

## Chapter 5: Actions of groups

Matthew Macauley

Department of Mathematical Sciences  
Clemson University

<http://www.math.clemson.edu/~macaule/>

Math 8510, Abstract Algebra

## Action graphs

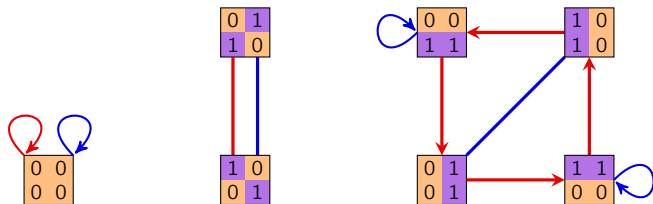
Technically, we started this class with [group actions](#), and a bijective correspondence between “actions” (group elements) and “configurations” (set elements).

*This need not always happen!*

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

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

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



Every group action on a finite set defines an [action graph](#), which generalizes Cayley graphs.

## The “group switchboard” analogy

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

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

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

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

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

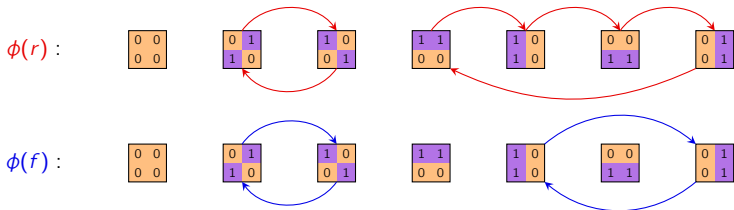
Let  $\text{Perm}(S)$  be the group of permutations of  $S$ .

### Definition

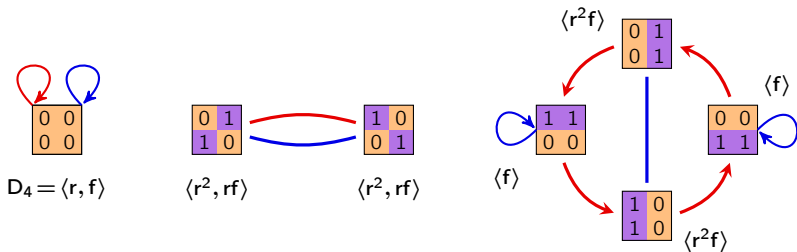
A group  $G$  **acts on** a set  $S$  if there is a homomorphism  $\phi: G \rightarrow \text{Perm}(S)$ .

# The “group switchboard” analogy

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

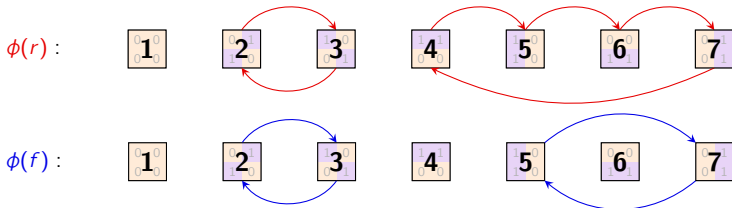


Observe how these permutations are encoded in the action graph. (Below each  $s \in S$  is the subgroup that fixes it.)

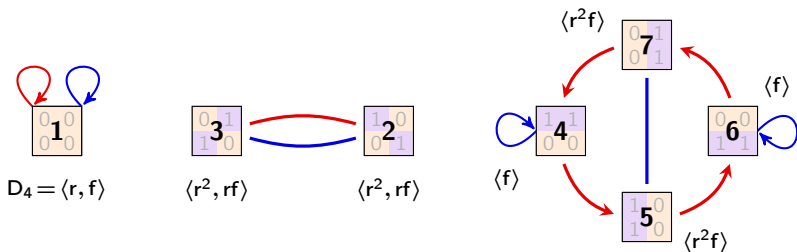


## The “group switchboard” analogy

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



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



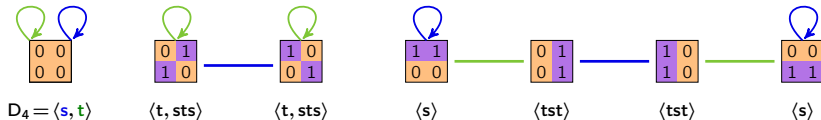
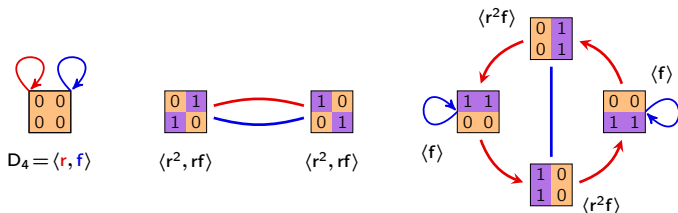
# Action graphs vs. $G$ -sets

## Definition

A set  $S$  with an action by  $G$  is called a  $G$ -set.

## Big ideas

- An action  $\phi: G \rightarrow \text{Perm}(S)$  endows  $S$  with an **algebraic structure**.
- *Action graphs are to  $G$ -sets, like how Cayley graphs are to groups.*



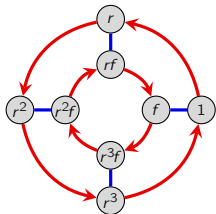
## $G$ -sets generalize groups. Action graphs generalize Cayley graphs

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

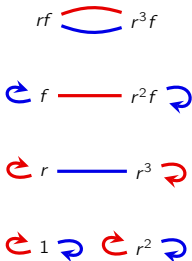
$$S = \{D_4, \langle r \rangle, \langle r^2, f \rangle, \langle r^2, rf \rangle, \langle f \rangle, \langle rf \rangle, \langle r^2 f \rangle, \langle r^3 f \rangle, \langle r^2 \rangle, \langle 1 \rangle\}.$$

There are several ways to define the result of “pressing the  $g$ -button on our switchboard”.

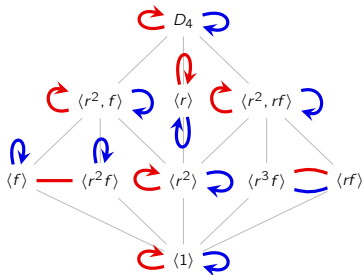
We say that: “ $G$  acts on...”



“... itself by multiplication”



“... itself by conjugation”



“... its subgroups by conjugation”

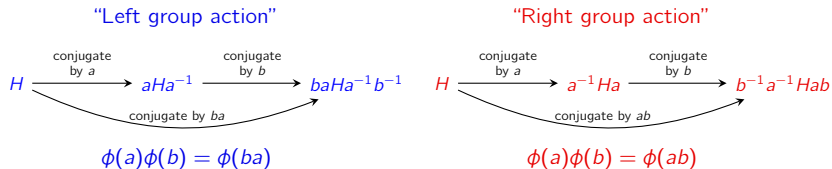
### Remark

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

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

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

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



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

Some books forgo our " $\phi$ -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  $\phi$ , 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** is defined similarly. Theorems for left actions have analogues for right actions.

Each left action has a related right action, and vice-versa. **We'll 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  $\phi(g).s$ .

If needed, we can distinguish **left  $G$ -sets** with **right  $G$ -sets**.

## Five features of every group action

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

There are several ways to classify them. For example:

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

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

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

We will see parallels within and between these classes.

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

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

We'll start by exploring the three local features.

### Notation

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

## Two local features: orbits and stabilizers

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

- (i) What other **states** (in  $S$ ) are reachable from  $s$ ? (We call this the **orbit** of  $s$ .)
- (ii) What **group elements** (in  $G$ ) fix  $s$ ? (We call this the **stabilizer** of  $s$ .)

### Definition

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

- (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 graph

- (i) The **orbit** of  $s \in S$  is the **connected component** containing  $s$ .
- (ii) The **stabilizer** of  $s \in S$  are the group elements whose paths start and end at  $s$ ; “**loops**.”

## The third local feature: fixators

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

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

### Definition

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

(iii) The **fixator** 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 graph

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

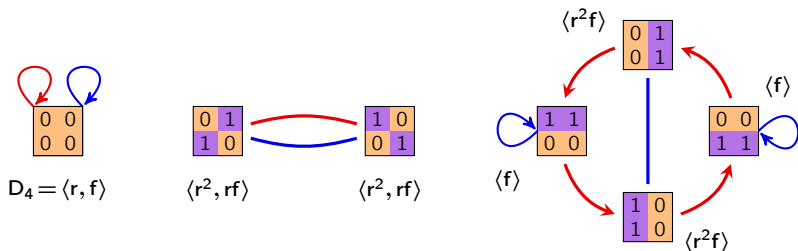
### In terms of the “group switchboard analogy”

- (i) The **orbit** of  $s \in S$  are the elements in  $S$  that can be reached by pressing buttons.
- (ii) The **stabilizer** of  $s \in S$  consists of the buttons that have no effect on  $s$ .
- (iii) The **fixator** of  $g \in G$  are the elements in  $S$  that don't move when we press the  $g$ -button.

## Three local features: orbits, stabilizers, and fixators

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

Each node is labeled by its **stabilizer**.



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

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

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

## Local duality: stabilizers vs. fixators

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

	$\begin{array}{ c c } \hline 0 & 0 \\ \hline 0 & 0 \\ \hline \end{array}$	$\begin{array}{ c c } \hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array}$	$\begin{array}{ c c } \hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array}$	$\begin{array}{ c c } \hline 0 & 0 \\ \hline 1 & 1 \\ \hline \end{array}$	$\begin{array}{ c c } \hline 0 & 1 \\ \hline 0 & 1 \\ \hline \end{array}$	$\begin{array}{ c c } \hline 1 & 1 \\ \hline 0 & 0 \\ \hline \end{array}$	$\begin{array}{ c c } \hline 1 & 0 \\ \hline 1 & 0 \\ \hline \end{array}$
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 **fixators** can be read off the **rows**: *set elements fixed by  $g \in G$ .*

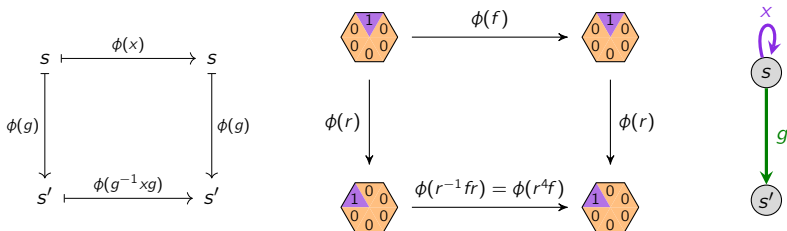
# The stabilizer subgroup

## Proposition (HW exercise)

For any  $s \in S$ , the set  $\text{stab}(s)$  is a **subgroup** of  $G$ . 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  $s \cdot \phi(g)$ .

