

Chapter 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 *permute* 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 *permute* 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.

The rich theory of group actions can be used to prove many deep results in group theory.

We have actually already seen many group actions, without knowing it, such as:

- groups acting on themselves by multiplication
- groups acting on themselves by conjugation
- groups acting on their subgroup by conjugation
- groups acting on cosets by multiplication.

Actions vs. configurations

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

1	2
4	3

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

$$1, \quad r, \quad r^2, \quad r^3, \quad f, \quad rf, \quad r^2f, \quad r^3f.$$

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

1	2
4	3

4	1
3	2

3	4
2	1

2	3
1	4

2	1
3	4

3	2
4	1

4	3
1	2

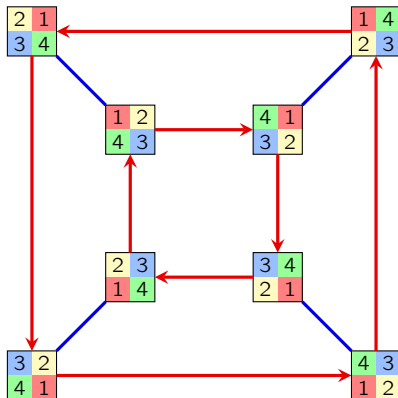
1	4
2	3

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

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

Action 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.

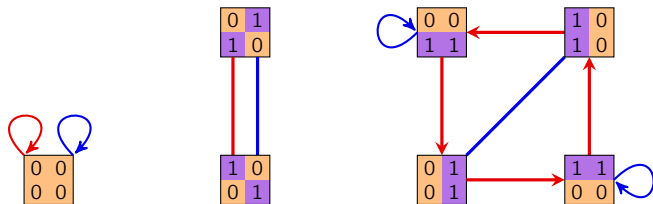
Actions diagrams

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.”

$$S = \left\{ \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 0 & 0 \\ \hline \end{array}, \begin{array}{|c|c|} \hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array}, \begin{array}{|c|c|} \hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array}, \begin{array}{|c|c|} \hline 1 & 1 \\ \hline 0 & 0 \\ \hline \end{array}, \begin{array}{|c|c|} \hline 0 & 1 \\ \hline 0 & 1 \\ \hline \end{array}, \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 1 & 1 \\ \hline \end{array}, \begin{array}{|c|c|} \hline 1 & 0 \\ \hline 1 & 0 \\ \hline \end{array} \right\}$$

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.

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,

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

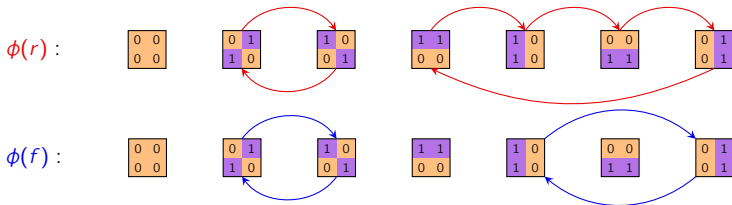
Let $\text{Perm}(S)$ be the group of permutations of S . Thus, if $|S| = n$, then $\text{Perm}(S) \cong S_n$. (We typically think of S_n as the permutations of $\{1, 2, \dots, n\}$.)

Definition

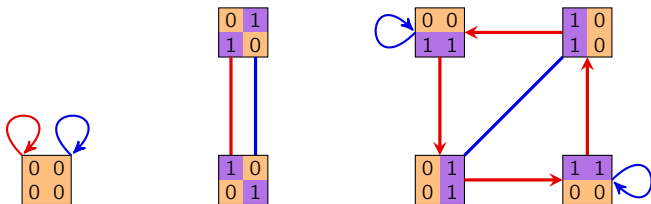
A group G **acts on** a set S if there is a homomorphism $\phi: G \rightarrow \text{Perm}(S)$.

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 diagram:

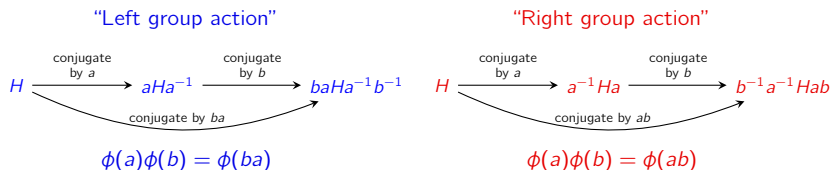


Left actions vs. right actions (an annoyance we can deal with)

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:



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:

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

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

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

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 theorems for left actions hold for right actions.

Generally, each left action has a related right action. **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 $\phi(g).s$.

Cayley diagrams as action diagrams

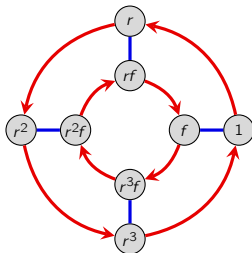
Every Cayley diagram is the action diagram of a particular (right) group action.

For example, consider the group $G = D_4 = \langle r, f \rangle$ acting on itself. That is,

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

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.”

Five features of every group action

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

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 $\phi: G \rightarrow \text{Perm}(S)$.

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

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

- (ii) The **stabilizer** of s in G is

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

In terms of the action diagram

- (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: fixed point sets

Our first two local features were specific to a certain element $s \in S$.

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

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

Definition

Suppose that G acts on a set S (on the right) via $\phi: G \rightarrow \text{Perm}(S)$.

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

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

In terms of the action diagram

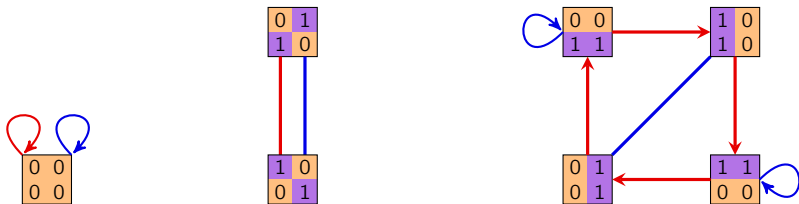
(iii) The **fixed point set** of $g \in S$ are the nodes from which the g -paths are loops.

