# Lecture 1.2: Group actions

Matthew Macauley

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

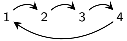
Math 8510, Abstract Algebra I

# The symmetric group

## Definition

The group of all permutations of $\{1, \dots, n\}$ is the symmetric group, denoted $S_n$.

We can concisely describe permutations in cycle notation, e.g.,

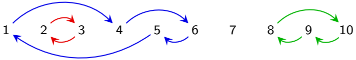



as $(1\ 2\ 3\ 4)$.

## Observation 1

Every permutation can be decomposed into a product of disjoint cycles, and disjoint cycles commute.

We usually don't write 1-cycles (fixed points). For example, in $S_{10}$, we can write




as $(1\ 4\ 6\ 5)\,(2\ 3)\,(8\ 10\ 9)$.

By convention, we'll read cycles from right-to-left, like function composition. [*Note.* Many sources read left-to-right.]

# The symmetric group

## Remarks

- The inverse of the cycle $(1\ 2\ 3\ 4)$ is $(4\ 3\ 2\ 1) = (1\ 4\ 3\ 2)$.
- If $\sigma$ is a $k$-cycle, then $|\sigma| = k$.
- If $\sigma = \sigma_1 \cdots \sigma_m$, all disjoint, then $|\sigma| = \operatorname{lcm}(|\sigma_1|, \dots, |\sigma_m|)$.
- A 2-cycle is called a transposition.
- Every cycle (and hence element of $S_n$) can be written as a product of transpositions:

$$(1\ 2\ 3 \cdots k) = (1\ k)\,(1\ k{-}1) \cdots (1\ 3)\,(1\ 2).$$

- We say $\sigma \in S_n$ is even if it can be written as a product of an even number of transpositions, otherwise it is odd.

It is easy to check that the following is a homomorphism:

$$f \colon S_n \longrightarrow \{1, -1\}, \qquad f(\sigma) = \begin{cases} 1 & \sigma \text{ even} \\ -1 & \sigma \text{ odd.} \end{cases}$$

Define the alternating group to be $A_n := \ker f$.

## Proposition

If $n \geq 2$, then $[S_n : A_n] = 2$. (Equivalently, $f$ is onto.)

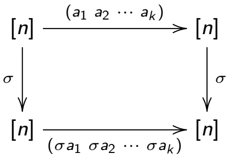
# The symmetric group

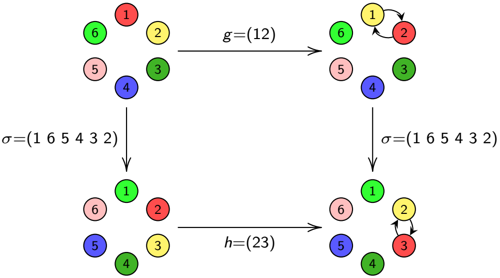
## Exercise

Let $(a_1\ a_2\ \cdots\ a_k) \in S_n$ be a $k$-cycle. Then

$$\sigma(a_1\ a_2\ \cdots\ a_k)\sigma^{-1} = (\sigma a_1\ \sigma a_2\ \cdots\ \sigma a_k).$$

A good way to visual this is with a commutative diagram:




Note that no matter what $\sigma$ is, $\sigma(1\ 2)\sigma^{-1}$ will be a transposition. (Why?)

# Conjugacy and cycle type

## Definition

Two elements $x, y \in G$ are conjugate if $x = gyg^{-1}$ for some $g \in G$.

It is easy to show that conjugacy is an equivalence relation. The equivalence class containing $x \in G$ is called its conjugacy class, denoted $\text{cl}_G(x)$.

Say that elements in $S_n$ have the same cycle type if when written as a product of disjoint cycles, there are the same number of length-$k$ cycles for each $k$.

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

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

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

## Proosition

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

As a corollary, $Z(S_n) = 1$ for $n \geq 3$.

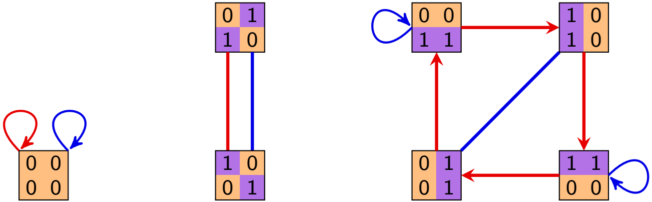
# Group actions

Intuitively, a group action occurs when a group $G$ naturally permutes a set $S$ of objects.