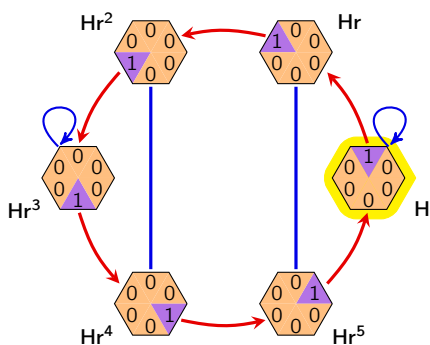


In other words, if  $x$  is a loop from  $s$ , and  $s \xrightarrow{g} s'$ , then  $g^{-1}xg$  is a loop from  $s'$ .

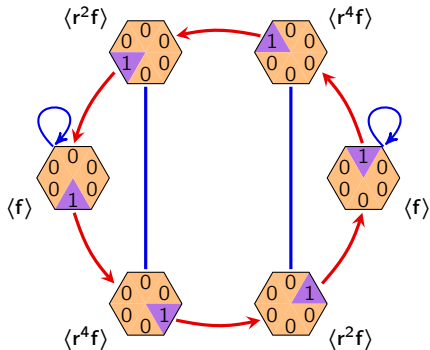
## The stabilizer subgroup

Here is another example of an action (or  $G$ -set), this time of  $G = D_6$ .

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



*labeled by destinations*



*labeled by stabilizers*



## Two global features: fixed points and the kernel

Our last two features are properties of the action  $\phi$ , 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** is the set

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

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

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

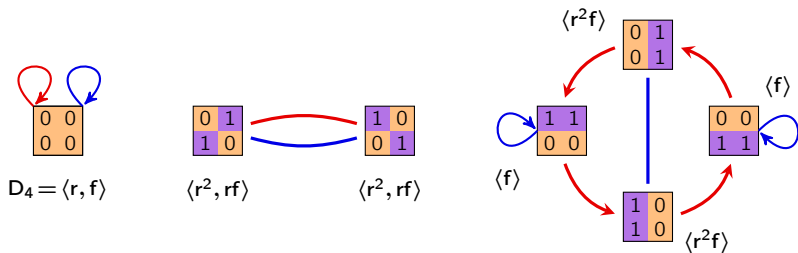
### Proposition (global duality: fixed points vs. kernel)

Suppose that  $G$  acts on a set  $S$  via  $\phi: G \rightarrow \text{Perm}(S)$ . 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 **Orb**( $\phi$ ) for the **set of orbits** of  $\phi$ .

## Two global features: fixed points and the kernel



### In terms of the action graph

- (iv) The **kernel of  $\phi$**  are the paths that are “loops from every  $s \in S$ .”
- (v) The **fixed points of  $\phi$**  are the **size-1 connected components**.

### In terms of the group switchboard analogy

- (iv) The **kernel of  $\phi$**  are the “**broken buttons**”; those  $g \in G$  that have no effect on any  $s$ .
- (v) The **fixed points of  $\phi$**  are those  $s \in S$  that are **not moved by pressing any button**.

## Global duality: fixed points vs. kernel

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

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

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

## Two theorems on orbits, and their consequences

Our binary square example gives us key 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 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  $s \in S$ ,

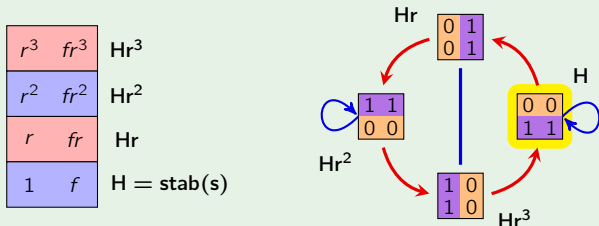
$$|\text{orb}(s)| \cdot |\text{stab}(s)| = |G|.$$

Equivalently, *the size of the orbit containing  $s$  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”.



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:

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

“ $\Leftarrow$ ” *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  $s.\phi(g) = s.\phi(k)$ . □

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:

	<table border="1"><tr><td>0</td><td>0</td></tr><tr><td>0</td><td>0</td></tr></table>	0	0	0	0	<table border="1"><tr><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td></tr></table>	0	1	1	0	<table border="1"><tr><td>1</td><td>0</td></tr><tr><td>0</td><td>1</td></tr></table>	1	0	0	1	<table border="1"><tr><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td></tr></table>	0	0	1	1	<table border="1"><tr><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td></tr></table>	0	1	0	1	<table border="1"><tr><td>1</td><td>1</td></tr><tr><td>0</td><td>0</td></tr></table>	1	1	0	0	<table border="1"><tr><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td></tr></table>	1	0	1	0
0	0																																		
0	0																																		
0	1																																		
1	0																																		
1	0																																		
0	1																																		
0	0																																		
1	1																																		
0	1																																		
0	1																																		
1	1																																		
0	0																																		
1	0																																		
1	0																																		
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 multiplication.
- $G$  acts on itself by conjugation.
- $G$  acts on its subgroups by conjugation.
- $G$  acts on the cosets of a fixed subgroup  $H \leq G$  by multiplication.

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

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

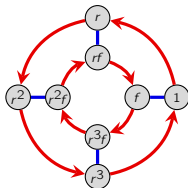
## Groups acting on themselves by multiplication

Assume  $|G| > 2$ . 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  $\text{stab}(x) = \langle 1 \rangle$
- the **fixator** of  $g \neq 1$  is  $\text{fix}(g) = \emptyset$ .
- there are no **fixed points**, and the **kernel** is trivial:

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



### Cayley's theorem

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

### Proof

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

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

Since  $\text{Ker}(\phi) = \langle 1 \rangle$ , 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 **right-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**:

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

- The **stabilizer** of  $x$  is its **centralizer**:

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

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

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

- The **fixed points** and **kernel** are the center, because

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

## Groups acting on themselves by conjugation

Let's apply our two theorems:

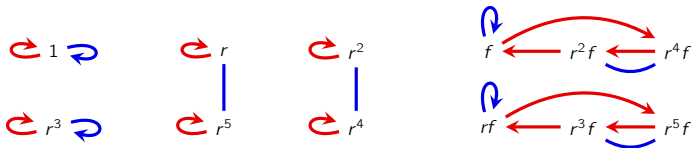
1. **Orbit-stabilizer theorem.** "the *size of an orbit* is the *index of the stabilizer*":

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

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 themselves by conjugation

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

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

Do you see how to enumerate 6 conjugacy classes from the orbit-counting theorem?

## Groups acting on subgroups by conjugation

Any group  $G$  acts on its set  $S$  of subgroups by **right-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 **fixator** of  $g$  are the **subgroups that  $g$  normalizes**:

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

- The **fixed points** of  $\phi$  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:

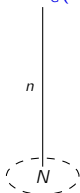
1. **Orbit-stabilizer theorem.** "the *size of an orbit* is the *index of the stabilizer*":

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

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

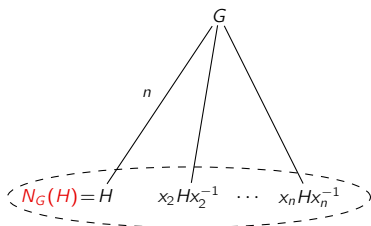
#conjugacy classes of subgroups of  $G$  = average size of a normalizer.

$$G = N_G(N)$$



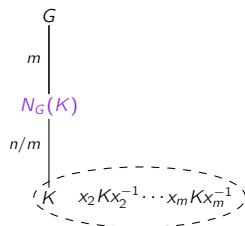
*normal*

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



*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.

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

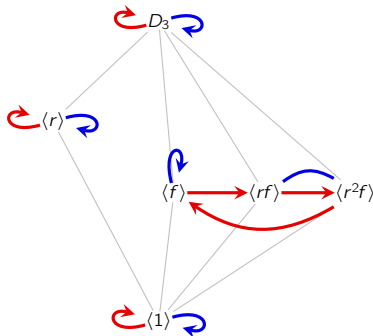
$$\tau(r) = \langle 1 \rangle \quad \langle r \rangle \quad \langle f \rangle \xrightarrow{\text{red}} \langle rf \rangle \xrightarrow{\text{red}} \langle r^2f \rangle \quad D_3$$

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

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

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

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



### 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

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

$r^2$	$r^2f$	$r^2$	$r^2f$	$r^2$	$f$	$r^2$	$rf$	$r^2$	$rf$		
$r$	$rf$	$r$	$rf$	$r$	$r^2f$	$r$	$f$	$r$	$rf$		
$1$	$f$	$1$	$f$	$1$	$f$	$1$	$r^2f$	$1$	$f$		
$D_3/D_3$		$D_3/\langle r \rangle$		$D_3/\langle f \rangle$		$D_3/\langle rf \rangle$		$D_3/\langle r^2f \rangle$		$D_3/\langle 1 \rangle$	

- $\text{fix}(g)$  are the subgroups  $H$  for which “ $g$  appears in a blue coset of  $H$ ”
- $\text{Ker}(\phi)$  are elements that “only appear in blue cosets”
- By the orbit-counting theorem, the subgroups fall into

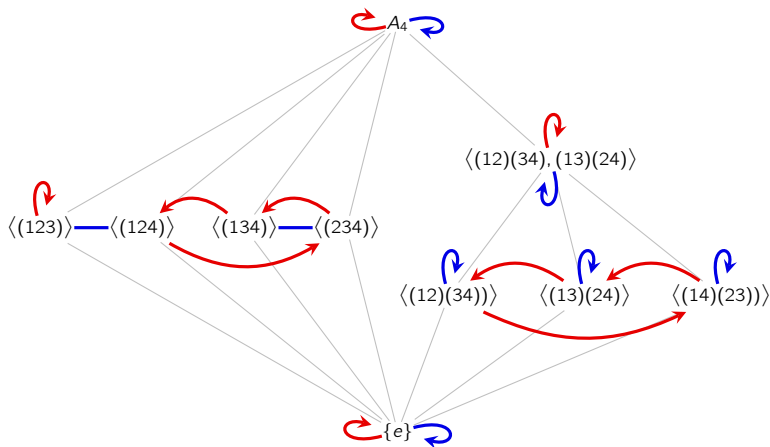
$$|\text{Orb}(\phi)| = \text{average \# check marks per row} = \frac{\text{total \# of blue entries}}{|G|}$$

conjugacy classes.