In terms of the “group switchboard analogy”

- (i) The **orbit** of $s \in S$ are the elements in S that can be obtained by pressing some combination of buttons.
- (ii) The **stabilizer** of $s \in S$ consists of the buttons that have no effect on s .
- (iii) The **fixed point set** 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 fixed point sets

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



The **stabilizers** are:

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

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

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








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

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

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

Local duality: stabilizers vs. fixed point sets

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

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

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

The stabilizer subgroup

Notice how in our example, the stabilizer of each $s \in S$ was a subgroup.

This holds true for any action.

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) **Identity.** That is, $s.\phi(e) = s$.
- (ii) **Inverses.** 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 $s.\phi(gh) = s$.

Alternatively, it suffices to show that if $s.\phi(g) = s$ and $s.\phi(h) = s$, then $s.\phi(gh^{-1}) = s$,

You'll do this on the homework.

All three of these are very intuitive in our our switchboard analogy.

The stabilizer subgroup

As we've seen, elements in the same orbit can have different stabilizers.

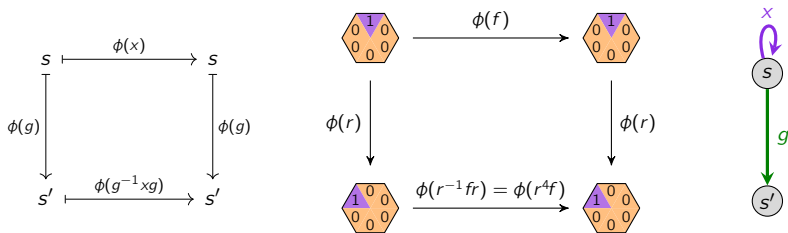
Proposition (HW exercise)

Set elements in the same orbit have **conjugate stabilizers**:

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

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

Here are several ways to visualize what this means and why.



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

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 a familiar concept in this new setting.

Definition

Suppose that G acts on a set S via $\phi: G \rightarrow \text{Perm}(S)$.

(iv) The **kernel** of the action is the set

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

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

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

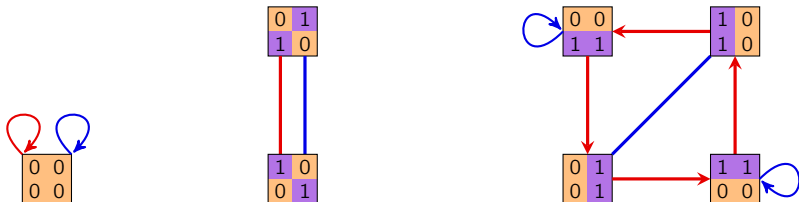
Proposition (global duality: fixed points vs. kernel)

Suppose that G acts on a set S via $\phi: G \rightarrow \text{Perm}(S)$. Then

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

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

Two global features: fixed points and the kernel



In terms of the action diagram








- (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 .

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

- the **fixed point set** 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 some key intuition 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 group 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 $\phi: G \rightarrow \text{Perm}(S)$, and any $s \in S$,

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

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

Proof

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

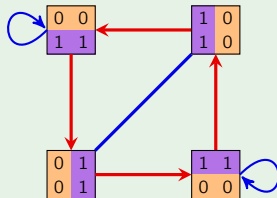
That is, “two g -buttons send s to the same place iff they’re in the same coset”.

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

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

$\text{stab}(s) = \langle f \rangle$.

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



Note that $s \cdot \phi(g) = s \cdot \phi(k)$ 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:

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

“ \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.

Our second theorem on orbits

Orbit-counting theorem

Let a finite group G act on a set S via $\phi: G \rightarrow \text{Perm}(S)$. Then

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

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

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

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

Proof

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

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

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

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

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

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

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, fixed point sets, fixed points, and kernel.

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

Theorems that we have observed but haven't been able to prove yet will fall in our lap!

Groups acting on themselves by right-multiplication

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

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

- there is only one **orbit**: $\text{orb}(x) = G$, for all $x \in G$
- the **stabilizer** of each $x \in G$ is $\text{stab}(x) = \langle e \rangle$
- the **fixed point set** of each $g \in G$ is $\text{fix}(g) = \{e\}$
- the **fixed points** and **kernel** are both trivial:

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

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

$$\phi: G \longrightarrow \text{Perm}(S) \cong S_n.$$

Since $\text{Ker}(\phi) = \langle e \rangle$, it 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**:

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

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

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

- 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 **fixed point set** of $g \in G$ is also its centralizer, because

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

- 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:

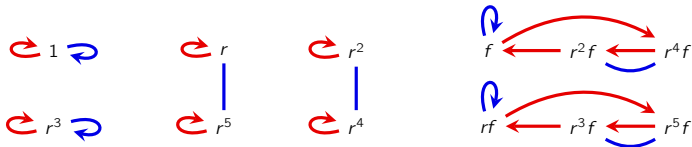
1. **Orbit-stabilizer theorem.** “the *size of an orbit* is the *index of the stabilizer*”:

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

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

#conjugacy classes of G = 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 $\text{stab}(r) = \text{stab}(r^2) = \text{stab}(r^4) = \text{stab}(r^5) = \langle r \rangle$,

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

Groups acting on themselves by conjugation

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

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

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

Groups acting on subgroups by conjugation

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

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

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**:

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

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

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

- The **fixed point set** of g are the **subgroups that g normalizes**:

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

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

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

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

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

Groups acting on subgroups by conjugation

Let's apply our two theorems:

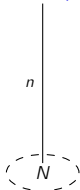
1. **Orbit-stabilizer theorem.** "the *size of an orbit* is the *index of the stabilizer*":

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

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

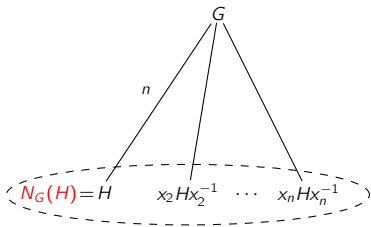
#conjugacy classes of subgroups of G = average size of a normalizer.