This is best motivated with an example. Consider the size-7 set consisting of the following "binary squares."

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

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



# A "group switchboard"

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

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

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

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

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

Let $\mathrm{Perm}(S)$ be the group of permutations of $S$. Thus, if $|S| = n$, then $\mathrm{Perm}(S) \cong S_n$.

### Definition

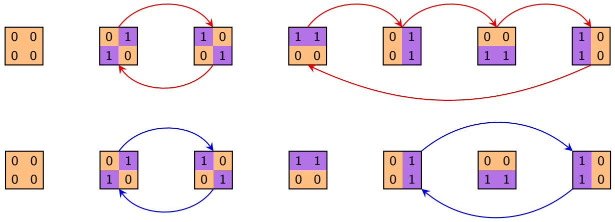
A group $G$ acts on a set $S$ if there is a homomorphism $\phi \colon G \to \mathrm{Perm}(S)$.

# A "group switchboard"

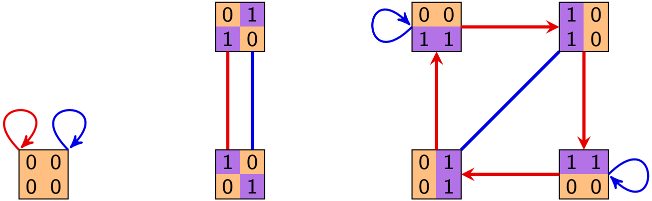
Returning to our binary square example, pressing the $r$-button and $f$-button permutes the set $S$ as follows:

$\phi(r)$ :

$\phi(f)$ :



Observe how these permutations are encoded in the action diagram:



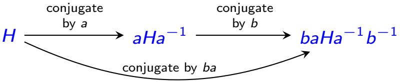
# Left actions vs. right actions (an annoyance we can deal with)

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

However, sometimes it has to be the same as "*pressing the ba-button*."

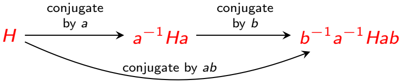
This is best seen by an example. Suppose our action is conjugation:

"Left group action"




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

"Right group action"




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

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

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

We'll usually keep the $\phi$, 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

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

such that

- $s.(ab) = (s.a).b$, for all $a, b \in G$ and $s \in S$
- $s.1 = s$, for all $s \in S$.

A left group action can be defined similarly.

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

Usually if there is a left action, there is a related right action. We will usually use right actions, and we will write

$$s.\phi(g)$$

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

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

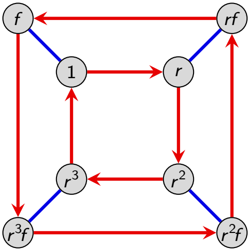
# Cayley diagrams as action diagrams

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

For example, consider the group $G = D_4 = \langle r, f \rangle$ acting on itself. That is, $S = D_4 = \{1, r, r^2, r^3, f, rf, r^2f, r^3f\}$.

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

Here is the action diagram:




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

# Orbits, stabilizers, and fixed points

Suppose $G$ acts on a set $S$. Pick a configuration $s \in S$. We can ask two questions about it:

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

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

## Definition

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

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

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

(ii) The stabilizer of $s$ in $G$ is

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

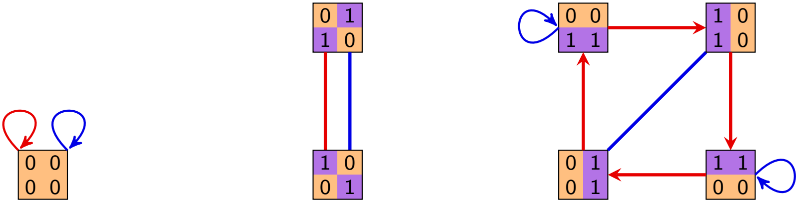
(iii) The fixed points of the action are the orbits of size 1:

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

Note that the orbits of $\phi$ are the connected components in the action diagram.