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

## Groups acting on subgroups by conjugation

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



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

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

## 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 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  $S = H \backslash G$  (the right cosets of  $H$ ).

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

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

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

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

- There doesn't seem to be a standard term for the **fixator** 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  $\phi$ .

- The **kernel** of this action is the intersection of all conjugate subgroups of  $H$ :

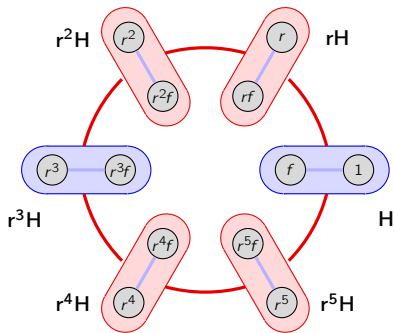
$$\text{Ker}(\phi) = \bigcap_{x \in G} \text{stab}(x) = \bigcap_{x \in G} x^{-1}Hx.$$

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

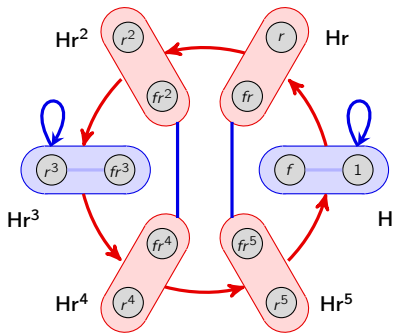
## Groups acting on cosets of $H$ by multiplication

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

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



*not a valid action graph*



*action graph of  $\phi$*

## 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,

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

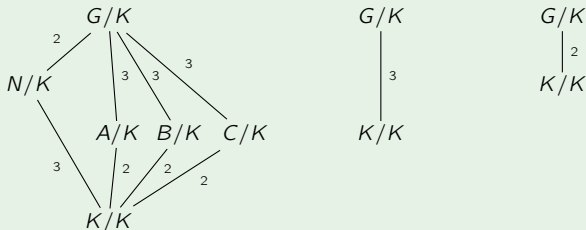
## Subgroups of small index

### 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  $K \leq H \leq G$ .

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

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

Do you see why  $q = 1$ ?

□

## A summary of our four actions

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

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

## Actions of automorphism groups

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

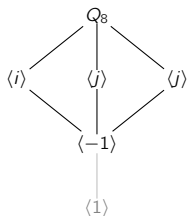
For any  $G$ , the automorphism group  $\text{Aut}(G)$  naturally acts on  $S = G$  via a homomorphism

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

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  $\text{Inn}(Q_8) = \{\text{Id}, \varphi_i, \varphi_j, \varphi_k\}$ .



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

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

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

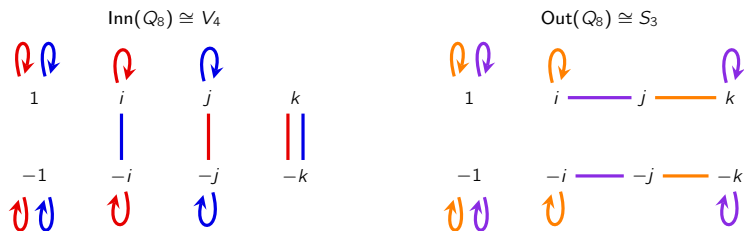
$\text{cl}(1)$	$1$	$i$	$j$	$k$
$\text{cl}(-1)$	$-1$	$-i$	$-j$	$-k$
		$\text{cl}(i)$	$\text{cl}(j)$	$\text{cl}(k)$

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 $Q_8$

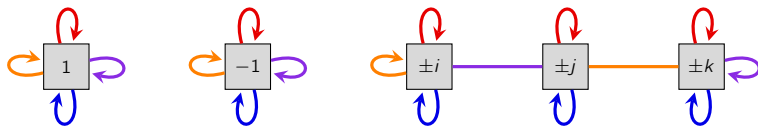
All three groups  $\text{Aut}(Q_8)$ ,  $\text{Inn}(Q_8)$ , and  $\text{Out}(Q_8) \cong \text{Aut}(Q_8)/\text{Inn}(Q_8)$  act on  $S = Q_8$ .



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

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

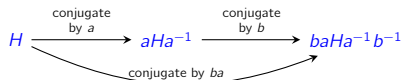
The group  $\text{Aut}(Q_8)$  also acts on the conjugacy classes:



## Action equivalence

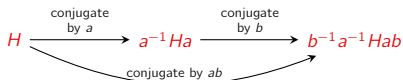
Let's recall the difference between left-conjugating and right conjugating:

“Left group action”



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

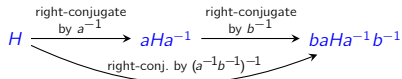
“Right group action”



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

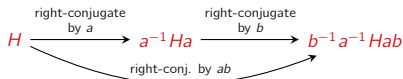
There's a better way to describe left actions than the faux-homomorphic  $\phi(a)\phi(b) = \phi(ba)$ .

“Left group action”



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

“Right group action”



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

### Big idea

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

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

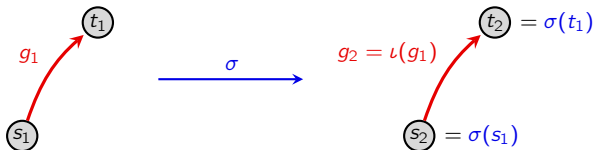
## Action equivalence, informally

Consider two actions:

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

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 graph

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 graph, 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

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

The resulting action graphs are **action equivalent**.

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

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

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

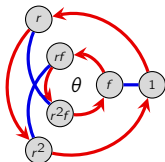
- defined  $\phi(r)$  to rotate clockwise, and  $\phi(f)$  to flip vertically
- used tiles with  $a$  and  $b$ , rather than 0 and 1
- read from right-to-left, rather than left-to-right, etc.

# 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	$H \mapsto Hg$	$H \mapsto g^{-1}H$

$$\begin{array}{ccc}
 x & \xrightarrow{\phi_R(g)} & xg \\
 \sigma \downarrow & & \downarrow \sigma \\
 x^{-1} & \xrightarrow{\phi_L(g)} & g^{-1}x^{-1}
 \end{array}$$

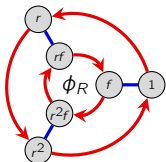
—  $x \mapsto rx$   
—  $x \mapsto fx$



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

$$\begin{array}{ccc}
 x & \xrightarrow{\phi_R(g)} & xg \\
 \sigma \downarrow & & \downarrow \text{not } \sigma \\
 x^{-1} & \xrightarrow{\theta(g)} & gx^{-1}
 \end{array}$$

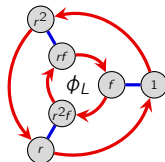
—  $x \mapsto xr$   
—  $x \mapsto xf$



$\xrightarrow{\sigma}$   
 action equivalence

$$\begin{array}{ccc}
 x & \xrightarrow{\phi_R(g)} & xg \\
 \text{Id} \downarrow & & \downarrow \text{not Id} \\
 x & \xrightarrow{\theta(g)} & gx
 \end{array}$$

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

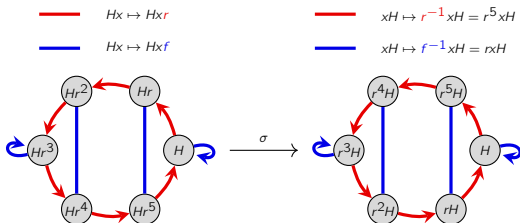
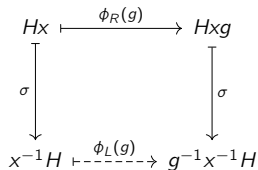




# Every right action has an equivalent left action

$G$ acting on...	right action	equivalent left action
itself by multiplication	$x \mapsto xg$	$x \mapsto g^{-1}x$
itself by conjugation	$x \mapsto g^{-1}xg$	$x \mapsto gxg^{-1}$
<b>its subgroups by conjugation</b>	$H \mapsto g^{-1}Hg$	$H \mapsto gHg^{-1}$
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 map  $xH \mapsto Hx$  is not even well-defined.

## Left and right actions of permutations

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

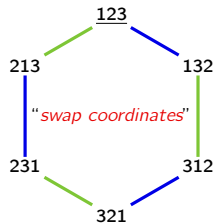
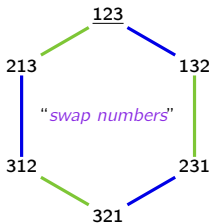
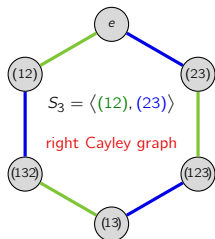
$$S = \{123, 132, 213, 231, 312, 321\}.$$

In one,  $(ij)$  can be interpreted to mean

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

Alternatively,  $(ij)$  could mean

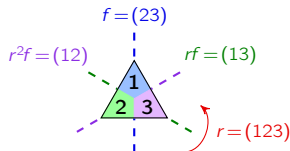
“swap the *numbers*  $i$  and  $j$ , regardless of where they are.”