$$G = N_G(N)$$



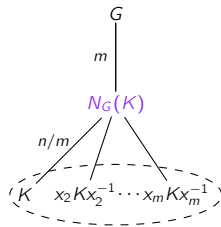
normal

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



fully unnormal

$$|\text{cl}_G(H)| = [G : H]; \text{ as large as possible}$$



moderately unnormal

$$1 < |\text{cl}_G(K)| < [G : K]$$

Groups acting on subgroups by conjugation

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

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

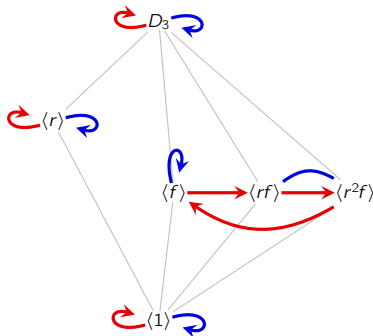
$$\tau(r) = \langle 1 \rangle \quad \langle r \rangle \quad \langle f \rangle \xrightarrow{\text{red}} \langle rf \rangle \xrightarrow{\text{red}} \langle r^2f \rangle \quad D_3$$

$$\tau(r^2) = \langle 1 \rangle \quad \langle r \rangle \quad \langle f \rangle \xrightarrow{\text{blue}} \langle rf \rangle \xrightarrow{\text{blue}} \langle r^2f \rangle \quad D_3$$

$$\tau(f) = \langle 1 \rangle \quad \langle r \rangle \quad \langle f \rangle \xrightarrow{\text{red}} \langle rf \rangle \xrightarrow{\text{red}} \langle r^2f \rangle \quad D_3$$

$$\tau(rf) = \langle 1 \rangle \quad \langle r \rangle \quad \langle f \rangle \xrightarrow{\text{blue}} \langle rf \rangle \xrightarrow{\text{blue}} \langle r^2f \rangle \quad D_3$$

$$\tau(r^2f) = \langle 1 \rangle \quad \langle r \rangle \quad \langle f \rangle \xrightarrow{\text{red}} \langle rf \rangle \xrightarrow{\text{red}} \langle r^2f \rangle \quad D_3$$



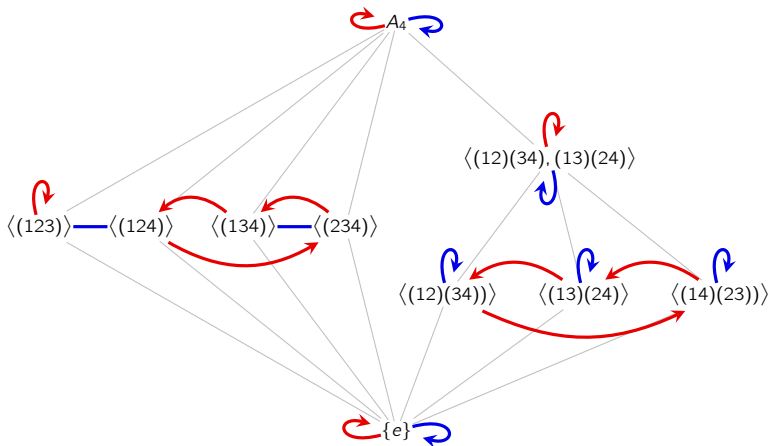
Observations

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

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

Groups acting on subgroups by conjugation

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



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

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

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 $|\text{Orb}(\phi)| = 60/|A_4| = 5$ 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**:

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

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** $x^{-1}Hx$:

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

- The doesn't seem to be a standard term for the **fixed point set** of g :

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

- 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 :

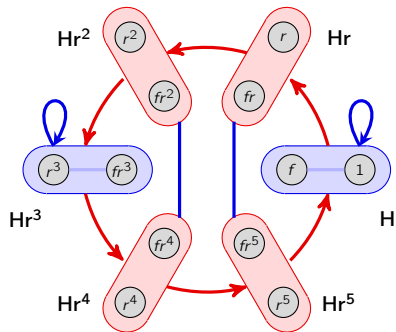
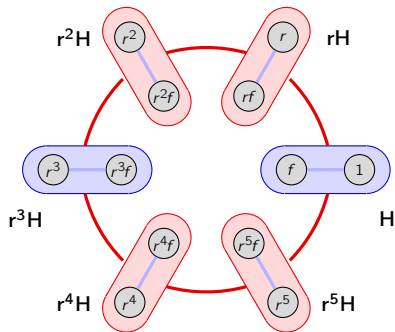
$$\text{Ker } \phi = \bigcap_{x \in G} \text{stab}(x) = \bigcap_{x \in G} x^{-1}Hx.$$

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

Groups acting on cosets of H by right-multiplication

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

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



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

$$\phi: G \longrightarrow S_3.$$

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

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

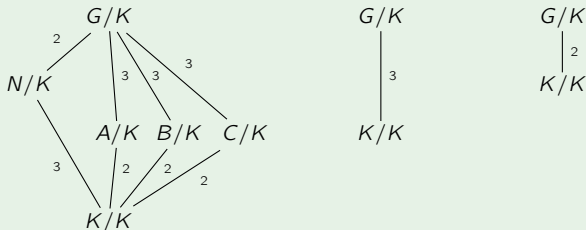
Subgroups of small index

Proof (contin.)

Thus, there are three cases for this quotient:

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

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



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

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

$$\phi: G \longrightarrow S_p.$$

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

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

$$\begin{array}{ccc} G & & G/K \cong S_p \\ | & & | \\ \rho & & \rho \\ H & & H/K \\ | & & | \\ q \text{ is not divisible by any prime } < p & & q \text{ divides } (p-1)! \\ K & & K/K \end{array}$$

Do you see why $q = 1$?

□

Subgroups of small index

Recall that G is **simple** if its only normal subgroups are G and $\langle e \rangle$.

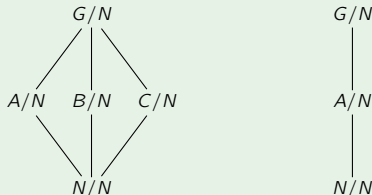
We just showed that if G is simple, then it cannot have a subgroup of index 2 or 3.

