Chapter 9: Group actions

Matthew Macauley

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

Math 4120, Spring 2014

Overview

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

For example:

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

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

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

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

Actions vs. configurations

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

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

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

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

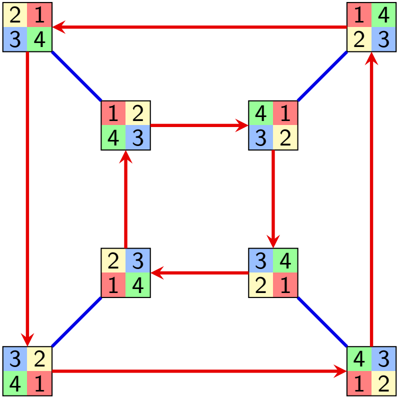
The 8 configurations (or *states*) of the square are the following:

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

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

Actions diagrams

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



In the beginning of this course, we picked a configuration to be the "solved state," and this gave us a bijection between configurations and actions (group elements). The resulting diagram was a Cayley diagram. In this chapter, we'll skip this step.

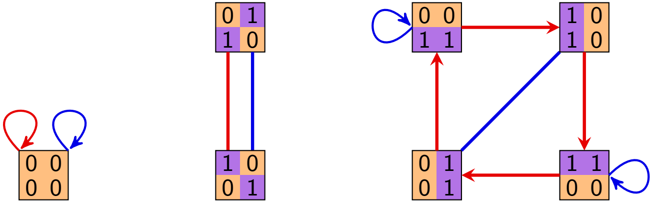
Actions diagrams

In all of the examples we saw in the beginning of the course, we had a bijective correspondence between actions and states. *This need not always happen!*

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

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

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



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

A "group switchboard"

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

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

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

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

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

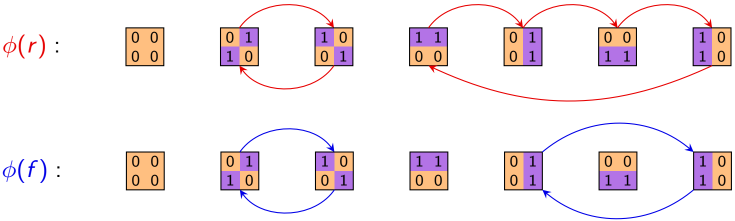
Let $\mathrm{Perm}(S)$ be the group of permutations of S. Thus, if $|S| = n$, then $\mathrm{Perm}(S) \cong S_n$. (We typically think of S_n as the permutations of $\{1, 2, \dots, n\}$.)

Definition

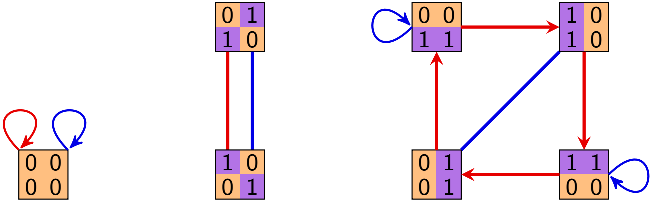
A group G acts on a set S if there is a homomorphism $\phi \colon G \to \mathrm{Perm}(S)$.

A "group switchboard"

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



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"

$$\begin{tikzcd} H \arrow[r, "\text{conjugate by } a"] \arrow[rr, bend right, "\text{conjugate by } ba"'] & aHa^{-1} \arrow[r, "\text{conjugate by } b"] & baHa^{-1}b^{-1} \end{tikzcd}$$

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

"Right group action"

$$\begin{tikzcd} H \arrow[r, "\text{conjugate by } a"] \arrow[rr, bend right, "\text{conjugate by } ab"'] & a^{-1}Ha \arrow[r, "\text{conjugate by } b"] & b^{-1}a^{-1}Hab \end{tikzcd}$$

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

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

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

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

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

Alternative definition (other textbooks)

A right group action is a mapping

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

such that

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

A left group action can be defined similarly.

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

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

$$s.\phi(g)$$

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

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

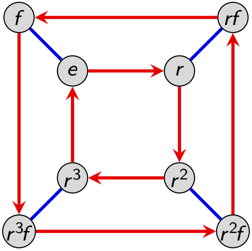
Cayley diagrams as action diagrams

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

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

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

Here is the action diagram:



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

Orbits, stabilizers, and fixed points

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

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

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

Definition

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

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

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

(ii) The stabilizer of s in G is

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

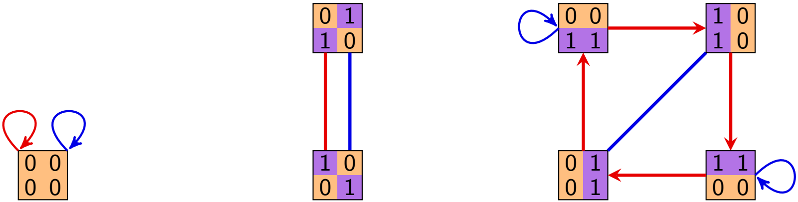
(iii) The fixed points of the action are the orbits of size 1:

