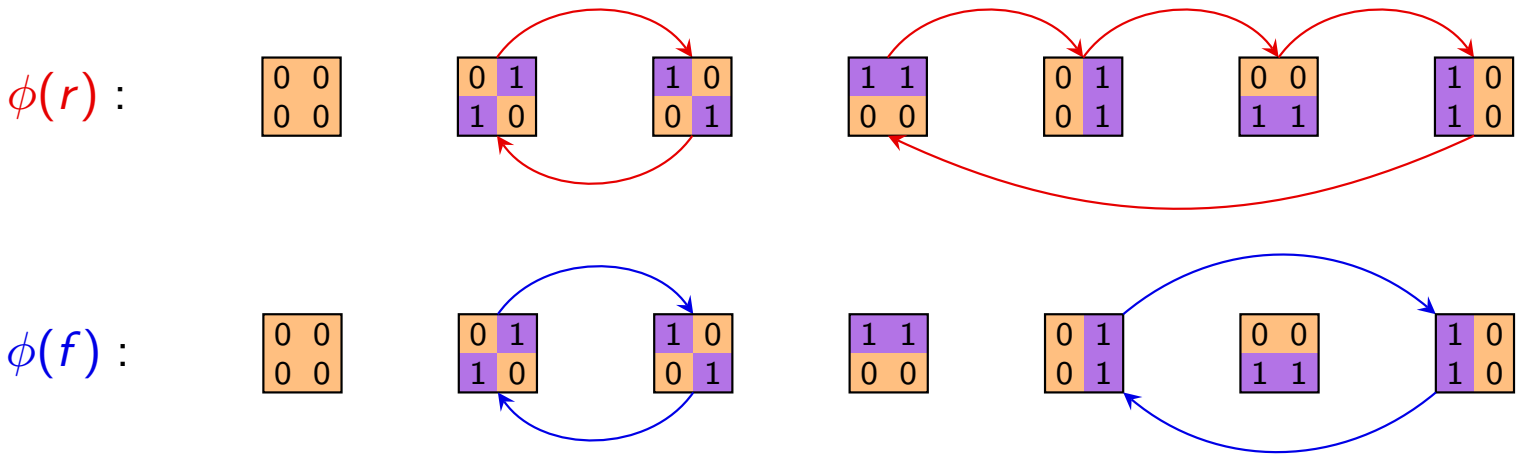
Let $\text{Perm}(S)$ be the group of permutations of S. Thus, if $|S| = n$, then $\text{Perm}(S) \cong S_n$. (We typically think of S_n as the permutations of $\{1, 2, \ldots, n\}$.)

Definition

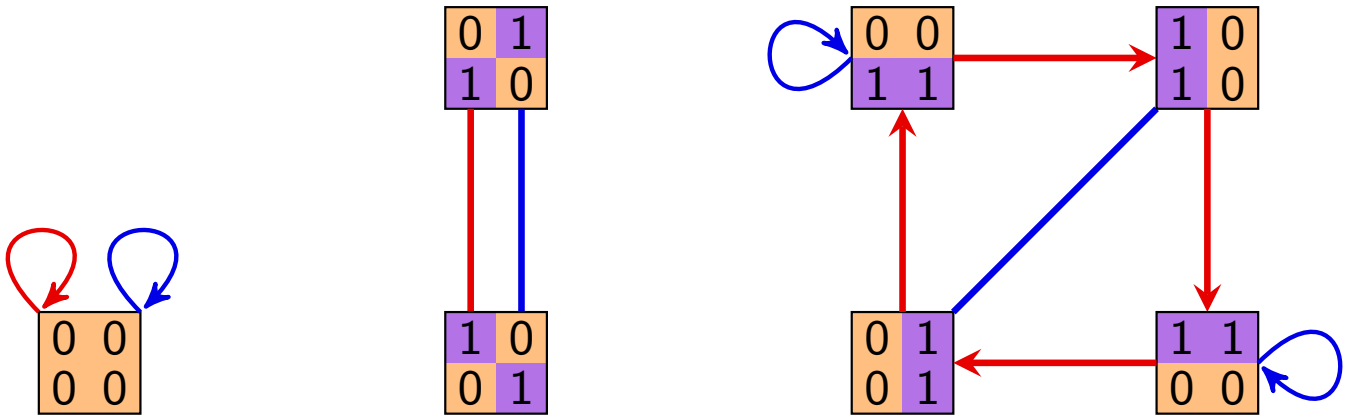
A group G acts on a set S if there is a homomorphism $\phi\colon G \to \text{Perm}(S)$.

A "group switchboard"

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



Observe how these permutations are encoded in the action diagram:



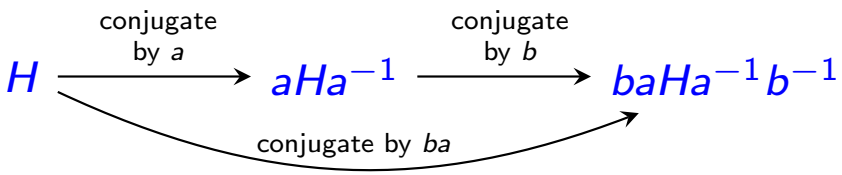
Left actions vs. right actions (an annoyance we can deal with)

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 has to be the same as "*pressing the ba-button*."

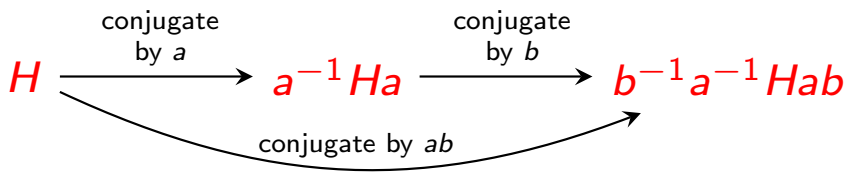
This is best seen by an example. Suppose our action is conjugation:

"Left group action"



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

"Right group action"



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

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

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

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.

Pretty much all of the theorems for left actions hold for right actions.

Usually if there is a left action, there is a related right action. We will usually use right actions, and we will 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 $\phi(g).s$.

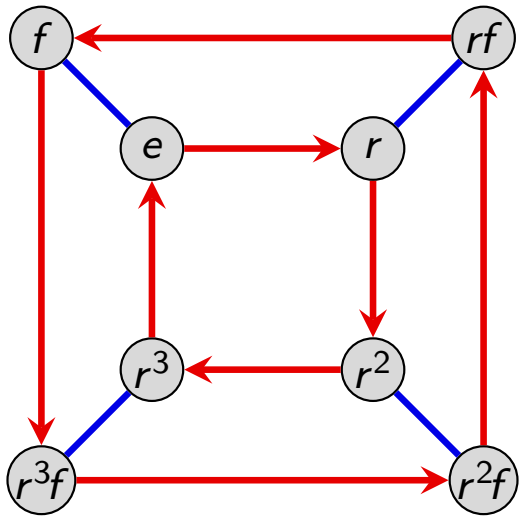
Cayley diagrams as action diagrams

Every Cayley diagram can be thought of as the action diagram of a particular (right) group action.

For example, consider the group $G = D_4 = \langle r, f \rangle$ acting on itself. That is, $S = D_4 = \{e, r, r^2, r^3, f, rf, r^2f, r^3f\}$.

Suppose that pressing the g-button on our "group switchboard" multiplies every element *on the right* by g.

Here is the action diagram:



We say that "*G acts on itself by right-multiplication*."

Orbits, stabilizers, and fixed points

Suppose G acts on a set S. Pick a configuration $s \in S$. 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 $\phi\colon G \to S$.