Proposition

If G is simple, then it cannot have a subgroup of index 4.

Proof

If $H \trianglelefteq G$ and $[G : H] = 4$, then $G/H \cong C_4$ or V_4 , so the subgroup lattice must be one of:



In either case, we would have $[G : A] = 2$ by the correspondence theorem.

This would give an index-2 subgroup $A \trianglelefteq G$, so G cannot be simple. □

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
$\text{orb}(s)$	all of G	$\text{cl}_G(g)$	$\text{cl}_G(H)$	all right cosets
$\text{stab}(s)$	$\{e\}$	$C_G(g)$	$N_G(H)$	$x^{-1}Hx$
$\text{fix}(g)$	$\{e\}$ or \emptyset	$C_G(g)$	$\{H \mid g \in N_G(H)\}$	
$\text{Ker}(\phi)$	$\{e\}$	$Z(G)$	$\bigcap_{H \leq G} N_G(H)$	largest norm. subgp. $N \leq H$
$\text{Fix}(\phi)$	none	$Z(G)$	normal subgroups	none

Actions of automorphism groups

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

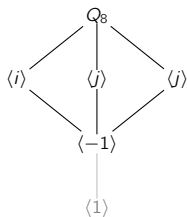
For any G , the automorphism group $\text{Aut}(G)$ naturally acts on $S = G$ via a homomorphism

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

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

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

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



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

	Z	iZ	jZ	kZ
	1	i	j	k
	-1	$-i$	$-j$	$-k$

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

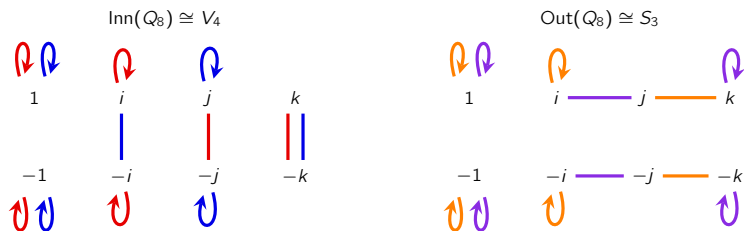
$\text{cl}(1)$	1	i	j	k
$\text{cl}(-1)$	-1	$-i$	$-j$	$-k$
		$\text{cl}(i)$	$\text{cl}(j)$	$\text{cl}(k)$

inner automorphisms of Q_8 permute elements within conjugacy classes

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

Automorphisms of Q_8

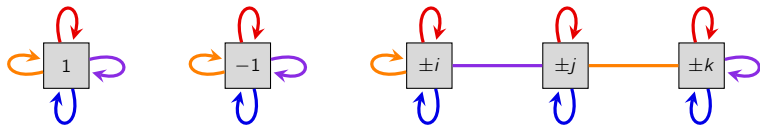
All three groups $\text{Aut}(Q_8)$, $\text{Inn}(Q_8)$, and $\text{Out}(Q_8) \cong \text{Aut}(Q_8)/\text{Inn}(Q_8)$ act on $S = Q_8$.



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

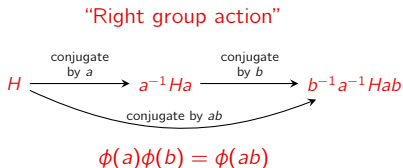
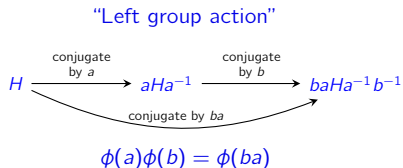
$$\text{Aut}(Q_8) \cong \text{Inn}(Q_8) \rtimes \text{Out}(Q_8) \cong V_4 \rtimes S_3 \cong S_4.$$

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

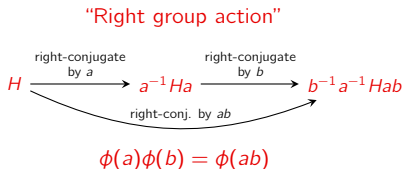
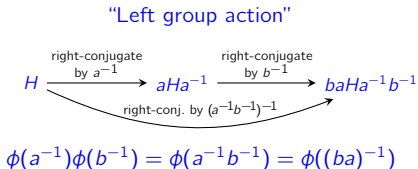


Action equivalence

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



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



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".

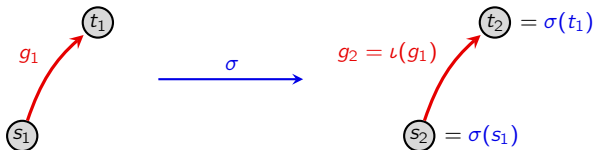
Action equivalence, informally

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

$$\phi_1: G_1 \longrightarrow \text{Perm}(S_1), \quad \text{and} \quad \phi_2: G_2 \longrightarrow \text{Perm}(S_2).$$

If these are “equivalent”, then we’ll need

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



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

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

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

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

Action equivalence, formally

Definition

Two actions $\phi_1: G_1 \rightarrow \text{Perm}(S_1)$ and $\phi_2: G_2 \rightarrow \text{Perm}(S_2)$ are **equivalent** if there is an isomorphism $\iota: G_1 \rightarrow G_2$ and a bijection $\sigma: S_1 \rightarrow S_2$ such that

$$\sigma \circ \phi_1(g) = \phi_2(\iota(g)) \circ \sigma, \quad \text{for all } g \in G_1.$$

We say that the resulting action diagrams are **action equivalent**.

This can be expressed with a **commutative diagram**:

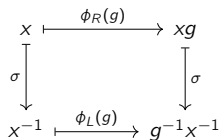
$$\begin{array}{ccc} S_1 & \xrightarrow{\phi_1(g)} & S_1 \\ \sigma \downarrow & & \downarrow \sigma \\ S_2 & \xrightarrow{\phi_2(\iota(g))} & S_2 \end{array}$$

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

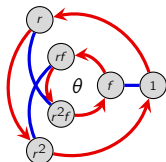
- defined $\phi(r)$ to rotate clockwise, and $\phi(f)$ to flip vertically
- used tiles with a and b , rather than 0 and 1
- read from right-to-left, rather than left-to-right, etc.