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

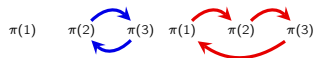
$$\phi_R: S_3 \longrightarrow \text{Perm}(S), \quad \phi_R(\tau): \pi(1)\pi(2)\pi(3) \longmapsto \pi(\tau(1))\pi(\tau(2))\pi(\tau(3)).$$

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

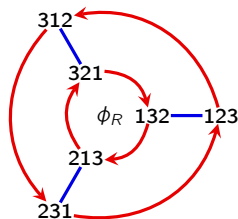
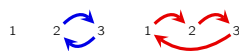
$$\phi_L: S_3 \longrightarrow \text{Perm}(S), \quad \phi_L(\tau): \pi(1)\pi(2)\pi(3) \longmapsto \tau^{-1}(\pi(1))\tau^{-1}(\pi(2))\tau^{-1}(\pi(3)).$$

# Left and right actions of permutations

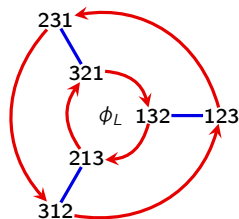
right action "permutes positions"



left action "permutes numbers"



$\xrightarrow{\sigma}$



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

$\downarrow \sigma$

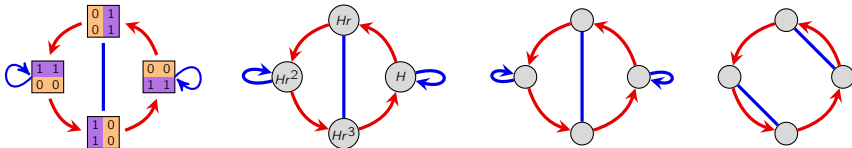
$\downarrow \sigma$

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

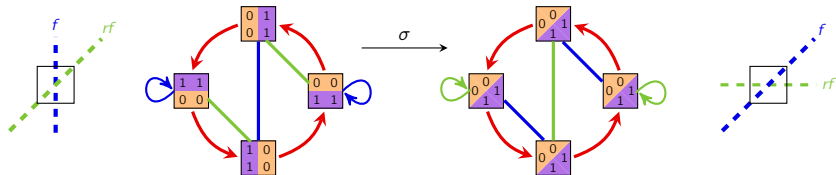
# Isomorphisms of $G$ -sets

Just like we did for groups, we can formalize what it means for  $G$ -sets to be **isomorphic**.

Which of the following should represent isomorphic  $D_4$ -sets?



Should the following  $D_4$ -sets be isomorphic?



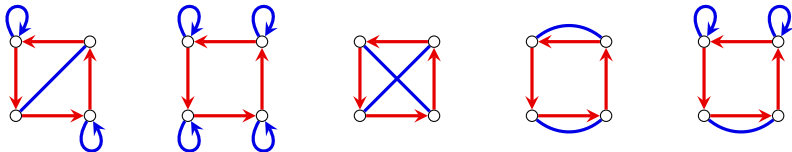
Let's start by first classifying action diagrams for a fixed generating set.

# Classification of $G$ -sets

## Natural question

Given a group  $G$ , what are the possible (connected)  $G$ -sets?

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



## Definition

An action  $\phi: G \rightarrow \text{Perm}(S)$  is

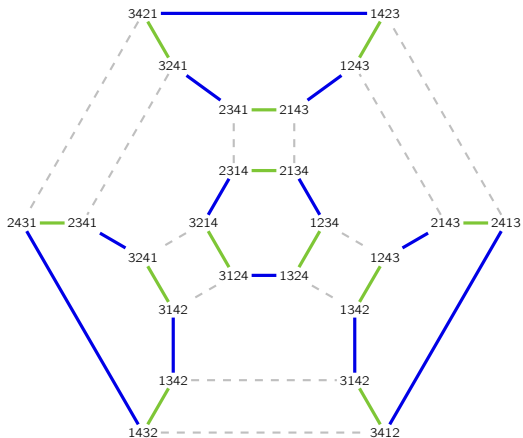
- **transitive** if it has only one orbit: ("*graph is connected*")
- **free** if  $\text{stab}(s) = \langle e \rangle$  for all  $s \in S$ . ("*uncollapsed – no nontrivial loops*")
- **faithful** if  $\text{Ker}(\phi) = \langle e \rangle$ .

In this language our question becomes: "*classify all transitive  $G$ -actions*" (or  $G$ -sets).

## An example of a free action that is not transitive

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

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

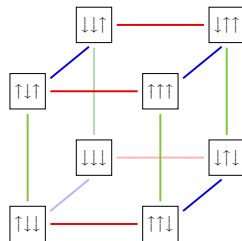
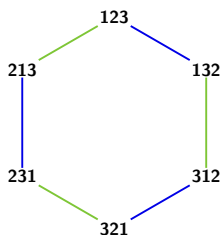
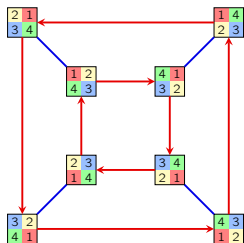


# Simply transitive actions

## Definition

An action  $\phi: G \rightarrow \text{Perm}(S)$  is **simply transitive** if it is transitive and free.

Here are some simply transitive actions that we have seen. What do you notice?



## Proposition

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

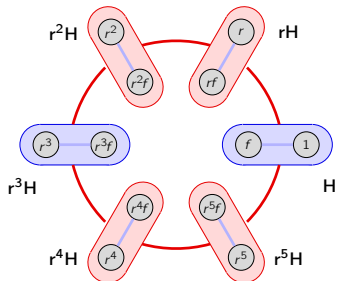
This just says that *simply transitive  $G$ -sets are groups!*



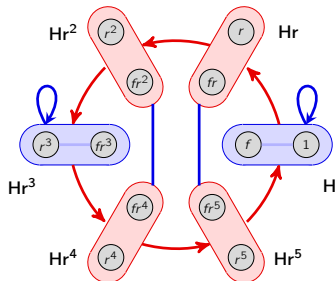
## Transitive actions

All transitive actions can be constructed by collapsing Cayley graphs.

But what to collapse? Recall the bijection between **nodes in  $\text{orb}(s)$**  and **cosets of  $\text{stab}(s)$** .



*collapse left cosets of  $H$  (not an action)*



*collapse right cosets of  $H$  (an action)*

### Proposition

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

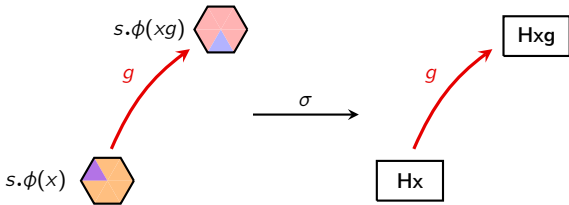
# Transitive actions

## Proposition

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

**Proof sketch.** Let  $\iota: G \rightarrow G$  be the identity, fix  $s \in S$ , let  $H = \text{stab}(s)$ , and define

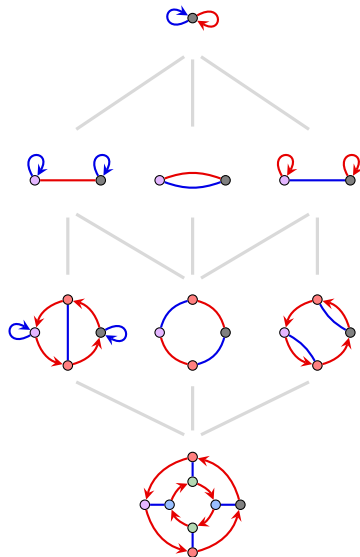
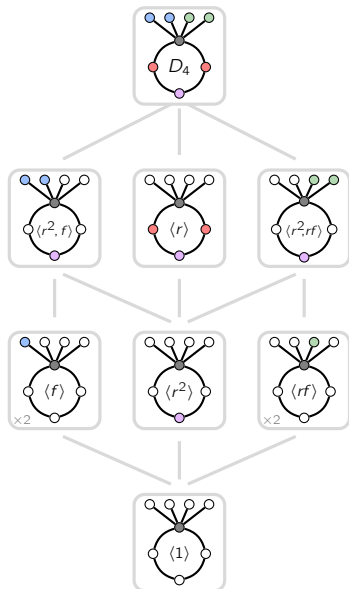
$$\sigma: S \rightarrow H \backslash G, \quad \sigma: s \cdot \phi(x) \mapsto Hx$$



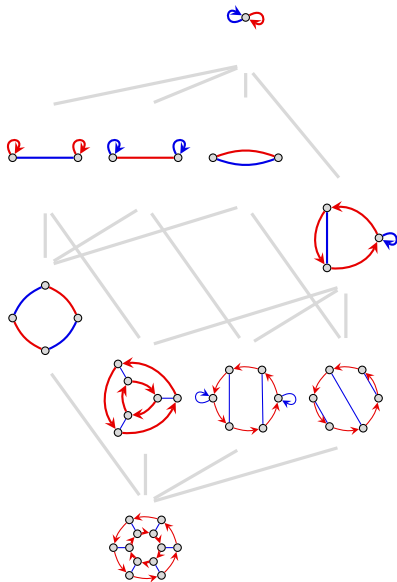
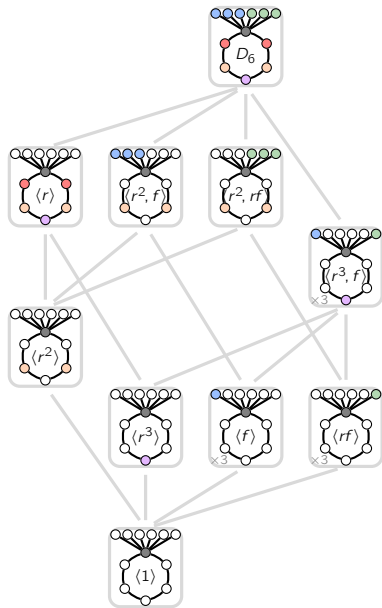
Show that  $\sigma$  is a well-defined bijection, and then the proof follows because:

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

# The transitive $D_4$ -sets: collapsing by right cosets



# The transitive $D_6$ -sets: collapsing by right cosets

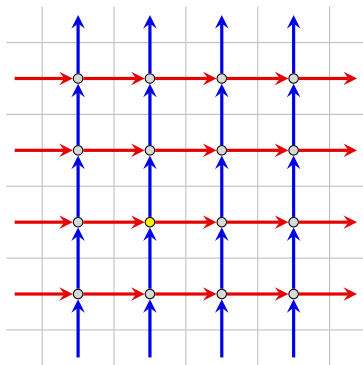


## Simply transitive actions from finite reflection groups

One place where simply transitive actions arise is from [tilings](#).