(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

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

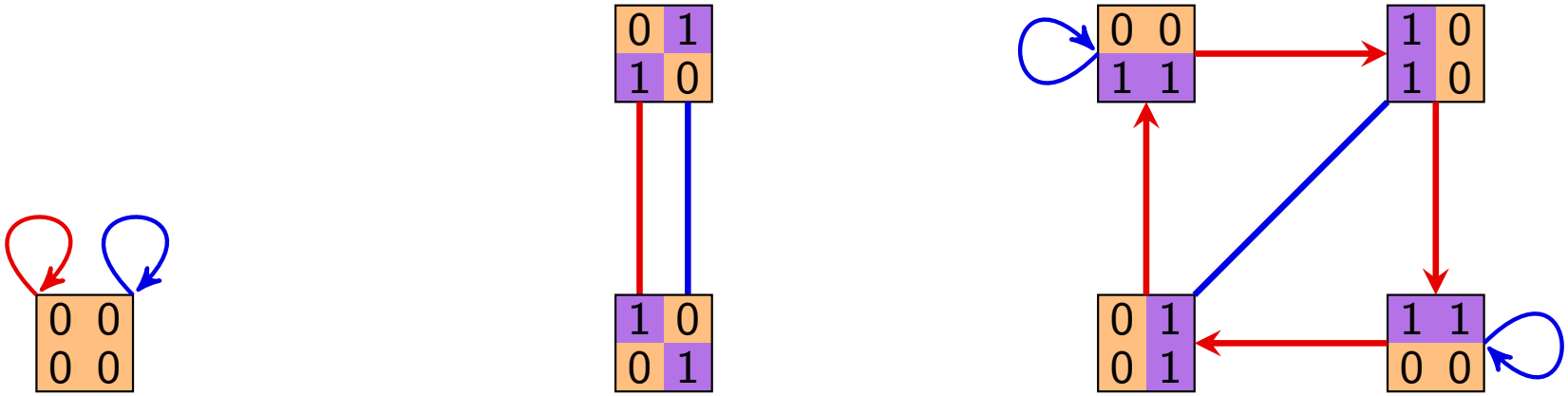
(iii) The fixed points of the action are the orbits of size 1:

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

Note that the orbits of ϕ are the connected components in the action diagram.

Orbits, stabilizers, and fixed points

Let's revisit our running example:



The orbits are the 3 connected components. There is only one fixed point of ϕ. The stabilizers are:

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

$$\mathrm{Stab}\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) = \{e, r^2, rf, r^3f\},$$

$$\mathrm{Stab}\left(\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right) = \{e, f\},$$

$$\mathrm{Stab}\left(\begin{smallmatrix}1&0\\1&0\end{smallmatrix}\right) = \{e, r^2f\},$$

$$\mathrm{Stab}\left(\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right) = \{e, f\},$$

$$\mathrm{Stab}\left(\begin{smallmatrix}0&1\\0&1\end{smallmatrix}\right) = \{e, r^2f\}.$$

Observations?

Orbits and stabilizers

Proposition

For any $s \in S$, the set $\text{Stab}(s)$ is a subgroup of G.

Proof (outline)

To show $\text{Stab}(s)$ is a group, we need to show three things:

(i) *Contains the identity.* That is, $s.\phi(e) = s$.

(ii) *Inverses exist.* That is, if $s.\phi(g) = s$, then $s.\phi(g^{-1}) = s$.

(iii) *Closure.* That is, if $s.\phi(g) = s$ and $s.\phi(h) = s$, then $s.\phi(gh) = s$.

You'll do this on the homework.

Remark

The kernel of the action ϕ is the set of all group elements that fix everything in S:

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

Notice that

$$\text{Ker}\,\phi = \bigcap_{s \in S} \text{Stab}(s).$$

The Orbit-Stabilizer Theorem

The following result is another one of the central results of group theory.

Orbit-Stabilizer theorem

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

$$|\operatorname{Orb}(s)| \cdot |\operatorname{Stab}(s)| = |G|.$$

Proof

Since $\operatorname{Stab}(s) < G$, Lagrange's theorem tells us that

$$\underbrace{[G\colon \operatorname{Stab}(s)]}_{\text{number of cosets}} \cdot \underbrace{|\operatorname{Stab}(s)|}_{\text{size of subgroup}} = |G|.$$

Thus, it suffices to show that $|\operatorname{Orb}(s)| = [G\colon \operatorname{Stab}(s)]$.

Goal: Exhibit a bijection between elements of $\operatorname{Orb}(s)$, and right cosets of $\operatorname{Stab}(s)$.

That is, *two elements in G send s to the same place iff they're in the same coset*.

The Orbit-Stabilizer Theorem: $|\mathrm{Orb}(s)| \cdot |\mathrm{Stab}(s)| = |G|$

Proof (cont.)

Let's look at our previous example to get some intuition for why this should be true.

We are seeking a bijection between Orb(s), and the right cosets of Stab(s).

That is, two elements in G send s to the same place iff they're in the same coset.

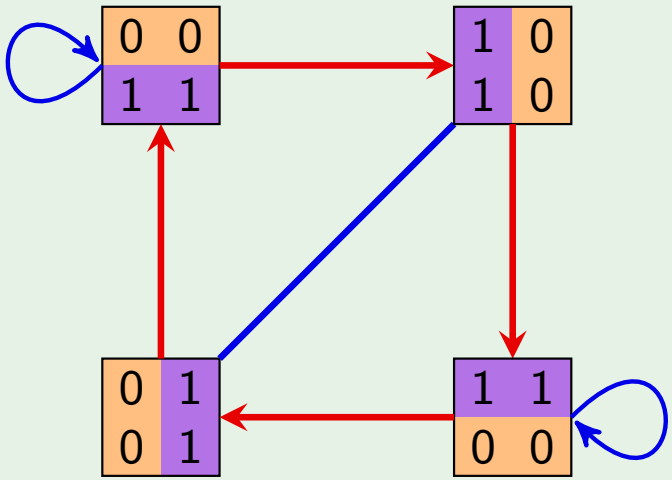
Let $s = \begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix}$

Then $\mathrm{Stab}(s) = \langle f \rangle$.

Partition of D_4 by the right cosets of H :

$G = D_4$ and $H = \langle f \rangle$

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



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:

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

"$\Leftarrow$" *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 $\implies$ into $\iff$, and thus conclude that $s.\phi(g) = s.\phi(k)$. $\square$

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

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 $H \leq G$.

Sometimes, the orbits and stabilizers of these actions are actually familiar algebraic objects.

Also, sometimes a deep theorem has a slick proof via a clever group action.

For example, we will see how Cayley's theorem (every group G is isomorphic to a group of permutations) follows immediately once we look at the correct 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 analyze the orbits, stabilizers, and fixed points.

Groups acting on themselves by right-multiplication

We've seen how groups act on themselves by right-multiplication. While this action is boring (any Cayley diagram is an action diagram!), it leads to a slick proof of Cayley's theorem.

Cayley's theorem

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

Proof.

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

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

There is only one orbit: $G = S$. The stabilizer of any $x \in G$ is just the identity element:

$$\text{Stab}(x) = \{g \in G \mid xg = x\} = \{e\}\,.$$

Therefore, the kernel of this action is $\text{Ker}\,\phi = \bigcap_{x \in G} \text{Stab}(x) = \{e\}$.

Since $\text{Ker}\,\phi = \{e\}$, the homomorphism ϕ is an embedding. □

Groups acting on themselves by conjugation

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

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

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

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

- The stabilizer of x is the set of elements that commute with x; called its centralizer:

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

- The fixed points of ϕ are precisely those in the center of G:

$$\mathrm{Fix}(\phi) = \{x \in G \mid g^{-1}xg = x \text{ for all } g \in G\} = Z(G)\,.$$

By the Orbit-Stabilizer theorem, $|G| = |\,\mathrm{Orb}(x)| \cdot |\,\mathrm{Stab}(x)| = |\,\mathrm{cl}_G(x)| \cdot |C_G(x)|$.
Thus, we immediately get the following new result about conjugacy classes:

Theorem

For any $x \in G$, the size of the conjugacy class $\mathrm{cl}_G(x)$ divides the size of G.

Groups acting on themselves by conjugation

As an example, consider the action of $G = D_6$ on itself by **conjugation**.

The orbits of the action are the conjugacy classes:

e	r	r^2	f	r^2f	r^4f
r^3	r^5	r^4	rf	r^3f	r^5f

The fixed points of ϕ are the size-1 conjugacy classes. These are the elements in the center: $Z(D_6) = \{e\} \cup \{r^3\} = \langle r^3 \rangle$.