Every right action has an equivalent left action

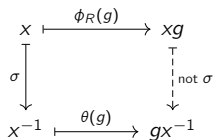
G acting on...	right action	equivalent left action
itself by multiplication	$x \mapsto xg$	$x \mapsto g^{-1}x$
itself by conjugation	$x \mapsto g^{-1}xg$	$x \mapsto gxg^{-1}$
its subgroups by conjugation	$H \mapsto g^{-1}Hg$	$H \mapsto gHg^{-1}$
cosets by multiplication	$H \mapsto Hg$	$H \mapsto g^{-1}H$



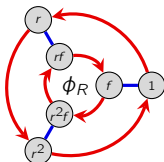
— $x \mapsto rx$
— $x \mapsto fx$



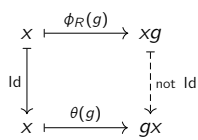
$\xleftarrow{\text{Id}}$
 not an equivalence



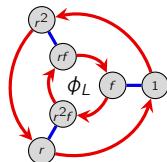
— $x \mapsto xr$
— $x \mapsto xf$



$\xrightarrow{\sigma}$
 action equivalence



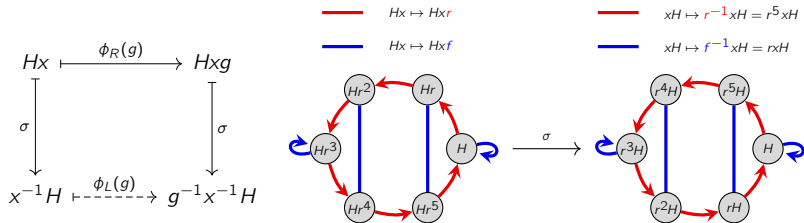
— $x \mapsto r^{-1}x = r^2x$
— $x \mapsto f^{-1}x = fx$



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 diagram for $S_3 = \langle (12), (23) \rangle$ with the set

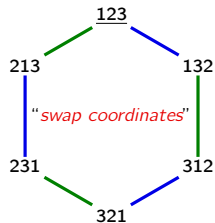
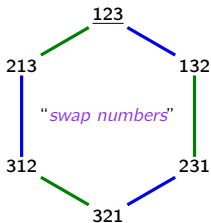
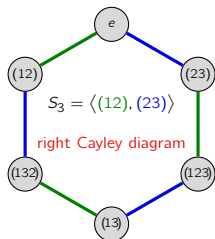
$$S = \{123, 132, 213, 231, 312, 321\}.$$

In one, (ij) can be interpreted to mean

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

Alternatively, (ij) could mean

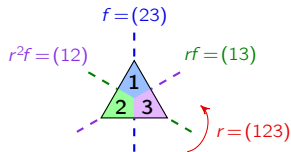
“swap the *numbers* i and j , regardless of where they are.”



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

where

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

$$\pi(1)\pi(2)\pi(3) \xrightarrow{\phi(r)} \pi(3)\pi(1)\pi(2), \quad \pi(1)\pi(2)\pi(3) \xrightarrow{\phi(f)} \pi(1)\pi(3)\pi(2).$$

This defines a *right action*, by the homomorphism

$$\phi_R: S_3 \longrightarrow \text{Perm}(S), \quad \phi_R(\tau): \pi(1)\pi(2)\pi(3) \longmapsto \pi(\tau(1))\pi(\tau(2))\pi(\tau(3)).$$

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

$$\phi_L: S_3 \longrightarrow \text{Perm}(S), \quad \phi_L(\tau): \pi(1)\pi(2)\pi(3) \longmapsto \tau^{-1}(\pi(1))\tau^{-1}(\pi(2))\tau^{-1}(\pi(3)).$$

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:

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

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

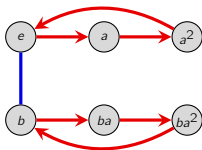
Since $p \nmid |G|^{p-1} - 1$, there must be other orbits of size 1. Thus, some $(x, \dots, x) \in P$, with $x \neq e$ satisfies $x^p = e$. \square

Classification of groups of order 6

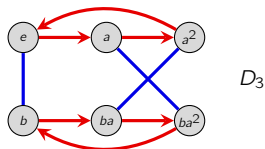
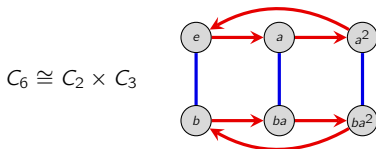
By Cauchy's theorem, every group of order 6 must have:

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

Clearly, $G = \langle a, b \rangle$, and so G must have the following "partial Cayley diagram":



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



Exercise. Classify groups of order 8 with a similar argument.

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 , $Pauli_1, \dots$

p -group Lemma

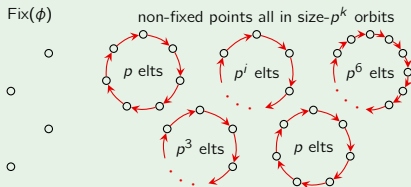
If a p -group G acts on a set S via $\phi: G \rightarrow \text{Perm}(S)$, then

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

Proof (sketch)

Suppose $|G| = p^n$.