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

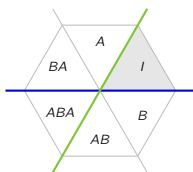
$A^{-1}B^2$	$B^2$	$AB^2$	$A^2B^2$
$A^{-1}B$	$B$	$AB$	$A^2B$
$A^{-1}$	$I$	$A$	$A^2$
$A^{-1}B^{-1}$	$B^{-1}$	$AB^{-1}$	$A^2B^{-1}$



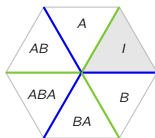
The shaded region is called a **fundamental chamber**.

## Simply transitive actions from finite reflection groups

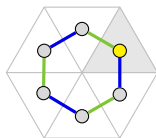
The dihedral group  $D_3 = \langle A, B \mid A^2 = B^2 = (AB)^3 = 1 \rangle$  acts simply transitively on the six regions of a hexagon.



*"left action"*

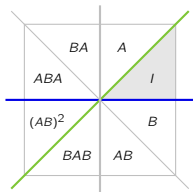


*"right action"*

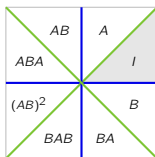


*"(right) Cayley graph"*

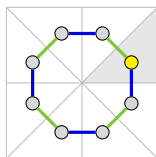
The dihedral group  $D_4$  acts simply transitively on the eight regions of a square.



*"left action"*



*"right action"*

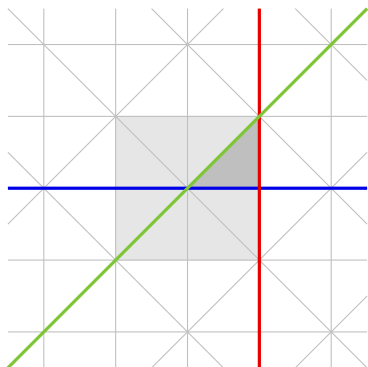
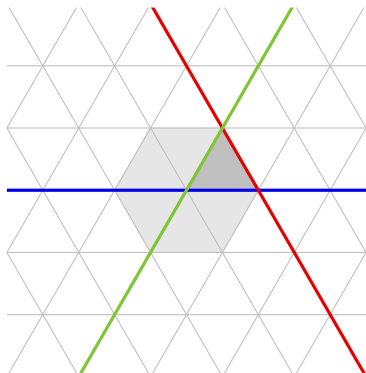


*"(right) Cayley graph"*

## Simply transitive actions from finite reflection groups

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

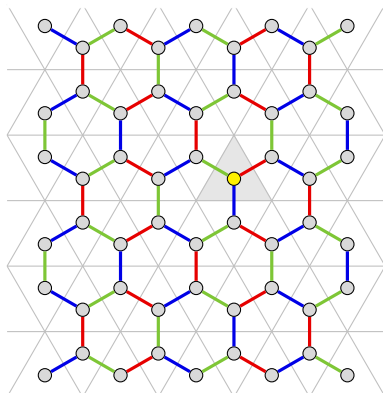
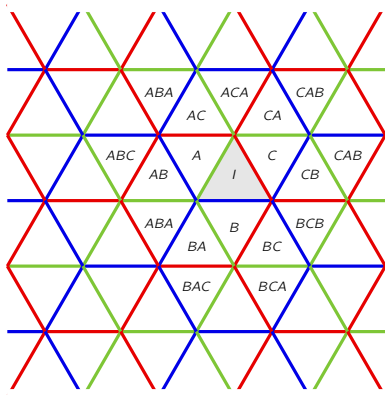
The resulting **affine** groups,  $\text{Aff}(D_3)$  and  $\text{Aff}(D_4)$ , act simply transitively on the chambers.



## Simply transitive actions and affine Weyl groups

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

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



It has presentation

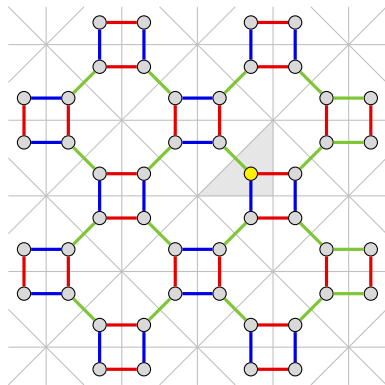
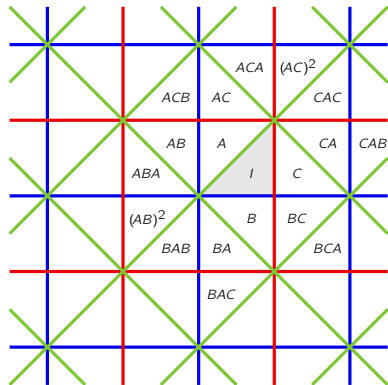
$$W(\tilde{A}_2) = \text{Aff}(D_3) = \langle A, B, C \mid A^2 = B^2 = C^2 = (AB)^3 = (AC)^3 = (BC)^3 = 1 \rangle.$$



## Simply transitive actions and affine Weyl groups

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

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



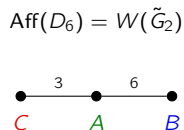
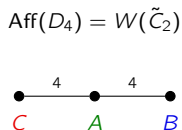
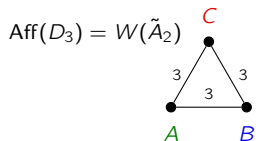
It has presentation

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

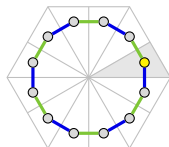
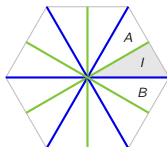
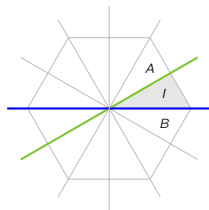
## Weyl groups and Dynkin diagrams

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

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



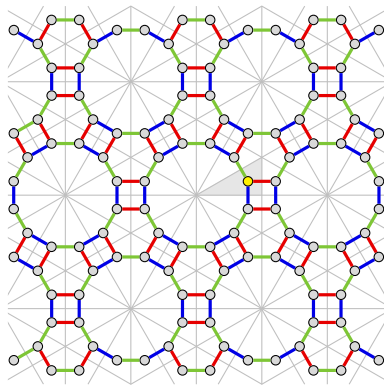
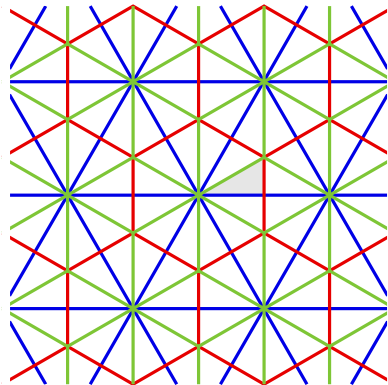
This last example is the affine version of  $D_6 = \langle A, B \mid A^2 = B^2 = (AB)^6 = 1 \rangle$  acting simply transitively on the 12 regions of a hexagon.



## One last affine Weyl group

The group  $\text{Aff}(D_6)$  is better known as the the **affine Weyl group of type  $G_2$** .

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



It has presentation

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

## Coxeter groups and tilings of hyperbolic space

A **Coxeter group** is a group generated by “reflections”, with presentation

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

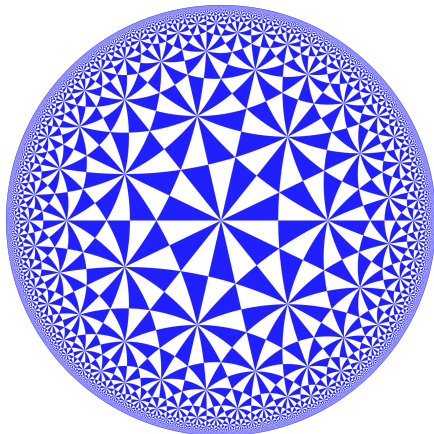
Like Weyl groups, this can be encoded by a **Coxeter graph**.

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

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



*A hyperbolic Coxeter group*



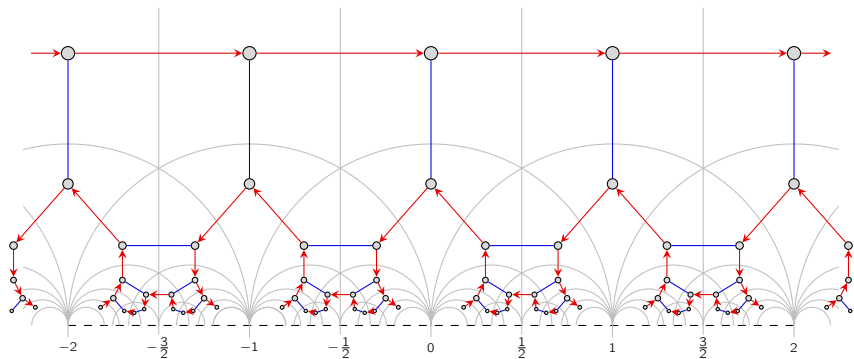
## A simply transitive action of $\mathrm{PSL}_2(\mathbb{Z})$

The projective special linear group

$$\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) / \langle -I \rangle, \quad \text{where } \mathrm{SL}_2(\mathbb{Z}) = \left\langle \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_S, \underbrace{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}}_T \right\rangle$$

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

$$S: z \mapsto \frac{0z - 1}{z + 0} = -\frac{1}{z}, \quad \text{and} \quad T: z \mapsto \frac{z + 1}{0z + 1} = z + 1.$$



# Equivariance and morphisms of $G$ -sets

## Key idea

- **Action equivalence** involves an isomorphism  $\iota: G_1 \rightarrow G_2$  and bijection  $\sigma: S_1 \rightarrow S_2$ .
- **Equivariant bijections** ( $\iota = \text{Id}$ ) define  **$G$ -set isomorphisms**.
- **Equivariant maps** ( $\iota = \text{Id}$ , but  $\sigma$  need not be bijective) define  **$G$ -set homomorphisms**.