By the Orbit-Stabilizer theorem:

$$|\operatorname{Stab}(x)| = \frac{|D_6|}{|\operatorname{Orb}(x)|} = \frac{12}{|\operatorname{cl}_G(x)|}.$$

The stabilizer subgroups are as follows:

- $\operatorname{Stab}(e) = \operatorname{Stab}(r^3) = D_6$,
- $\operatorname{Stab}(r) = \operatorname{Stab}(r^2) = \operatorname{Stab}(r^4) = \operatorname{Stab}(r^5) = \langle r \rangle = C_6$,
- $\operatorname{Stab}(f) = \{e, r^3, f, r^3f\} = \langle r^3, f \rangle$,
- $\operatorname{Stab}(rf) = \{e, r^3, rf, r^4f\} = \langle r^3, rf \rangle$,
- $\operatorname{Stab}(r^if) = \{e, r^3, r^if, r^if\} = \langle r^3, r^if \rangle$.

Groups acting on subgroups by conjugation

Let $G = D_3$, and let S be the set of proper subgroups of G:

$$S = \Big\{ \langle e \rangle,\ \langle r \rangle,\ \langle f \rangle,\ \langle rf \rangle,\ \langle r^2 f \rangle \Big\}.$$

There is a right group action of $D_3 = \langle r, f \rangle$ on S by conjugation:

$$\tau \colon D_3 \longrightarrow \mathrm{Perm}(S), \qquad \tau(g) = \text{the permutation that sends each } H \text{ to } g^{-1}Hg.$$

$\tau(e) = \langle e \rangle \quad \langle r \rangle \quad \langle f \rangle \quad \langle rf \rangle \quad \langle r^2 f \rangle$

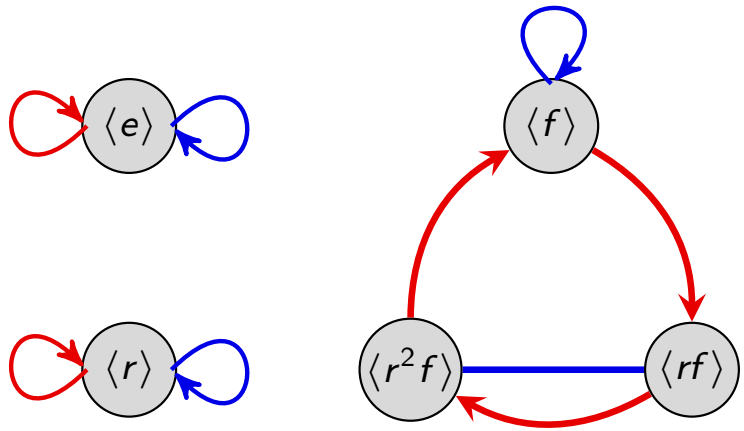
$\tau(r) = \langle e \rangle \quad \langle r \rangle \quad \langle f \rangle \quad \langle rf \rangle \quad \langle r^2 f \rangle$

$\tau(r^2) = \langle e \rangle \quad \langle r \rangle \quad \langle f \rangle \quad \langle rf \rangle \quad \langle r^2 f \rangle$

$\tau(f) = \langle e \rangle \quad \langle r \rangle \quad \langle f \rangle \quad \langle rf \rangle \quad \langle r^2 f \rangle$

$\tau(rf) = \langle e \rangle \quad \langle r \rangle \quad \langle f \rangle \quad \langle rf \rangle \quad \langle r^2 f \rangle$

$\tau(r^2 f) = \langle e \rangle \quad \langle r \rangle \quad \langle f \rangle \quad \langle rf \rangle \quad \langle r^2 f \rangle$



The action diagram.

$$\mathrm{Stab}(\langle e \rangle) = \mathrm{Stab}(\langle r \rangle) = D_3 = N_{D_3}(\langle r \rangle)$$
$$\mathrm{Stab}(\langle f \rangle) = \langle f \rangle = N_{D_3}(\langle f \rangle),$$
$$\mathrm{Stab}(\langle rf \rangle) = \langle rf \rangle = N_{D_3}(\langle rf \rangle),$$
$$\mathrm{Stab}(\langle r^2 f \rangle) = \langle r^2 f \rangle = N_{D_3}(\langle r^2 f \rangle).$$

Groups acting on subgroups by conjugation

More generally, 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:
$$\mathrm{Orb}(H) = \{g^{-1}Hg \mid g \in G\}\,.$$
- 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 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 G iff every subgroup of G is normal. In this case, ϕ is the trivial homomorphism: pressing the g-button fixes (i.e., normalizes) every subgroup.

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 $S = G/H$ (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 $x^{-1}Hx$:

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

- Assuming $H \neq G$, there are no fixed points of ϕ. The only orbit has size $[G : H] > 1$.
- The kernel of this action is the intersection of all conjugate subgroups of H:

$$\mathrm{Ker}\,\phi = \bigcap_{x \in G} x^{-1}Hx$$

Notice that $\langle e \rangle \leq \mathrm{Ker}\,\phi \leq H$, and $\mathrm{Ker}\,\phi = H$ iff $H \lhd G$.

Fixed points of group actions

Recall the subtle difference between fixed points and stabilizers:

- The fixed points of an action $\phi\colon G \to \text{Perm}(S)$ are the elements of S fixed by every $g \in G$.
- The stabilizer of an element $s \in S$ is the set of elements of G that fix s.

Lemma

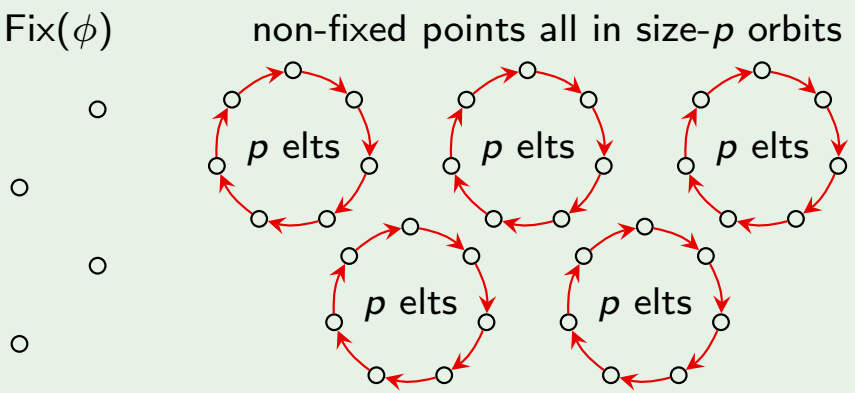
If a group G of prime order p acts on a set S via $\phi\colon G \to \text{Perm}(S)$, then

$$|\operatorname{Fix}(\phi)| \equiv |S| \pmod{p}.$$

Proof (sketch)

By the Orbit-Stabilizer theorem, all orbits have size 1 or p.

I'll let you fill in the details.



Cauchy's Theorem

Cauchy's theorem

If p is a prime number dividing $|G|$, then G has an element g of order p.

Proof

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

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

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

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

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

(This is because if $x_1 x_2 \cdots x_p = e$, then $x_2 x_3 \cdots x_p x_1 = e$ as well.)

The elements of P are partitioned into orbits. By the orbit-stabilizer theorem, $|\,\text{Orb}(s)| = [\mathbb{Z}_p : \text{Stab}(s)]$, which divides $|\mathbb{Z}_p| = p$. Thus, $|\,\text{Orb}(s)| = 1$ or p.

Observe that the only way that an orbit of $(x_1, x_2, \ldots, x_p)$ could have size 1 is if $x_1 = x_2 = \cdots = x_p$.

Cauchy's Theorem

Proof (cont.)

Clearly, $(e, e, \ldots, e) \in P$, and the orbit containing it has size 1.

Excluding $(e, \ldots, e)$, there are $|G|^{p-1} - 1$ other elements in P, and these are partitioned into orbits of size 1 or p.

Since $p \nmid |G|^{p-1} - 1$, there must be some other orbit of size 1.

Thus, there is some $(x, x, \ldots, x) \in P$, with $x \neq e$ such that $x^p = e$. $\square$

Corollary

If p is a prime number dividing $|G|$, then G has a subgroup of order p.