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



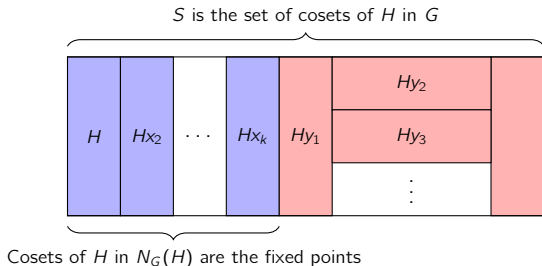
Normalizer lemma, Part 1

If H is a p -subgroup of G , then

$$[N_G(H) : H] \equiv_p [G : H].$$

Approach:

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



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

Normalizer lemma, Part 1

If H is a p -subgroup of G , then

$$[N_G(H) : H] \equiv_p [G : H].$$

Proof

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

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

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

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

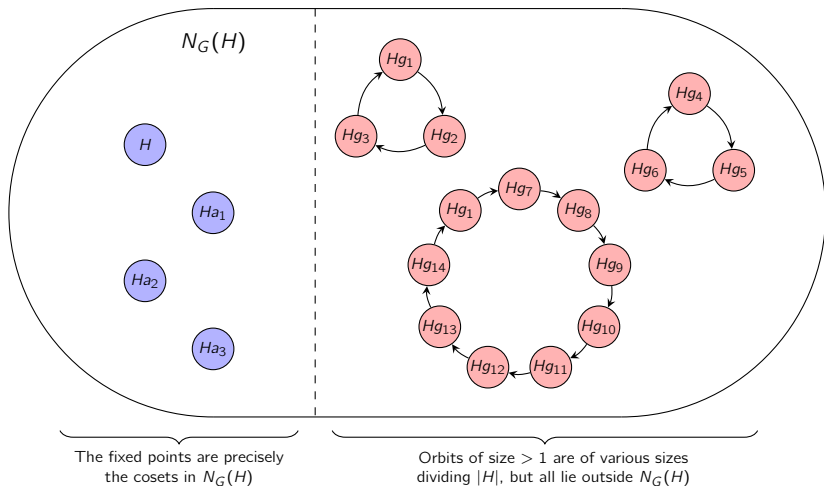
Therefore, $|\text{Fix}(\phi)| = [N_G(H) : H]$, and $|S| = [G : H]$. By our p -group Lemma,

$$|\text{Fix}(\phi)| \equiv_p |S| \implies [N_G(H) : H] \equiv_p [G : H]. \quad \square$$

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.

$S = G/H =$ set of right cosets of H in G

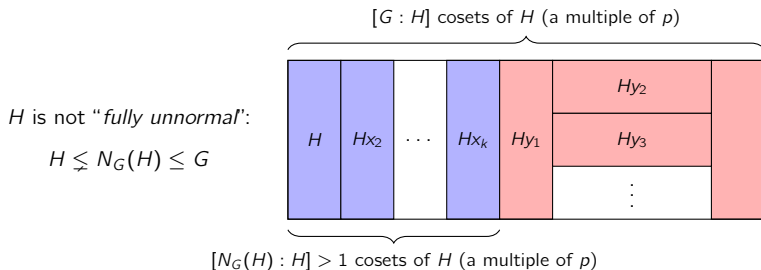


p -subgroups

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 $H \subsetneq N_G(H)$, and the index $[N_G(H) : H]$ is a multiple of p .



Important corollaries

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

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 $H \not\leq N_G(H)$, 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

$$q: N_G(H) \longrightarrow N_G(H)/H, \quad q: g \longmapsto gH.$$

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

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

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

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

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 :

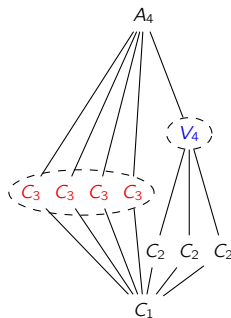
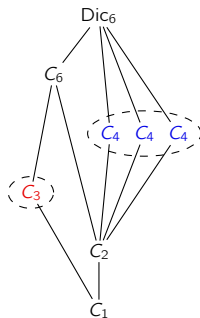
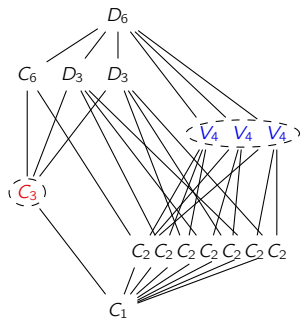
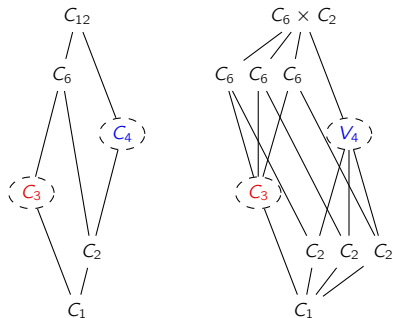
1. How big are its p -subgroups?
2. How are the p -subgroups related?
3. How many p -subgroups are there?
4. Are any of them normal?

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

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 $|G|$.

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

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

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, 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.

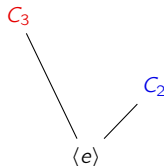
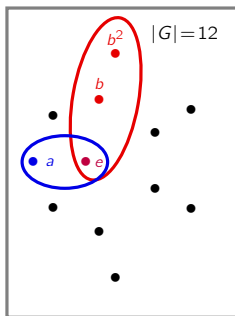
Together, these place strong restrictions on the structure of a group G with a fixed order.

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 uncover as much about its structure as we can.

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 non-Sylow p -subgroup sits inside a larger p -subgroup.

Proof

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

Big idea: Given a subgroup $H < G$ of order $p^j < p^n$, we'll construct H' of order p^{j+1} .

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

By Cauchy's theorem, $N_G(H)/H$ has an element aH of order p . Therefore, $\langle aH \rangle \cong C_p$.

Key idea: The group H' we seek consists of the elements in these p cosets ("shoeboxes").

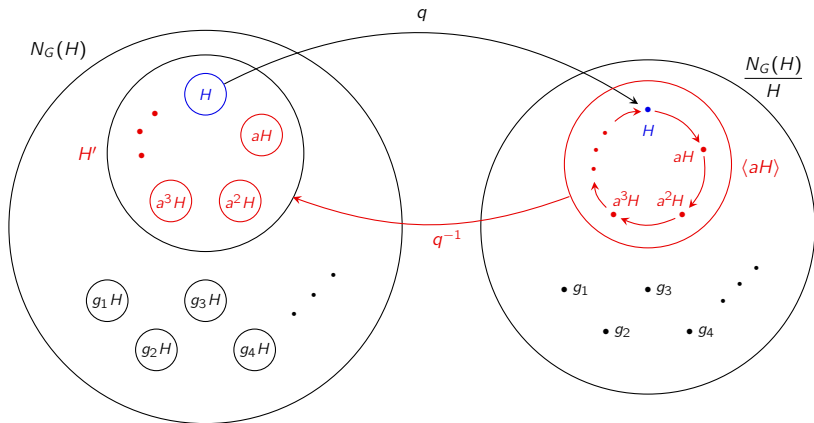
Formally, this is the **preimage** of $\langle aH \rangle$ under the quotient $q: N_G(H) \rightarrow N_G(H)/H$.