## Definition

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

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

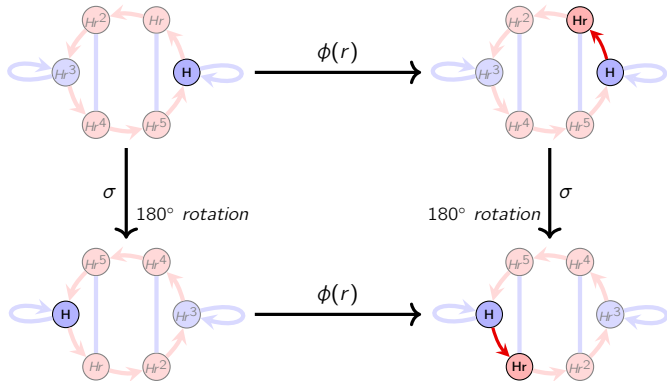
$$\begin{array}{ccc} S_1 & \xrightarrow{\phi_1(g)} & s_1 \cdot \phi_1(g) \\ \sigma \downarrow & & \downarrow \sigma \\ S_2 & \xrightarrow{\phi_2(g)} & s_2 \cdot \phi_2(g) \end{array}$$

Special cases:

- Equivariant bijection ( **$G$ -set isomorphism**): when  $\sigma$  is bijective.
- If  $S := S_1 = S_2$ , then we get the group  $\text{Aut}_G(S)$  of  **$G$ -set automorphisms**.

## $G$ -set automorphisms as symmetries of the action graph

Let  $S = G \setminus H$ , for  $G = D_6$  and  $H = \langle f \rangle$ .

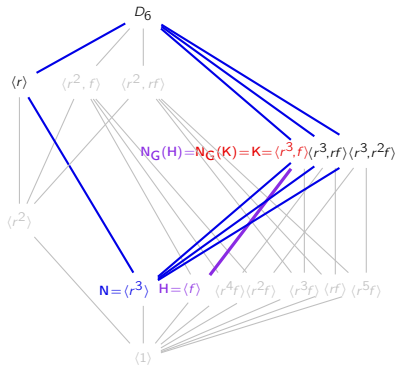
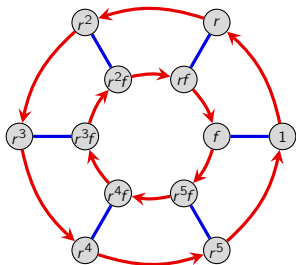


### Key idea

The action and bijection clearly commute upon thinking of:

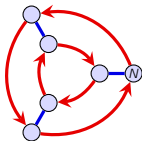
- the **action**  $\phi(r)$  as **right-multiplying**  $Hr^i$  by  $r$ ,
- the **bijection**  $\sigma$  as **left-multiplying**  $Hr^i$  by  $r^3$ . (This works because  $r^3 \in N_G(H)$ ).

# G-set automorphisms



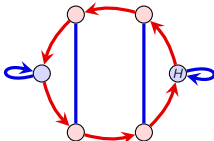
What do you notice about normalizers vs. symmetries of the actions graphs?

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



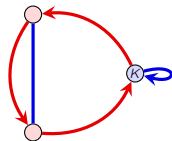
$$\text{Aut}_G(N \setminus G) \cong D_3 \cong N_G(N)/N$$

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



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

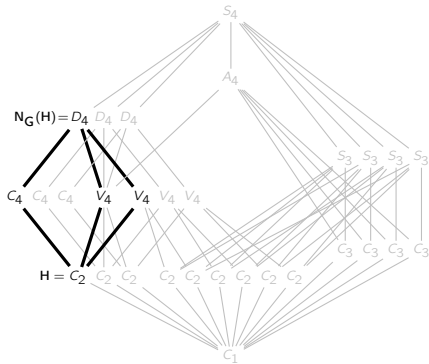
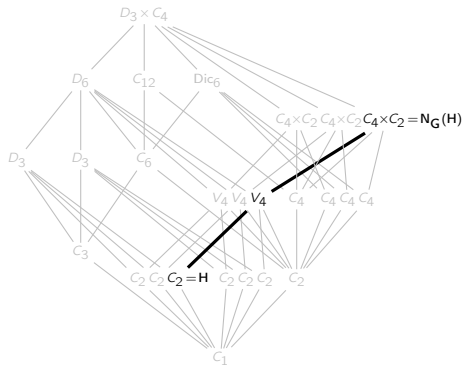
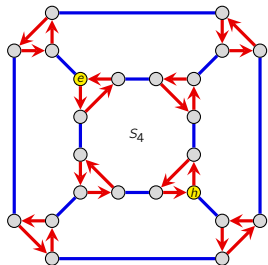
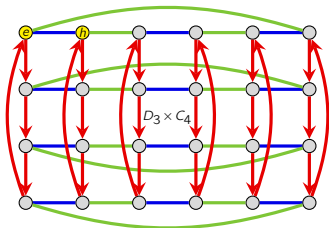
$K = \langle r^3, f \rangle$ ; fully unnormal



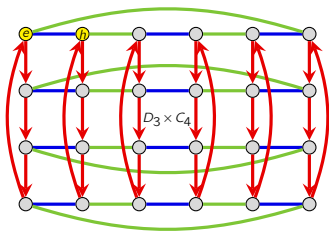
$$\text{Aut}_G(K \setminus G) \cong \langle 1 \rangle \cong N_G(K)/K$$



# G-set automorphisms

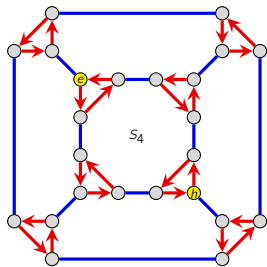
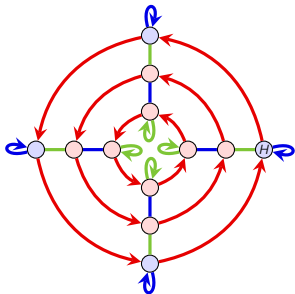


# G-set automorphisms



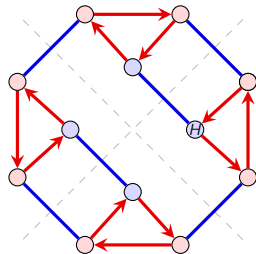
$$H = \langle (f, 1) \rangle \leq D_3 \times C_4 = G$$

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



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

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



# The $G$ -set automorphism group

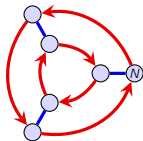
## Theorem

For any  $H \leq G$ , the  $G$ -set automorphism group of  $S = H \backslash G$  is

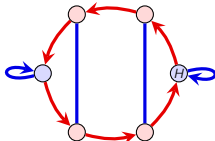
$$\text{Aut}_G(S) \cong N_G(H)/H.$$

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

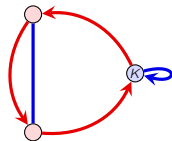
1. **Lemma 1:**  $\sigma: Hg \mapsto Hxg$ , for some fixed  $x \in G$  (i.e.,  $\sigma = \phi(x)$ ).
2. **Lemma 2:**  $\phi(x) \in \text{Aut}_G(S)$  iff  $x \in N_G(H)$ . That is,  $\sigma: Hg \mapsto xHg$ .
3. **FHT:** Two  $\phi(x) = \phi(x')$  iff  $x, x'$  are in the same coset of  $H$ .



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



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



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

# The $G$ -set automorphism group

## Lemma 1

Any  $G$ -set automorphism  $\sigma \in \text{Aut}_G(S)$ , for  $S = H \backslash G$ , is determined by the image of  $H$ :

if  $\sigma: H \mapsto Hx$ , then  $\sigma: Hg \mapsto Hxg$ , for all  $g \in G$ .

## Proof

Since  $\sigma$  is  $G$ -equivariant, it commutes with each  $\phi(g) \in \text{Perm}(S)$ .

That is, the following diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{\phi(g)} & S \\ \sigma \downarrow & & \downarrow \sigma \\ S & \xrightarrow{\phi(g)} & S \end{array} \qquad \begin{array}{ccc} H & \xrightarrow{\phi(g)} & Hg \\ \sigma \downarrow & & \downarrow \sigma \\ Hx & \xrightarrow{\phi(g)} & Hxg \end{array}$$

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

# The $G$ -set automorphism group

## Lemma 2

Let  $S = H \backslash G$ . The map of right cosets

$$\sigma_x: S \rightarrow S, \quad \sigma_x: Hg \mapsto Hxg$$

is a  $G$ -set automorphism iff  $x \in N_G(H)$ .

## Proof

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

$$\begin{array}{ccc} S & \xrightarrow{\phi(h)} & S \\ \sigma_x \downarrow & & \downarrow \sigma_x \\ S & \xrightarrow{\phi(h)} & S \end{array}$$

$$\begin{array}{ccc} H & \xrightarrow{\phi(h)} & H \\ \sigma_x \downarrow & & \downarrow \sigma_x \\ Hx & \xrightarrow{\phi(h)} & Hxh = Hx \end{array}$$

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

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

# The $G$ -set automorphism group

## Lemma 2

Let  $S = H \backslash G$ . The map of right cosets

$$\sigma_x: S \longrightarrow S, \quad \sigma_x: Hg \longmapsto Hxg$$

is a  $G$ -set automorphism iff  $x \in N_G(H)$ .

## Proof

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

By Lemma 1:  $\sigma_x: Hg \mapsto Hxg = xHg$ .

The operations  $\sigma_x$  (left-multiplying by  $x$ ), and  $\phi(g)$  (right-multiplying by  $g$ ) clearly commute. ✓

$$\begin{array}{ccc} S & \xrightarrow{\phi(g)} & S \\ \sigma_x \downarrow & & \downarrow \sigma_x \\ S & \xrightarrow{\phi(g)} & S \end{array}$$

$$\begin{array}{ccc} H & \xrightarrow{\phi(g)} & Hg \\ \phi(x) \downarrow & & \downarrow \phi(x) \\ Hx & \xrightarrow{\phi(g)} & Hxg = xHg \end{array}$$

## The $G$ -set automorphism group

### Theorem

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

$$\text{Aut}_G(S) \cong N_G(H)/H.$$

### Proof

We'll apply the FHT to the map

$$f: N_G(H) \longrightarrow \text{Aut}_G(S), \quad x \longmapsto \sigma_x,$$

where  $\sigma_x: Hg \longmapsto Hxg$ .