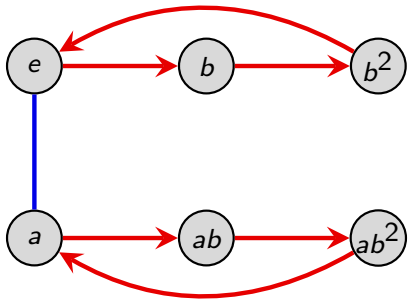
Note that just by using the theory of group actions, and the orbit-stabilzer theorem, we have already proven:

- Cayley's theorem: Every group G is isomorphic to a group of permutations.
- The size of a conjugacy class divides the size of G.
- Cauchy's theorem: If p divides $|G|$, then G has an element of order p.

Classification of groups of order 6

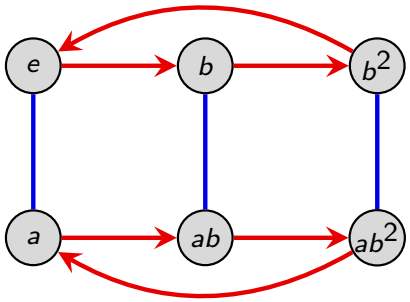
By Cauchy's theorem, every group of order 6 must have an element a of order 2, and an element b of order 3.

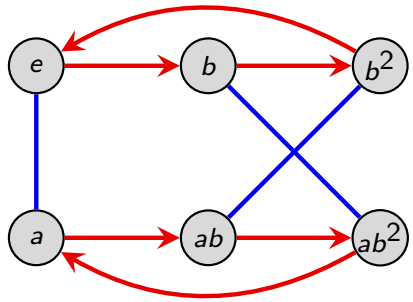
Clearly, $G = \langle a, b \rangle$ for two such elements. Thus, G must have a Cayley diagram that looks like the following:



It is now easy to see that up to isomorphism, there are only 2 groups of order 6:

$C_6 \cong C_2 \times C_3$





D_3

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**: There are 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. For example, C_1, C_4, V_4, D_4 and Q_8 are all 2-groups.

p-group Lemma

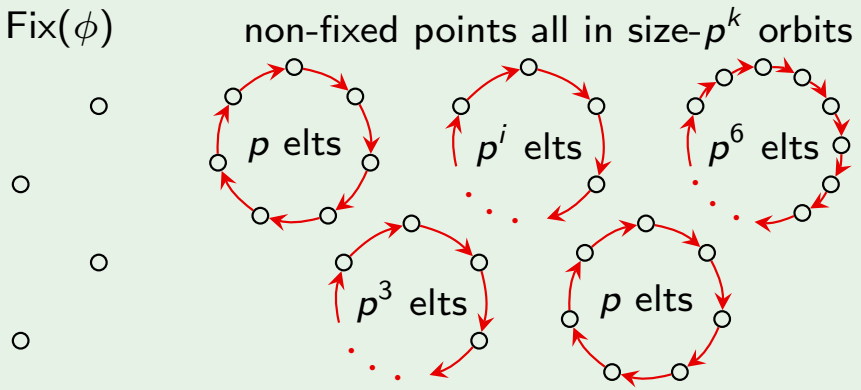
If a p-group G acts on a set S via $\phi\colon G \to \text{Perm}(S)$, then

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

Proof (sketch)

Suppose $|G| = p^n$.

By the Orbit-Stabilizer theorem, the only possible orbit sizes are $1, p, p^2, \ldots, p^n$.



Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Proof

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

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

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

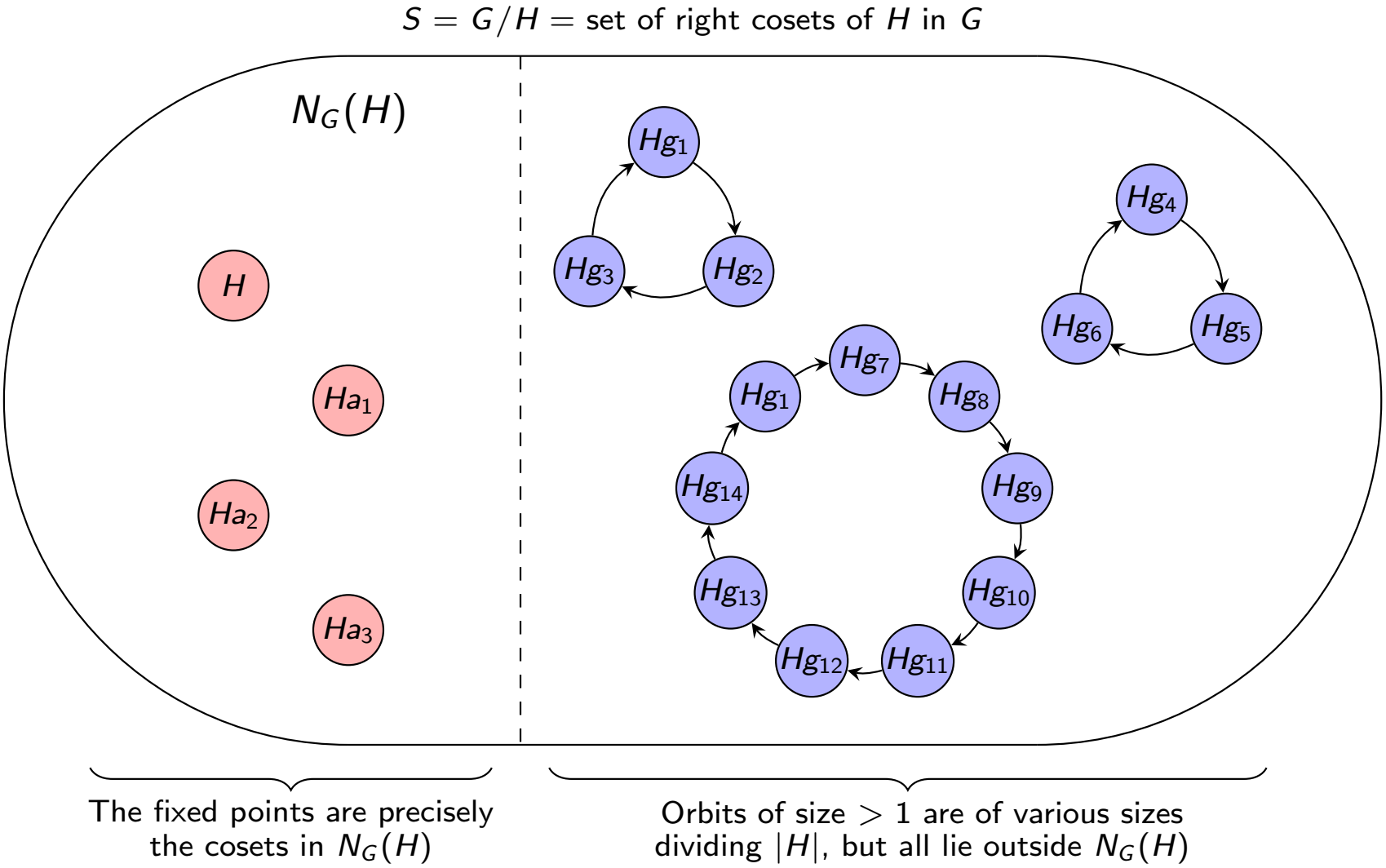
$$\begin{aligned} Hxh = Hx, \quad \forall h \in H \quad &\iff \quad Hxhx^{-1} = H, \quad \forall h \in H \\ &\iff \quad xhx^{-1} \in H, \quad \forall h \in H \\ &\iff \quad x \in N_G(H)\,. \end{aligned}$$

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 $S = G/H$, from the proof of the Normalizer Lemma.