Specifically, $q^{-1}(H)$, $q^{-1}(aH)$, $q^{-1}(a^2H)$, \dots , $q^{-1}(a^{p-1}H)$ are distinct cosets of H in $N_G(H)$, each of size p^j .

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

The 1st Sylow theorem: existence of p -subgroups

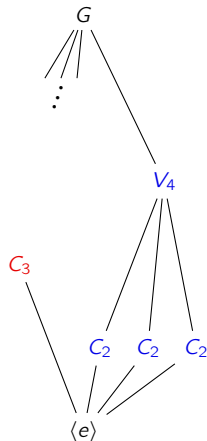
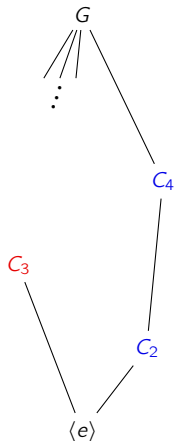
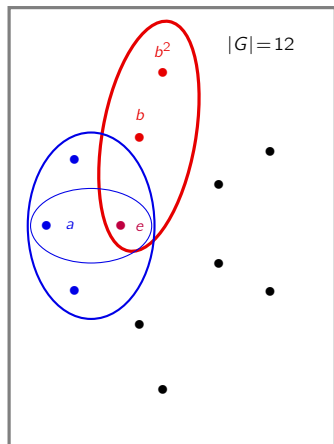
Here is a picture of how we found the group $H' = q^{-1}(\langle aH \rangle)$.



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

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 2nd Sylow theorem: relationship among p -subgroups

Second Sylow theorem

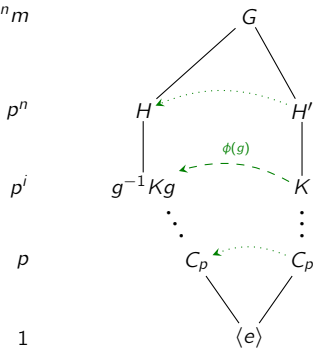
Any two Sylow p -subgroups are conjugate (and hence isomorphic).

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 $K \leq G$ any p -subgroup. Then K is conjugate to a subgroup of H .

Order: $p^n m$



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

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

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

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

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

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

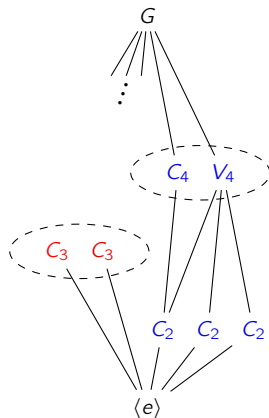
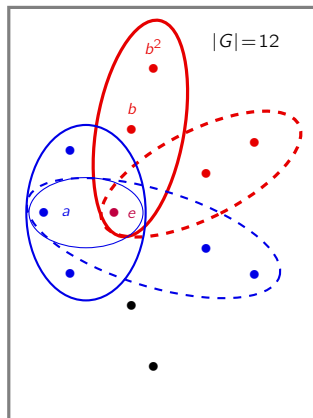
All we need to do is show that $|\text{Fix}(\phi)| \not\equiv_p 0$. By the p -group Lemma,

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

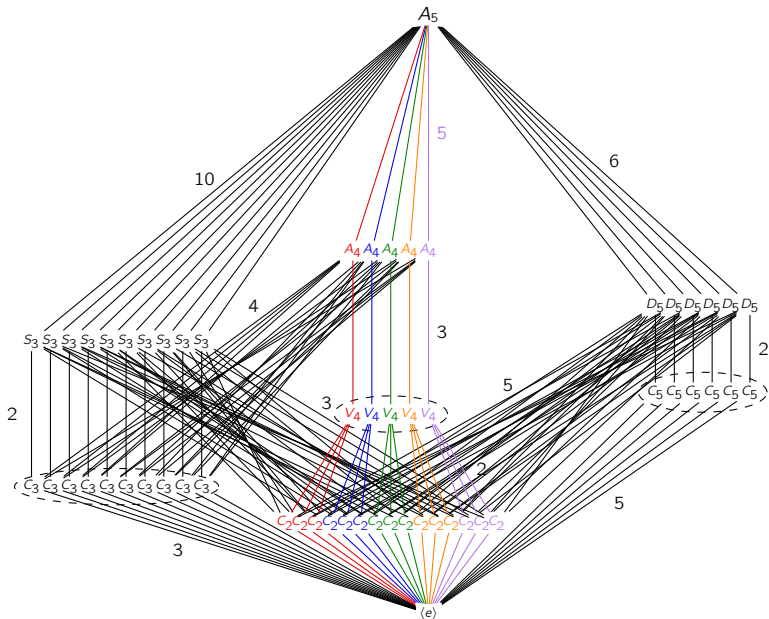
Our unknown group of order 12

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.



Application: 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

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

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

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

(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 $\phi: G \rightarrow \text{Perm}(S)$, 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,

$$\underbrace{|\text{orb}(H)|}_{=n_p} \cdot |\text{stab}(H)| = |G| \quad \implies \quad n_p \text{ divides } |G|.$$

The 3rd Sylow theorem: number of p -subgroups

Proof (cont.)

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

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

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

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

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.)
- $K \trianglelefteq N_G(K)$, thus the only conjugate of K in $N_G(K)$ is itself.

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

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

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, \dots, p^n .

For the 2nd and 3rd 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 $|\text{orb}(s)| \cdot |\text{stab}(s)| = |G|$.
- (ii) *p -group lemma*. If a p -group acts on S , then $|S| \equiv_p |\text{Fix}(\phi)|$.