# Orbits, stabilizers, and fixed points

Let's revisit our running example:




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

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

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

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

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

Observations?

# Orbits and stabilizers

## Proposition

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

## Proof (outline)

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

(i) *Contains the identity*. That is, $s.\phi(1) = s$.

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

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

You'll do this on the homework.

## Remark

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

$$\mathrm{Ker}\,\phi = \{g \in G \mid \phi(g) = 1\} = \{g \in G \mid s.\phi(g) = s \text{ for all } s \in S\}.$$

Notice that

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

# The Orbit-Stabilizer Theorem

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

## Orbit-Stabilizer theorem

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

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

## Proof

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

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

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

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

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

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

## Proof (cont.)

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

We are seeking a bijection between $\text{Orb}(s)$, and the right cosets of $\text{Stab}(s)$.

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

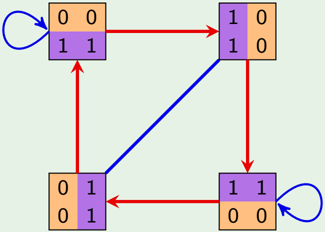
Let $s =$ 


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

Partition of $D_4$ by the right cosets of $H$ :

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

| | | | |
|---|---|---|---|
| $1$ | $r$ | $r^2$ | $r^3$ |
| $f$ | $fr$ | $fr^2$ | $fr^3$ |
| $H$ | $Hr$ | $Hr^2$ | $Hr^3$ |




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

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

### Proof (cont.)

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

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

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

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

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

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

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

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

# Groups acting on elements, subgroups, and cosets

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

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

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

For example, we will see how Cayley's theorem (every group $G$ is isomorphic to a group of permutations) follows immediately once we look at the correct action.

Here are common examples of group actions:

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

For each of these, we'll analyze the orbits, stabilizers, and fixed points.

# Groups acting on themselves by right-multiplication

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

*Every group is isomorphic to a group of permutations.*

## Cayley's theorem

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

## Proof.

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

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

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

$$\text{Stab}(x) = \{g \in G \mid xg = x\} = \{1\}\,.$$

Therefore, the kernel of this action is $\text{Ker}\,\phi = \bigcap_{x \in G} \text{Stab}(x) = \{1\}$.

Since $\text{Ker}\,\phi = \{1\}$, the homomorphism $\phi$ is 1–1. □

## Groups acting on themselves by conjugation

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

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

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

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

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

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

- The fixed points of $\phi$ are precisely those in the center of $G$:

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

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

### Theorem

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

### The Class Equation

For any finite group $G$,

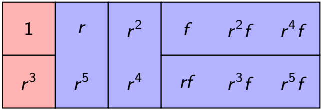
$$|G| = |Z(G)| + \sum |\,\mathrm{cl}_G(x_i)|$$

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

# Groups acting on themselves by conjugation

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

The orbits of the action are the conjugacy classes:




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

By the Orbit-Stabilizer theorem:

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

The stabilizer subgroups are as follows:

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

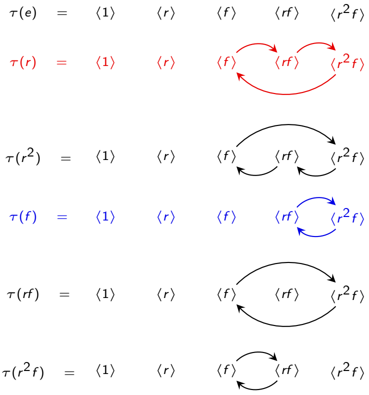
# Groups acting on subgroups by conjugation

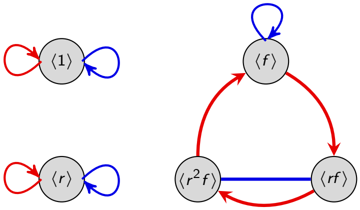
Let $G = D_3$, and let $S$ be the set of proper subgroups of $G$:

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

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

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




The action diagram.