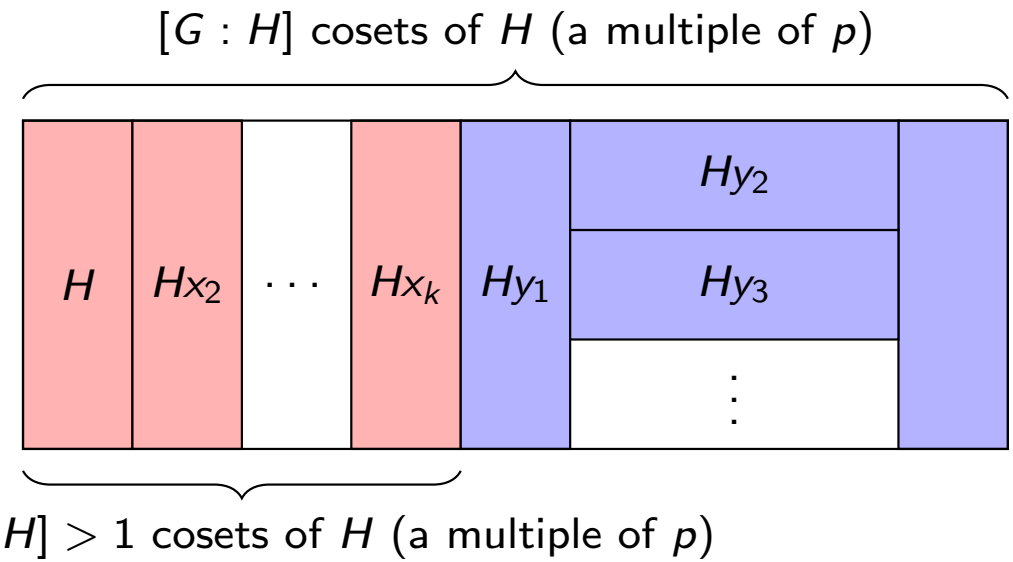
p-subgroups

The following result will be useful in proving the first Sylow theorem.

The 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.

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



Conclusions:

- $H = N_G(H)$ is impossible!
- p^{i+1} divides $|N_G(H)|$.

Proof of the normalizer lemma

The 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 $H \lhd N_G(H)$, 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. $\square$

The Sylow theorems

The Sylow theorems are about one question:

What finite groups are there?

Early on, we saw five families of groups: cyclic, dihedral, abelian, symmetric, alternating.

Later, we classified all (finitely generated) *abelian* groups.

But what *other* groups are there, and what do they look like? For example, for a fixed order $|G|$, we may ask the following questions about G:

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

There is no one general method to answer this for any given order.

However, the Sylow Theorems, developed by Norwegian mathematician Peter Sylow (1832–1918), are powerful tools that help us attack this question.

p-subgroups

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

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 $|G|$.

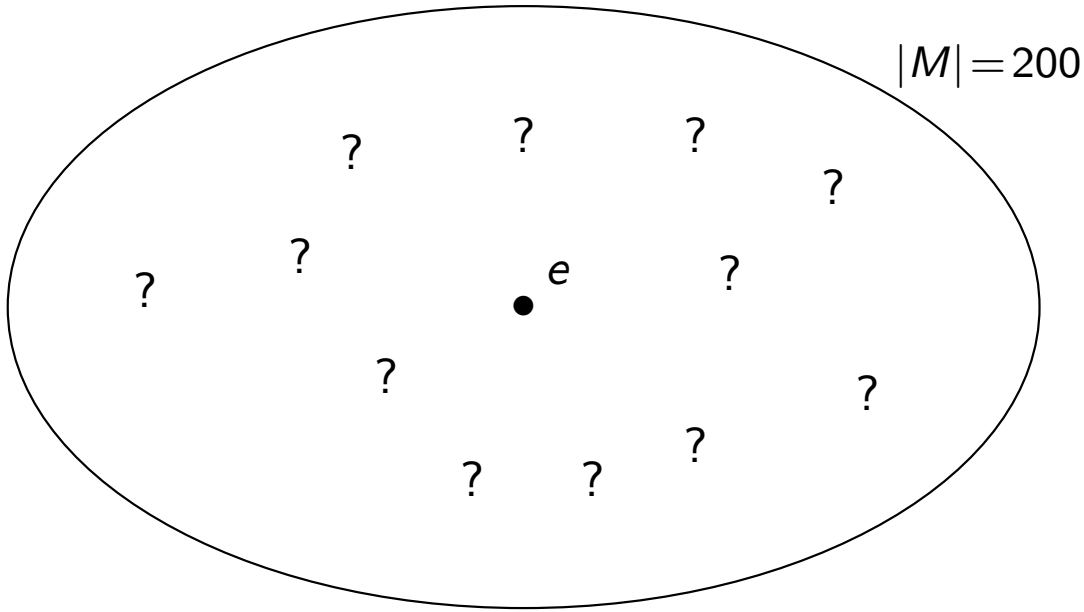
There are three Sylow theorems, and loosely speaking, they describe the following about a group's p-subgroups:

1. **Existence**: In every group, p-subgroups of all possible sizes exist.
2. **Relationship**: All maximal p-subgroups are conjugate.
3. **Number**: There are 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.

Our unknown group of order 200

Throughout our two lectures on the Sylow theorems, we will have a running example, a "mystery group" M of order 200.



Using *only* the fact that $|M| = 200$, we will unconver as much about the structure of M as we can.

We actually already know a little bit. Recall Cauchy's theorem:

Cauchy's theorem

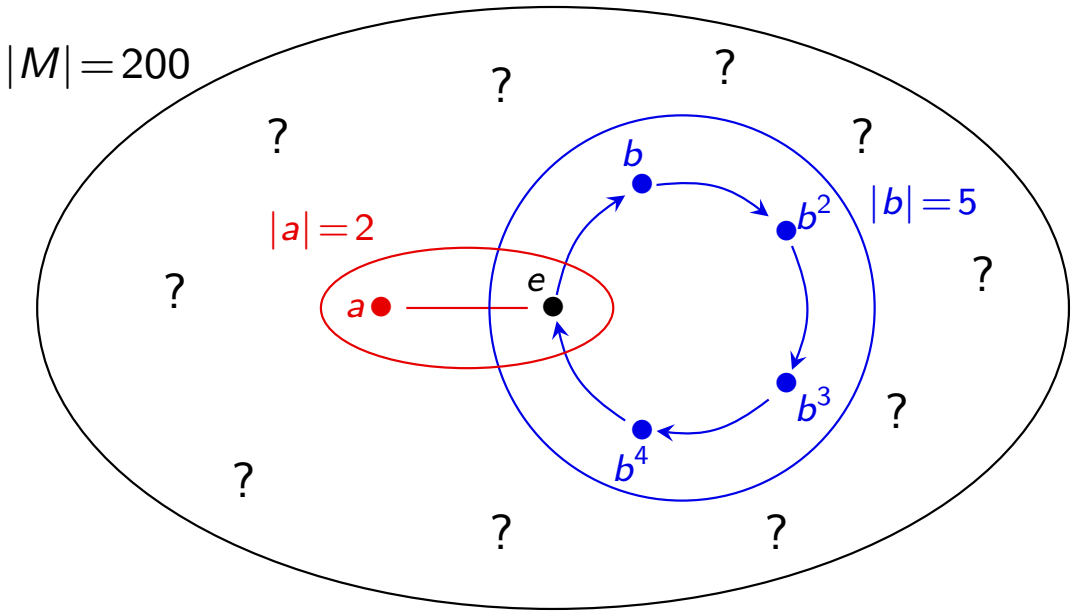
If p is a prime number dividing $|G|$, then G has an element g of order p.

Our mystery group of order 200

Since our mystery group M has order $|M| = 2^3 \cdot 5^2 = 200$, Cauchy's theorem tells us that:

- M has an element a of order 2;
- M has an element b of order 5;

Also, by Lagrange's theorem, $\langle a \rangle \cap \langle b \rangle = \{e\}$.



The 1st 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 p-subgroup with fewer than p^n elements sits inside one of the larger p-subgroups.

The First Sylow Theorem is in a sense, a generalization of Cauchy's theorem. Here is a comparison:

Cauchy's Theorem	First Sylow Theorem
If p divides $\|G\|$, then ...	*If p^k divides $\|G\|$, then ...*
There is a subgroup of order p	There is a subgroup of order p^k
which is cyclic and has no non-trivial proper subgroups.	which has subgroups of order $1, p, p^2 \ldots p^k$.
G contains an element of order p	G might not contain an element of order p^k.

The 1st Sylow Theorem: Existence of p-subgroups

Proof

The trivial subgroup $\{e\}$ has order $p^0 = 1$.

Big idea: Suppose we're given a subgroup $H < G$ of order $p^i < p^n$. We will construct a subgroup H' of order p^{i+1}.