Homomorphism: Straightforward exercise. ✓

Onto: Immediate from Lemma 2. ✓

Ker( $\phi$ ) =  $H$ . " $\subseteq$ ":

$$x \in \text{Ker}(\phi) \iff Hg = Hxg, \forall g \in G \iff H = Hx \iff x \in H.$$

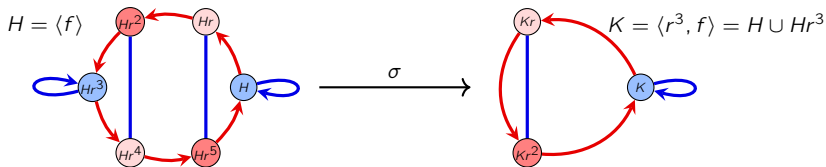
" $\supseteq$ ": If  $h \in H$ , then  $\sigma_h: Hg \mapsto Hhg = Hx$ . ✓

The result now follows from the FHT. □

## G-set homomorphisms

Dropping bijectivity of  $\sigma: S_1 \rightarrow S_2$  defines a **G-set homomorphism**, or **G-equivariant map**.

Consider this example of  $D_6$ -sets:



This can be described by the following commutative diagram:

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

### Key idea

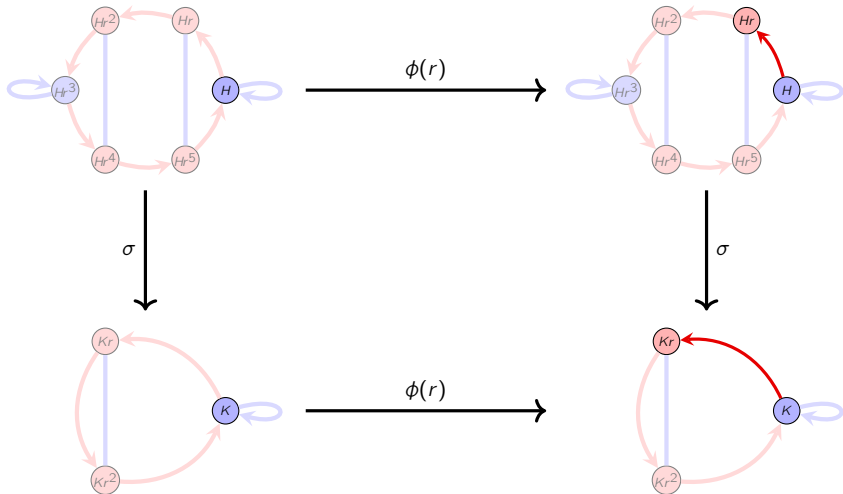
We say that “the map  $\sigma$  commutes with the action of the group.”



## G-set homomorphisms

Here is that example again for  $G = D_6$  and subgroups:

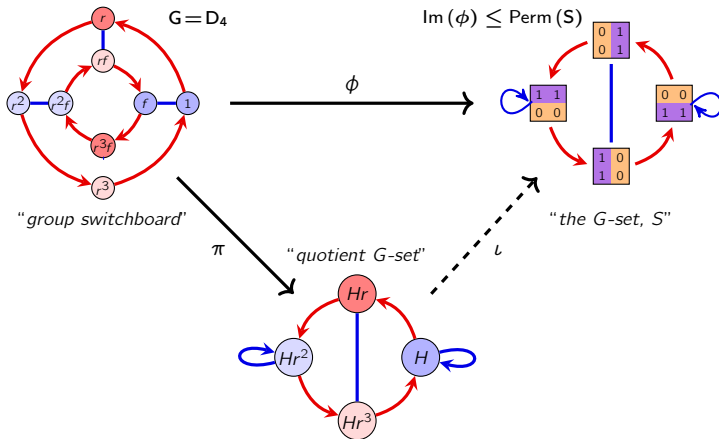
$H = \langle f \rangle$  (moderately unnormal),  $K = \langle r^3, f \rangle = H \cup Hr^3 = N_G(H)$ , (fully unnormal)



# The orbit-stabilizer theorem, restated

## FHT for $G$ -sets

If  $\phi: G \rightarrow \text{Perm}(S)$  is a transitive action and  $s \in S$ , then  $S$  is isomorphic to set of cosets of the stabilizer, as  $G$ -sets.



## 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  $x^p = e$ .  $\square$

## $p$ -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, in “ $p$ -group towers.”
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  $Q_8$ ,  $C_8$ ,  $C_4 \times C_2$ ,  $D_8$ ,  $SD_8$ ,  $Q_{16}$ ,  $SA_8$ ,  $SA_8$ ,  $DQ_8$ , ...

### $p$ -group Lemma

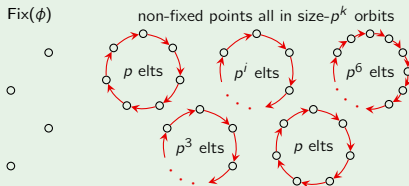
If a  $p$ -group  $G$  acts on a set  $S$  via  $\phi: G \rightarrow \text{Perm}(S)$ , then

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

### Proof (sketch)

Suppose  $|G| = p^n$ .

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



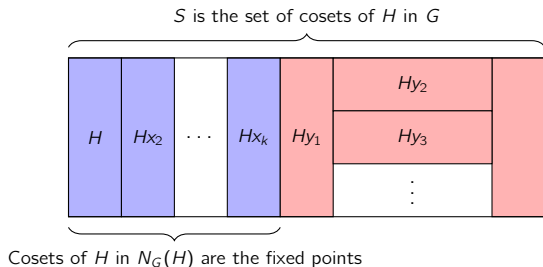
### Normalizer lemma, Part 1

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  $S = H \backslash G = \{Hx \mid x \in G\}$ . 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  $\phi$  are the cosets  $Hx$  in the **normalizer**  $N_G(H)$ :

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

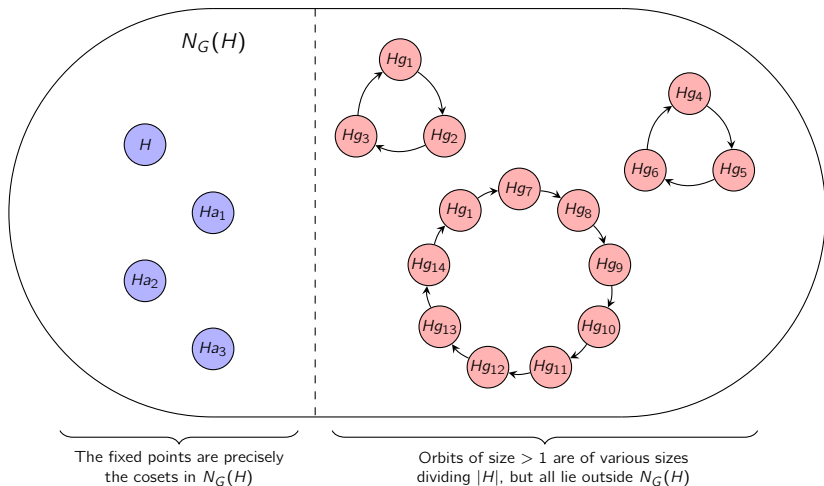
Therefore,  $|\text{Fix}(\phi)| = [N_G(H) : H]$ , and  $|S| = [G : H]$ . By our  $p$ -group Lemma,

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

## $p$ -groups

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

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



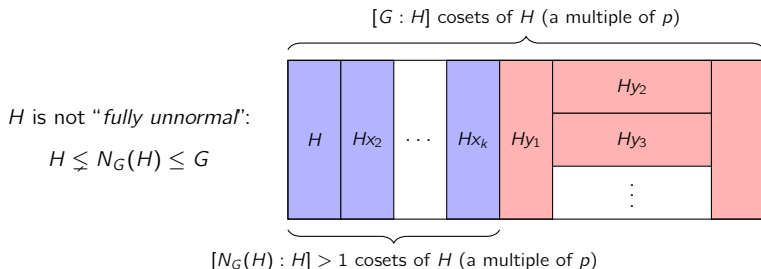


## $p$ -subgroups

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

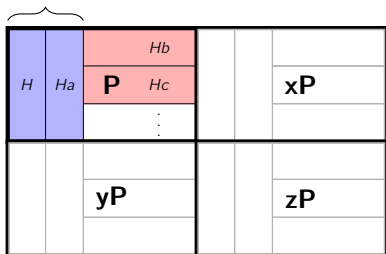
- $p$ -groups cannot have any fully unnormal subgroups (i.e.,  $H \subsetneq N_G(H)$ ).
- In any finite group, the only fully unnormal  $p$ -subgroups are maximal.

## Normalizers of $p$ -subgroups

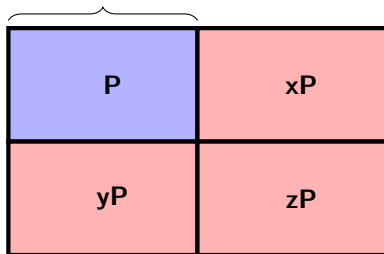
Let  $H$  be properly contained in a maximal  $p$ -subgroup  $P \leq G$ .

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

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



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



## Proof of the normalizer lemma

### Normalizer lemma, Part 2

Suppose  $|G| = p^n m$ , and  $H \leq G$  with  $|H| = p^i < p^n$ . Then  $H \not\leq N_G(H)$ , 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  $G$ :

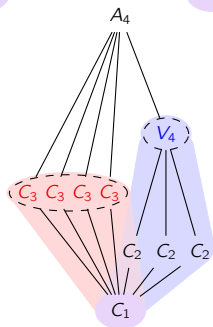
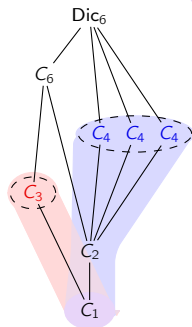
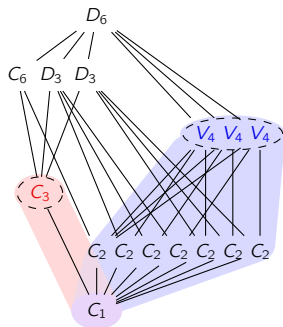
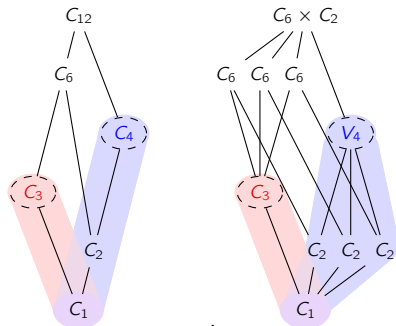
1. How big are its  $p$ -subgroups?
2. How are the  $p$ -subgroups related?
3. How many  $p$ -subgroups are there?
4. Are any of them normal?