$$\mathrm{Stab}(\langle 1\rangle) = \mathrm{Stab}(\langle r\rangle) = D_3 = N_{D_3}(\langle r\rangle)$$
$$\mathrm{Stab}(\langle f\rangle) = \langle f\rangle = N_{D_3}(\langle f\rangle),$$
$$\mathrm{Stab}(\langle rf\rangle) = \langle rf\rangle = N_{D_3}(\langle rf\rangle),$$
$$\mathrm{Stab}(\langle r^2 f\rangle) = \langle r^2 f\rangle = N_{D_3}(\langle r^2 f\rangle).$$

# Groups acting on subgroups by conjugation

More generally, any group $G$ acts on its set $S$ of subgroups by **conjugation**:

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

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

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

- The orbit of $H$ consists of all conjugate subgroups:
$$\mathrm{Orb}(H) = \{g^{-1}Hg \mid g \in G\}\,.$$
- The stabilizer of $H$ is the normalizer of $H$ in $G$:
$$\mathrm{Stab}(H) = \{g \in G \mid g^{-1}Hg = H\} = N_G(H)\,.$$
- The fixed points of $\phi$ are precisely the normal subgroups of $G$:
$$\mathrm{Fix}(\phi) = \{H \leq G \mid g^{-1}Hg = H \text{ for all } g \in G\}\,.$$
- The kernel of this action is $G$ iff every subgroup of $G$ is normal. In this case, $\phi$ is the trivial homomorphism: pressing the $g$-button fixes (i.e., normalizes) every subgroup.

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

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

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

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

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

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

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

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

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

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

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

# Fixed points of group actions

Recall the subtle difference between fixed points and stabilizers:

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

## Lemma

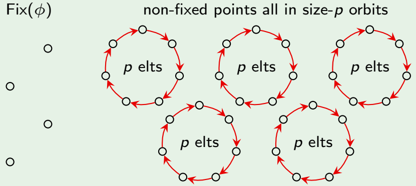
If a group $G$ of prime order $p$ acts on a set $S$ via $\phi\colon G \to \text{Perm}(S)$, then

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

## Proof (sketch)

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

I'll let you fill in the details.



# Cauchy's Theorem

## Cauchy's theorem

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

## Proof

Let $P$ be the set of ordered $p$-tuples of elements from $G$ whose product is 1, i.e.,

$$(x_1, x_2, \ldots, x_p) \in P \quad \text{iff} \quad x_1 x_2 \cdots x_p = 1\,.$$

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

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

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

(This is because if $x_1 x_2 \cdots x_p = 1$, then $x_2 x_3 \cdots x_p x_1 = 1$ as well.)

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

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

# Cauchy's Theorem

## Proof (cont.)

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

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

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

Thus, there is some $(x, \dots, x) \in P$, with $x \neq 1$ such that $x^p = 1$. $\square$

## Corollary

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

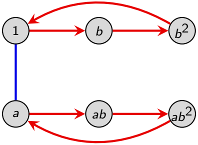
Note that just by using the theory of group actions, and the orbit-stabilzer theorem, we have already proven:

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

# Application of group actions: Classification of groups of order 6

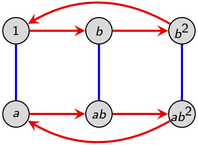
By Cauchy's theorem, every group of order 6 must have an element $a$ of order 2, and an element $b$ of order 3.

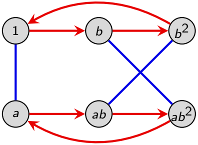
Clearly, $G = \langle a, b \rangle$ for two such elements. Thus, $G$ must have a Cayley diagram that looks like the following:




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

$C_6 \cong C_2 \times C_3$




$D_3$

# Application of group actions: Conjugacy in $S_n$

A group $G$ is simple if its only normal subgroups are 1 and $G$.

**Proposition (proofs will be done on the board)**

1. If $n \geq 5$, then all 3-cycles are conjugate in $A_n$.
2. If $n \geq 3$, then $A_n$ is generated by 3-cycles.
3. If $n \neq 4$, then $A_n$ is simple.

The following Cayley diagram for $A_4$ shows why it is not simple.

$a = (1\ 2\ 3)$

$b = (1\ 3\ 4)$

$c = (1\ 4\ 2)$

$d = (2\ 4\ 3)$

$x = (1\ 2)(3\ 4)$

$y = (1\ 3)(2\ 4)$

$z = (1\ 4)(2\ 3)$