By the normalizer lemma, $H \lneq N_G(H)$, and the order of the quotient group $N_G(H)/H$ is a multiple of p.

By Cauchy's Theorem, $N_G(H)/H$ contains an element (a coset!) of order p. Call this element aH. Note that $\langle aH \rangle$ is cyclic of order p.

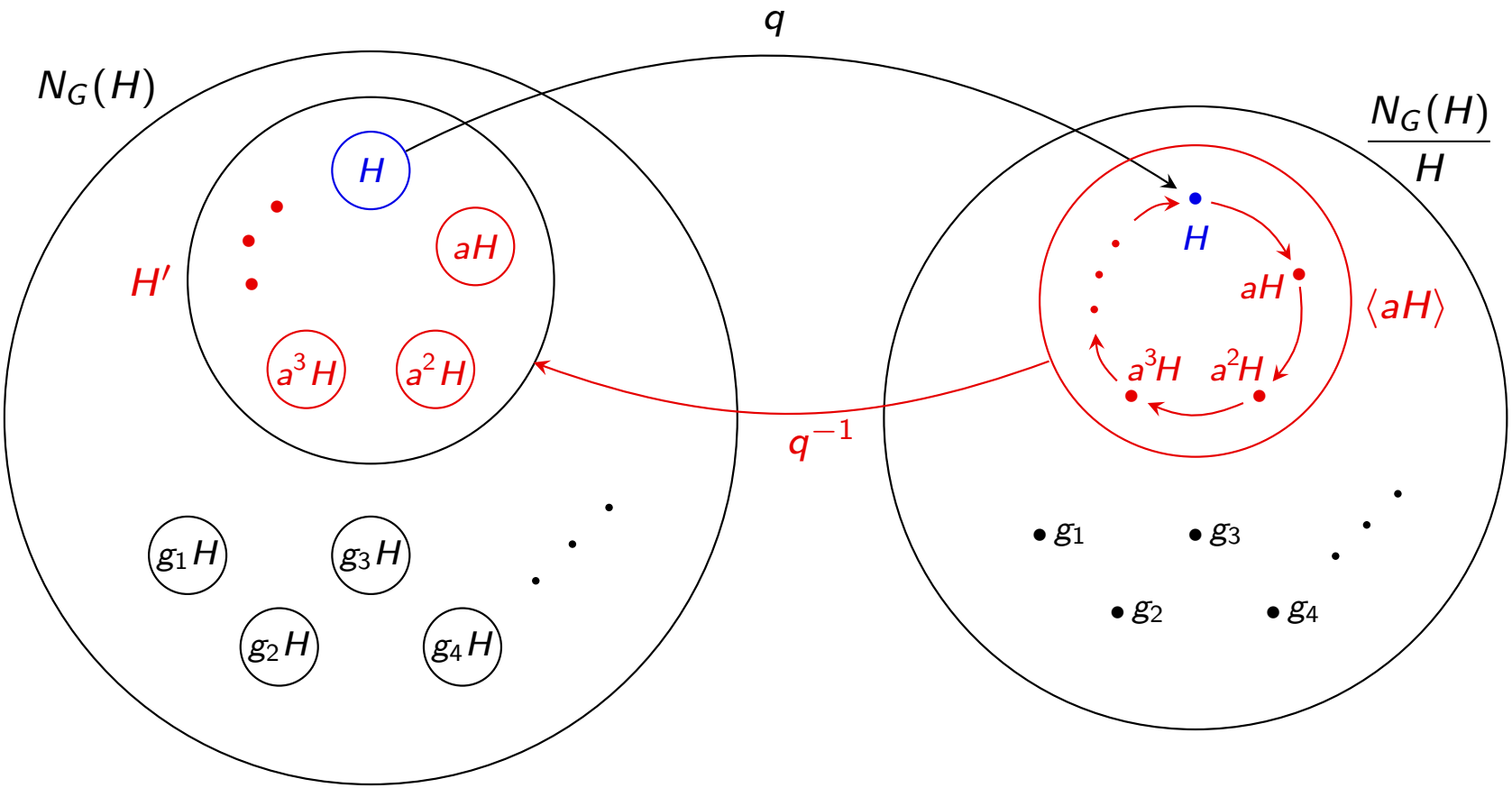
Claim: The preimage of $\langle aH \rangle$ under the quotient $q \colon N_G(H) \to N_G(H)/H$ is the subgroup H' we seek.

The preimages $q^{-1}(H)$, $q^{-1}(aH)$, $q^{-1}(a^2H)$, $\ldots$, $q^{-1}(a^{p-1}H)$ are all distinct cosets of H in $N_G(H)$, each of size p^i.

Thus, the preimage $H' = q^{-1}(\langle aH \rangle)$ contains $p \cdot |H| = p^{i+1}$ elements. $\square$

The 1st Sylow Theorem: Existence of p-subgroups

Here is a picture of how we found the group $H' = q^{-1}(\langle aH \rangle)$.

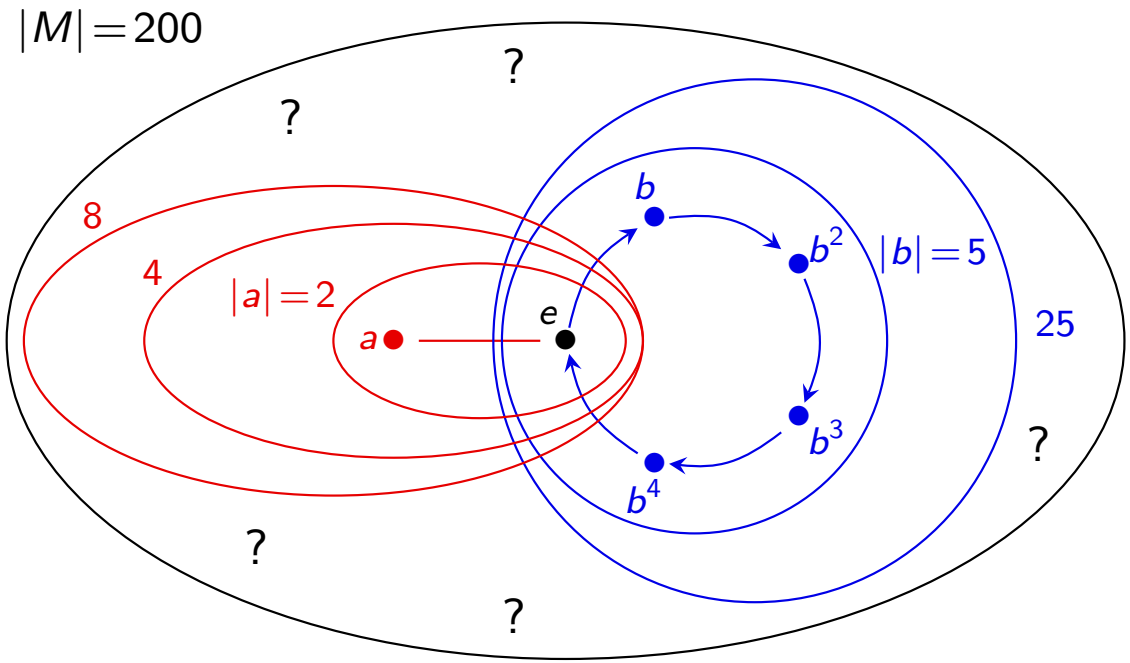


Since $|H| = p^i$, the subgroup $H' = \bigcup_{k=0}^{p-1} a^k H$ contains $p \cdot |H| = p^{i+1}$ elements.

Our unknown group of order 200

We now know a little bit more about the structure of our mystery group of order $|M| = 2^3 \cdot 5^2$:

- M has a 2-subgroup P_2 of order $2^3 = 8$;
- M has a 5-subgroup P_5 of order $25 = 5^2$;
- Each of these subgroups contains a nested chain of p-subgroups, down to the trivial group, $\{e\}$.



The 2nd Sylow Theorem: Relationship among p-subgroups

Definition

A subgroup $H < G$ of order p^n, where $|G| = p^n \cdot m$ with $p \nmid m$ is called a Sylow p-subgroup of G. Let $\text{Syl}_p(G)$ denote the set of Sylow p-subgroups of G.