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

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

Orbits, stabilizers, and fixed points

Let's revisit our running example:



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

$$\mathrm{Stab}\left(\begin{array}{|cc|}\hline 0&0\\0&0\\\hline\end{array}\right)=D_4,$$

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

$$\mathrm{Stab}\left(\begin{array}{|cc|}\hline 0&0\\1&1\\\hline\end{array}\right)=\{e,f\},\qquad \mathrm{Stab}\left(\begin{array}{|cc|}\hline 1&0\\1&0\\\hline\end{array}\right)=\{e,r^2f\},$$

$$\mathrm{Stab}\left(\begin{array}{|cc|}\hline 1&1\\0&0\\\hline\end{array}\right)=\{e,f\},\qquad \mathrm{Stab}\left(\begin{array}{|cc|}\hline 0&1\\0&1\\\hline\end{array}\right)=\{e,r^2f\}.$$

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, $s.\phi(e) = s$.

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

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

You'll do this on the homework.

Remark

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

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

Notice that

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

The Orbit-Stabilizer Theorem

The following result is another one of the "crowning achievements" 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

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

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

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

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 $\operatorname{Orb}(s)$, and the right cosets of $\operatorname{Stab}(s)$.

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

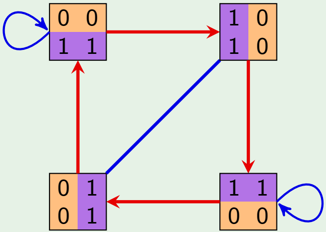
Let $s = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$

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

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

Partition of D_4 by the right cosets of H :

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



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

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

Proof (cont.)

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

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

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

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

"$\Leftarrow$" *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.

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**:

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

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

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

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

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

Groups acting on themselves by conjugation

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

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

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

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

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

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

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

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

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

Theorem

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

Groups acting on themselves by conjugation

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

The orbits of the action are the conjugacy classes:

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

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

By the Orbit-Stabilizer theorem:

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

The stabilizer subgroups are as follows:

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

Groups acting on subgroups by conjugation

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

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

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

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

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

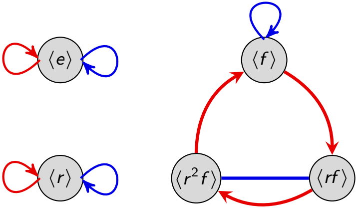
$\tau(r) \quad = \quad \langle e\rangle \quad \langle r\rangle \quad \langle f\rangle \quad \langle rf\rangle \quad \langle r^2 f\rangle$

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

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

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

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



The action diagram.

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

Groups acting on subgroups by conjugation

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

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

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

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

- The orbit of H consists of all conjugate subgroups:

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

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

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

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

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

- The kernel of this action is G iff every subgroup of G is normal. In this case, ϕ is the trivial homomorphism: pressing the g-button fixes (i.e., normalizes) every subgroup.

Groups acting on cosets of H by right-multiplication

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

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

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

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

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

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

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

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

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

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

More on fixed points

Recall the subtle difference between fixed points and stabilizers:

- The fixed points of an action $\phi\colon G \to \mathrm{Perm}(S)$ 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

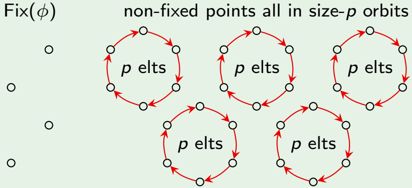
If a group G of prime order p acts on a set S via $\phi\colon G \to \mathrm{Perm}(S)$, then

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

Proof (sketch)

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

I'll let you fill in the details.



Cauchy's Theorem

Cauchy's theorem

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

Proof

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

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

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

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

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

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

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

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

Cauchy's Theorem

Proof (cont.)

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

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

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

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

Corollary

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

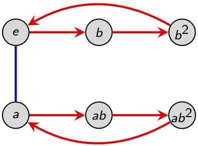
Note that just by using the theory of group actions, and the orbit-stabilzer theorem, we have already proven:

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

Classification of groups of order 6

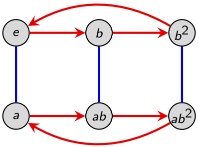
By Cauchy's theorem, every group of order 6 must have an element a of order 2, and an element b of order 3.

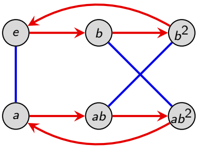
Clearly, $G = \langle a, b \rangle$ for two such elements. Thus, G must have a Cayley diagram that looks like the following:



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

$C_6 \cong C_2 \times C_3$





D_3