To summarize, we used:

- S2 The action of $K \in \text{Syl}_p(G)$ on $S = G/H$ by **right multiplication** for some other $H \in \text{Syl}_p(G)$.
- S3a The action of G on $S = \text{Syl}_p(G)$, by **conjugation**.
- S3b The action of $H \in \text{Syl}_p(G)$ on $S = \text{Syl}_p(G)$, by **conjugation**.

Our mystery group order 12

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

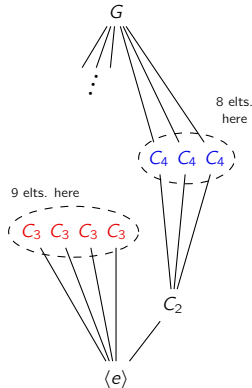
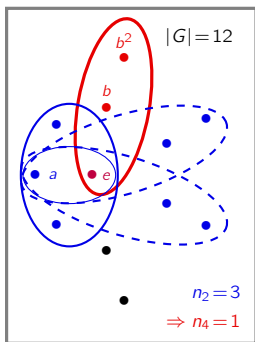
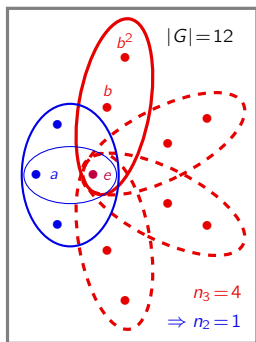
- n_3 Sylow 3-subgroups, each of order 3.

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

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

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

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

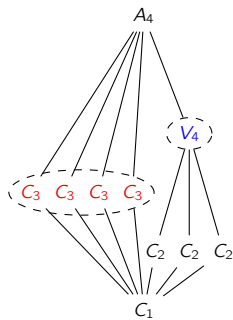
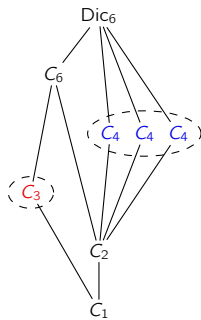
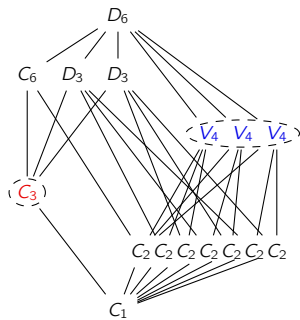
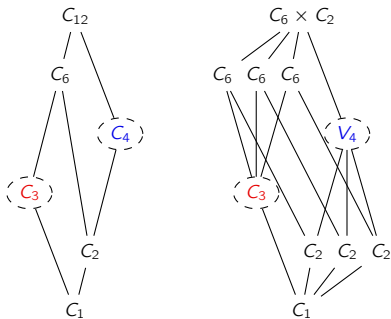


The five groups of order 12

With a little 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 $n_3 \in \{1, 2, 4, 7, 14, 28\}$.
- 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 possibilities 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. \square

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., $S = G/H$) by **right-multiplication**:

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

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

$$\langle e \rangle \leq \text{Ker } \phi = \bigcap_{x \in G} x^{-1} H x \triangleleft G$$

If $\text{Ker } \phi = \langle e \rangle$ then $\phi: G \hookrightarrow S_n$ is an **embedding**, which is impossible because $|G| \nmid n!$. \square

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 $\sigma \in A_n$, and consider its conjugacy class in S_n . By the orbit-stabilizer theorem,

$$|\text{cl}_{S_n}(\sigma)| = [S_n : C_{S_n}(\sigma)] = \frac{n!}{|C_{S_n}(\sigma)|}.$$

There are two cases: (1) $C_{S_n} \leq A_n$, or (2) $C_{S_n} \not\leq A_n$.

Case 1. $C_{A_n}(\sigma) = C_{S_n}(\sigma)$, and by the orbit-stabilizer theorem,

$$|\text{cl}_{A_n}(\sigma)| = [A_n : C_{A_n}(\sigma)] = \frac{n!/2}{|C_{A_n}(\sigma)|} = \frac{n!}{2|C_{S_n}(\sigma)|} = \frac{1}{2} |\text{cl}_{S_n}(\sigma)|.$$

Conclusion: the conjugacy class splits into two.

Case 2. By the diamond theorem, exactly half of the permutations in $C_{S_n}(\sigma)$ are even, so

$$|\text{cl}_{A_n}(\sigma)| = [A_n : C_{A_n}(\sigma)] = [A_n : C_{S_n}(\sigma) \cap A_n] = \frac{n!/2}{|C_{S_n}(\sigma)|/2} = |\text{cl}_{S_n}(\sigma)|.$$

Conclusion: the conjugacy class is preserved upon restricting to A_n .

Simplicity of A_5

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

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

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

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

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

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

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 others of sizes 12, 12, 15, and 20.

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

A generating set for A_n

Lemma

For $n \geq 3$, the alternating group A_n is generated by 3-cycles.

Proof

By definition, A_n is generated by all products of pairs of transpositions.

- **Type 1.** Disjoint transpositions:

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

- **Type 2.** Overlapping transpositions:

$$(ab)(bc) = (acb).$$

We know that $A_3 = \langle (123) \rangle$ and $A_4 = \langle (123), (234) \rangle$, so let $n \geq 5$.

Claim. All 3-cycles are conjugate to (123) in A_n .

Take any 3-cycle (abc) , and write

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

If $\sigma \in A_n$, we're done. Otherwise, conjugating by $\sigma \cdot (45) \in A_n$ gives the same result. \square

Simplicity of A_n

Theorem

The alternating group A_5 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:

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

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

Simplicity of A_n

Theorem

The alternating group A_5 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 .

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

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

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

✓

and this completes the proof. □

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**: $\text{PSL}(n, q)$, $\text{PSU}(n, q)$, $\text{PsP}(2n, p)$, 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 ≈ 500 journal articles by over 100 authors, published between 1955 and 2004.

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

★★★★☆ 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