Second Sylow Theorem

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

Proof

Let $H < G$ be any Sylow p-subgroup of G, and let $S = G/H = \{Hg \mid g \in G\}$, the set of right cosets of H.

Pick *any other* Sylow p-subgroup K of G. (If there is none, the result is trivial.)

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

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

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

Proof

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

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

Thus, if ϕ has a fixed point Hg, then H and K are conjugate by g, and we're done!

All we need to do is show that $|\operatorname{Fix}(\phi)| \not\equiv_p 0$.

By the p-group Lemma, $|\operatorname{Fix}(\phi)| \equiv_p |S|$. Recall that $|S| = [G, H]$.

Since H is a Sylow p-subgroup, $|H| = p^n$. By Lagrange's Theorem,

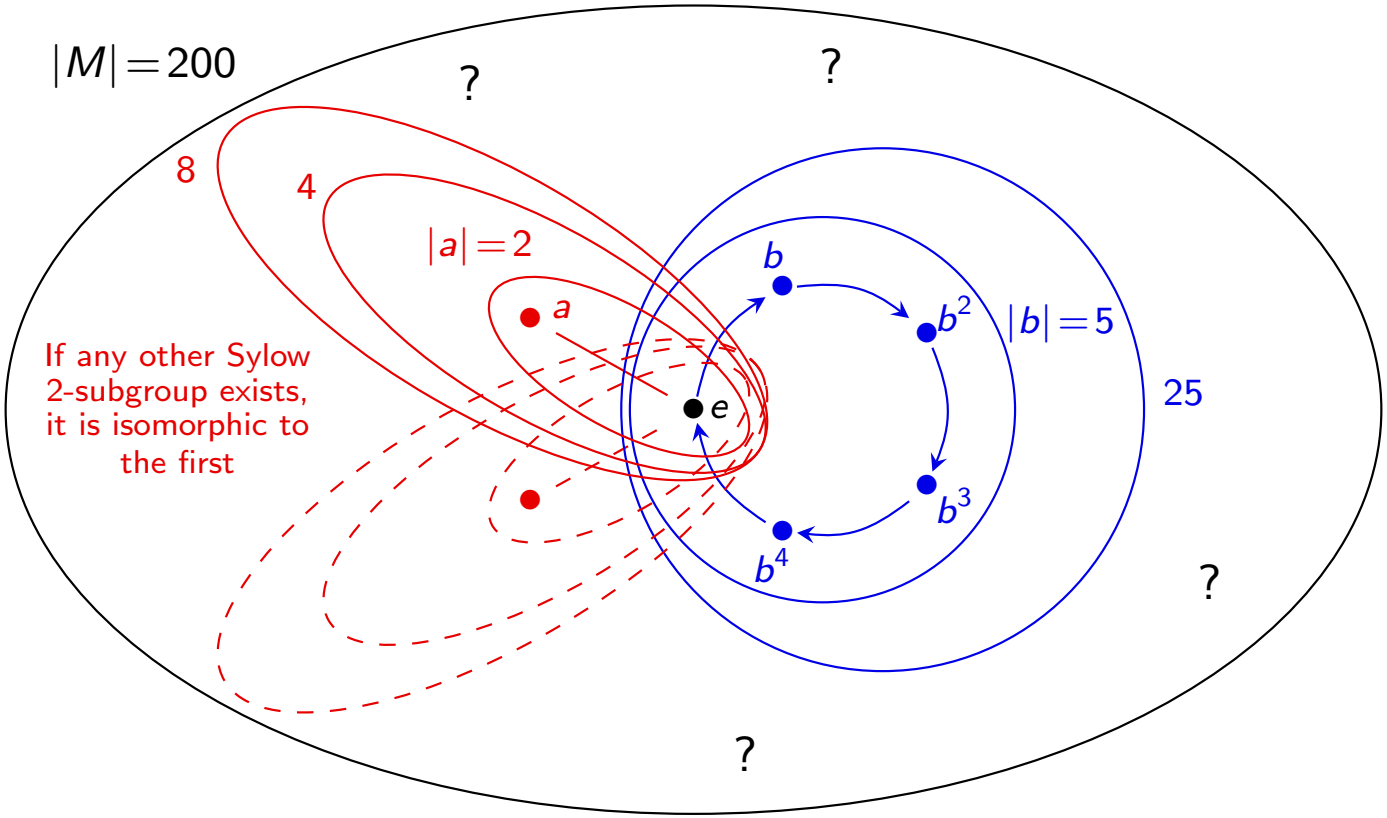
$$|S| = [G\colon H] = \frac{|G|}{|H|} = \frac{p^n m}{p^n} = m, \qquad p \nmid m\,.$$

Therefore, $|\operatorname{Fix}(\phi)| \equiv_p m \not\equiv_p 0$. □

Our unknown group of order 200

We now know even more about the structure of our mystery group M, of order $|M| = 2^3 \cdot 5^2$:

- If M has any other Sylow 2-subgroup, it is isomorphic to P_2;
- If M has any other Sylow 5-subgroup, it is isomorphic to P_5.



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

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

$$\phi(g) = \text{the permutation sending each } H \text{ to } g^{-1}Hg.$$

By the Second Sylow Theorem, all Sylow p-subgroups are conjugate! Thus there is only one orbit, $\text{Orb}(H)$, of size $n_p = |S|$.

By the Orbit-Stabilizer Theorem,

$$\underbrace{|\text{Orb}(H)|}_{=n_p} \cdot |\text{Stab}(H)| = |G| \qquad \Longrightarrow \qquad n_p \text{ divides } |G|\,.$$

The 3rd Sylow Theorem: Number of p-subgroups

Proof (cont.)

Now, pick any $H \in \mathrm{Syl}_p(G) = S$. The group H acts on S by conjugation, via $\theta\colon H \to \mathrm{Perm}(S)$, where

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

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

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

We know that:

- H and K are Sylow p-subgroups of G, but also of $N_G(K)$.
- Thus, H and K are conjugate in $N_G(K)$. (2nd Sylow Thm.)
- $K \lhd N_G(K)$, thus the only conjugate of K in $N_G(K)$ is itself.

Thus, $K = H$. That is, $\mathrm{Fix}(\theta) = \{H\}$ contains only 1 element.

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

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 $p, p^2, \ldots, p^n$.

For the 2^{nd} and 3^{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 $|\operatorname{Orb}(s)| \cdot |\operatorname{Stab}(s)| = |G|$.

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

To summarize, we used:

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

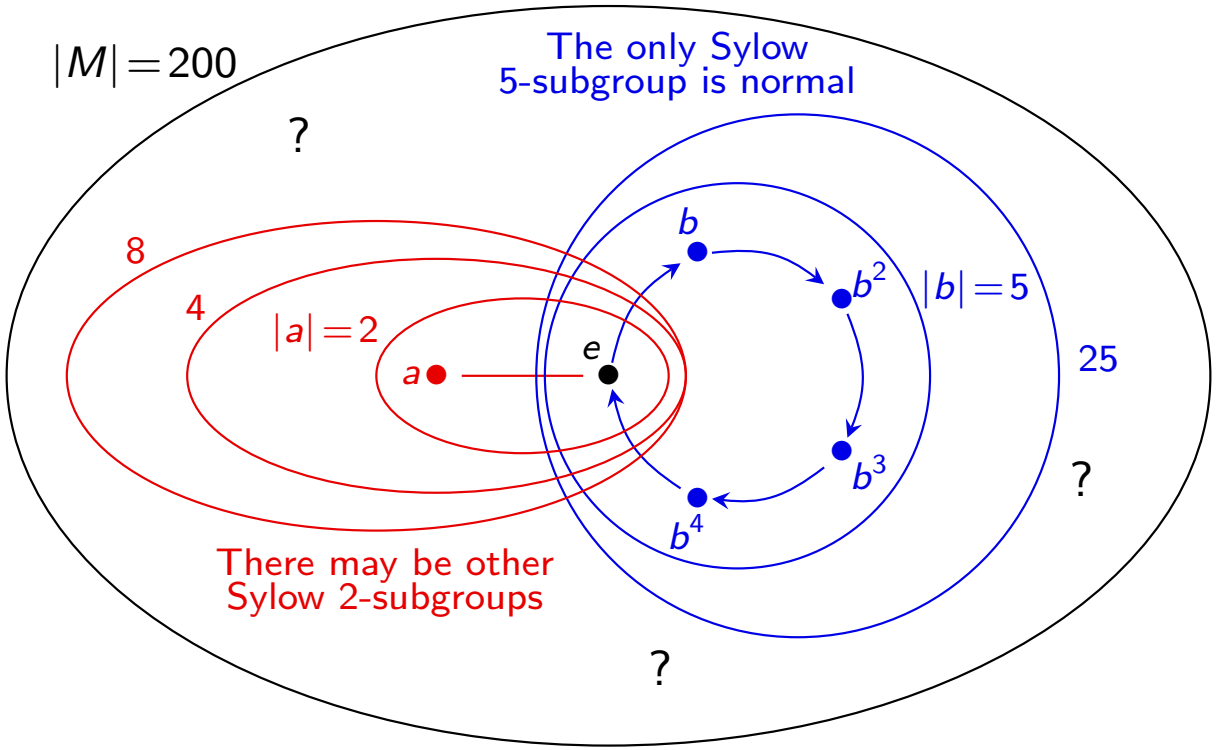
S3a The action of G on $S = \operatorname{Syl}_p(G)$, by conjugation.