## 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.

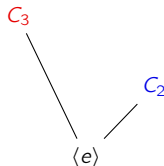
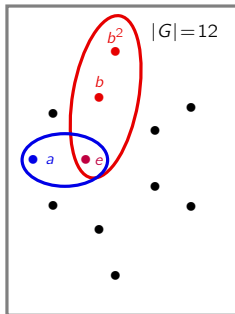
Together, these place strong restrictions on the structure of a group  $G$  with a fixed order.

## 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 1<sup>st</sup> Sylow theorem: existence of $p$ -subgroups

## First Sylow theorem

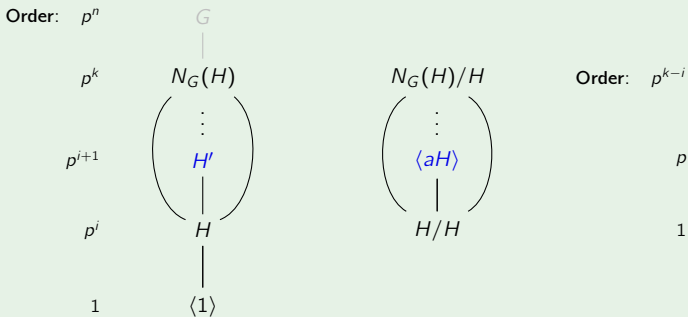
$G$  has a subgroup of order  $p^k$ , for each  $p^k$  dividing  $|G|$ .

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

## Proof

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

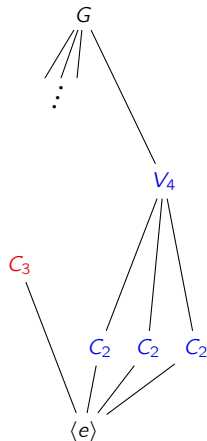
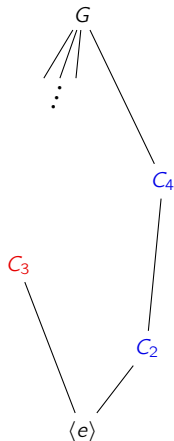
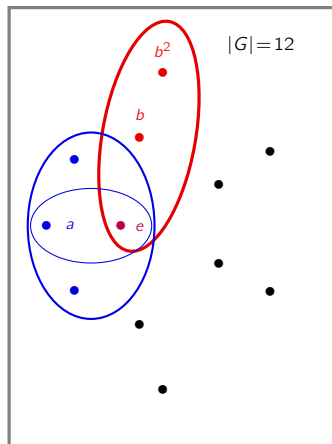
Find an element  $aH$  of order  $p$ . The union of cosets in  $\langle aH \rangle$  is a subgroup of order  $p^{i+1}$ .





## Our unknown group of order 12

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



# The 2<sup>nd</sup> Sylow theorem: relationship among $p$ -subgroups

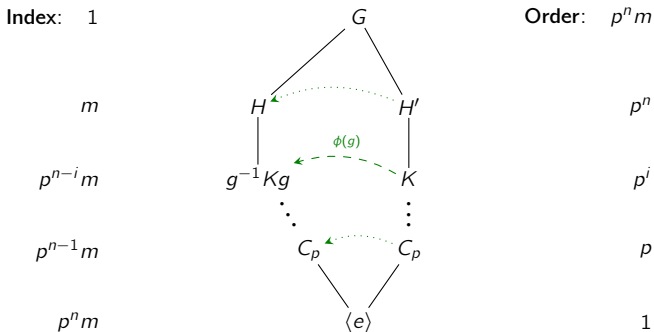
## Second Sylow theorem

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  $H$ .



## The 2<sup>nd</sup> Sylow theorem: All Sylow $p$ -subgroups are conjugate

### Strong second Sylow theorem

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

### Proof

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

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

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

A **fixed point** of  $\phi$  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  $\phi$  has a fixed point  $Hg$ , we're done!*

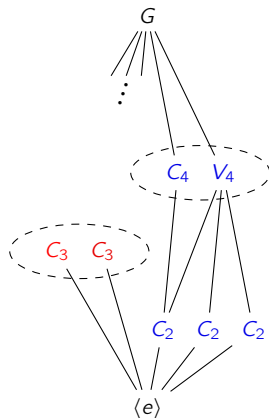
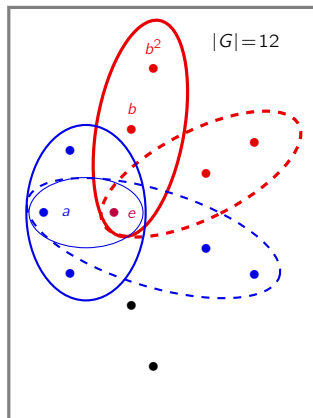
All we need to do is show that  $|\text{Fix}(\phi)| \not\equiv_p 0$ . By the  $p$ -group Lemma,

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

## 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.





## 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 3<sup>rd</sup> 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

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

The subgroup  $H$  acts on  $S = \text{Syl}_p(G)$  by **conjugation**, via  $\phi: G \rightarrow \text{Perm}(S)$ , where

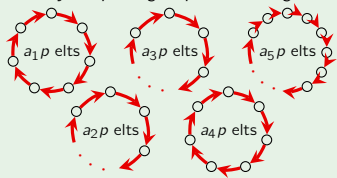
$$\phi(h) = \text{the permutation sending each } K \text{ to } h^{-1}Kh.$$

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

$$|\text{Fix}(\phi)| = 1$$



*other Sylow  $p$ -subgroups are in larger orbits*



$$\left. \begin{array}{l} \text{total \# Sylow } p\text{-subgroups} \\ = n_p = |S| \equiv_p |\text{Fix}(\phi)| \end{array} \right\}$$

# The 3<sup>rd</sup> Sylow theorem: number of $p$ -subgroups

## Proof (cont.)

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

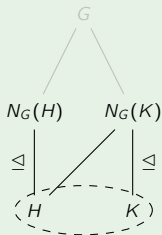
Let  $K \in \text{Fix}(\phi)$ . Then  $K \leq G$  is a Sylow  $p$ -subgroup satisfying

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

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

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

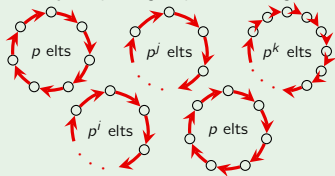
By the  $p$ -group Lemma,  $n_p := |S| \equiv_p |\text{Fix}(\phi)| = 1$ . □



$$|\text{Fix}(\phi)| = 1$$

$$H = K$$

other Sylow  $p$ -subgroups are in larger orbits



$$\left. \begin{array}{l} \text{total \# Sylow } p\text{-subgroups} \\ = n_p = |S| \equiv_p |\text{Fix}(\phi)| = 1 \end{array} \right\}$$



## Summary of the proofs of the Sylow theorems

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

For the 2<sup>nd</sup> and 3<sup>rd</sup> 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  $S = H \setminus G$  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:

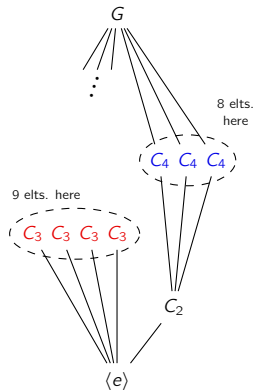
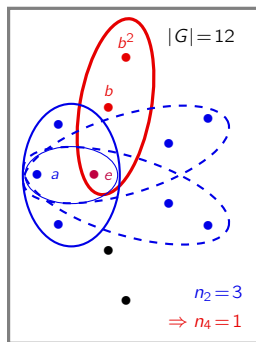
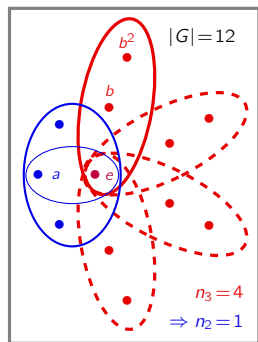
- $n_3$  Sylow 3-subgroups, each of order 3.

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

- $n_2$  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.)

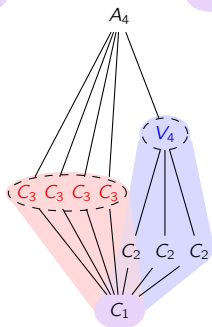
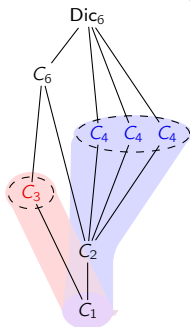
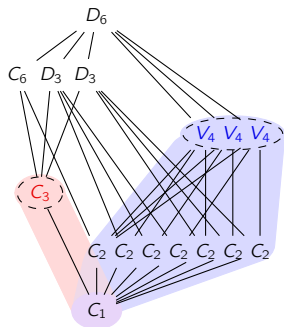
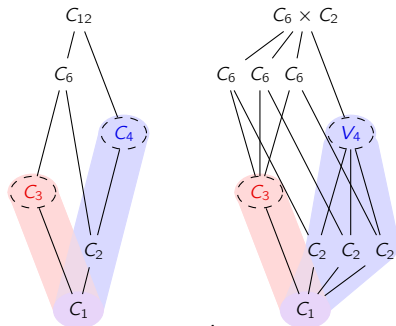


## The five groups of order 12

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.  $\square$

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.,  $S = H \backslash G$ ) 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  $H$ :

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

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