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

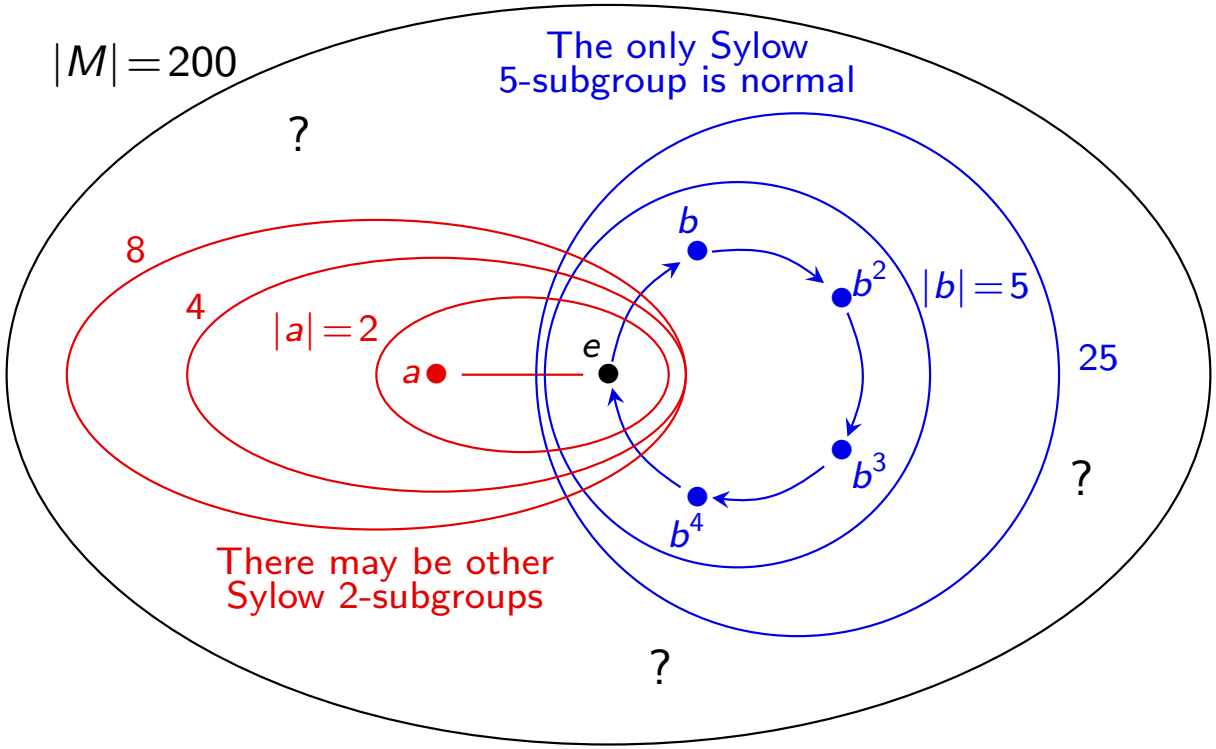
Our unknown group of order 200

We now know a little bit more about the structure of our mystery group M, of order $|M| = 2^3 \cdot 5^2 = 200$:

- $n_5 \mid 8$, thus $n_5 \in \{1, 2, 4, 8\}$. But $n_5 \equiv_5 1$, so $n_5 = 1$.
- $n_2 \mid 25$ and is odd. Thus $n_2 \in \{1, 5, 25\}$.
- We conclude that M has a unique (and hence normal) Sylow 5-subgroup P_5 (of order $5^2 = 25$), and either 1, 5, or 25 Sylow 2-subgroups (of order $2^3 = 8$).



Our unknown group of order 200



Suppose M has a subgroup isomorphic to D_4.

This would be a Sylow 2-subgroup. Since all of them are conjugate, M *cannot* contain a subgroup isomorphic to Q_8, $C_4 \times C_2$, or C_8!

In particular, M cannot even contain an element of order 8. (Why?)

Simple groups and the Sylow theorems

Definition

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

Since all Sylow p-subgroups are conjugate, the following result is straightforward:

Proposition (HW)

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

The Sylow theorems are very useful for establishing statements like:

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

To do this, we usually just need to show that $n_p = 1$ for some p dividing $|G|$.

Since we established $n_5 = 1$ for our running example of a group of size $|M| = 200 = 2^3 \cdot 5^2$, there are no simple groups of order 200.

An easy example

Tip

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

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 $n_3 \in \{1, \cancel{2}, 4, 7, \cancel{14}, 28\}$.
- 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

If $H \lneq G$ and $|G|$ does not divide $[G : H]!$, then G cannot be simple.

Proof

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

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

Recall that the kernel of ϕ is the intersection of all conjugate subgroups of H:

$$\text{Ker}\,\phi = \bigcap_{x \in G} x^{-1}Hx.$$

Notice that $\langle e \rangle \leq \text{Ker}\,\phi \leq H \lneq G$, and $\text{Ker}\,\phi \lhd G$.

If $\text{Ker}\,\phi = \langle e \rangle$ then $\phi\colon G \hookrightarrow S_n$ is an embedding. But this is *impossible* because $|G|$ does not divide $|S_n| = [G : H]!$. □

Corollary

There are no simple groups of order 24.

Theorem (classification of finite simple groups)

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

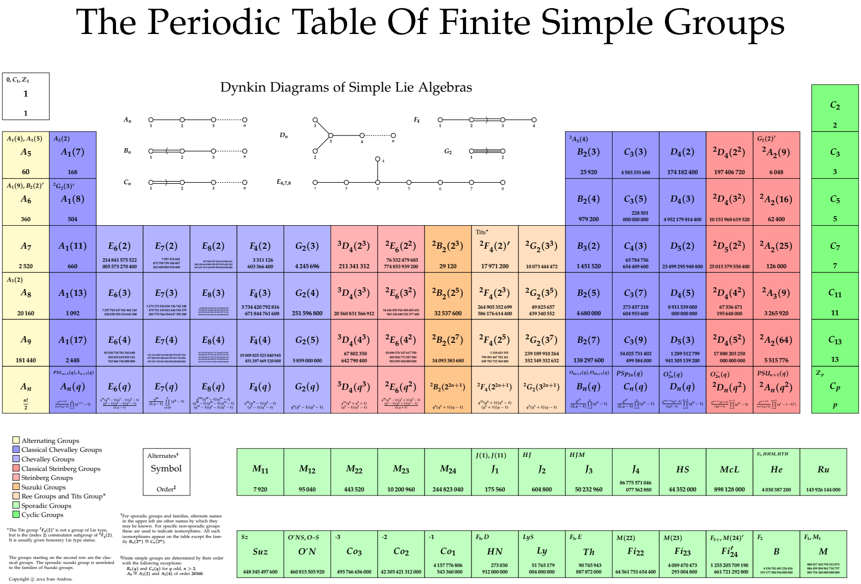
$$|B| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \approx 4.15 \times 10^{33};$$

- "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™

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