Applications of group actions!

Spencer Bagley

With many thanks to Matthew Macauley,
`http://www.math.clemson.edu/~macaule/`

14 Apr 2025

Overview

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

Formal definition

A group G acts on a set S if there is a homomorphism $\phi\colon G \longrightarrow \mathrm{Perm}(S)$.
We'll use right group actions,
and we'll write $s.\phi(g)$ to denote "where pushing the g-button sends state s."

Definition

A set S with a (right) action by G is called a (right) G-set.

Big ideas

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

Notation

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

Five features of every group action

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

	local (about an s or a g)	global (about the whole action ϕ)
subsets of S	$\mathrm{orb}(s)$ $\mathrm{fix}(g)$	$\mathrm{Fix}(\phi) = \bigcap_{g \in G} \mathrm{fix}(g)$
subgroups of G	$\mathrm{stab}(s)$	$\mathrm{Ker}(\phi) = \bigcap_{s \in S} \mathrm{stab}(s)$

"Duality:" columns vs. rows in the fixed-point table:

- the stablizers can be read off the columns: *group elements that fix $s \in S$*
- the kernel is the rows with a check in every column
- the fixators can be read off the rows: *set elements fixed by $g \in G$*
- the fixed points are the columns with a check in every row

Fixed-point tables

Here is the fixed-point table for $G = D_4$ acting on S the list of 7 “binary squares.”

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

$\text{Ker}(\phi) = \{1\}$ and $\text{Fix}(\phi) = \{$ the 0 0 0 0 one$\}$.

Two big theorems

Orbit-stabilizer theorem

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

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

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

Proof: Put elements $s.\phi(g)$ of $\mathrm{orb}(s)$ in correspondence with cosets of the stabilizer.

Orbit-counting theorem

Let a finite group G act on a set S via $\phi\colon G \to \mathrm{Perm}(S)$.
Then the number of orbits is the average size of the fixators:

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

Equivalently, the number of orbits is the average size of the stabilizers:

$$|\mathrm{Orb}(\phi)| = \frac{1}{|G|} \sum_{s \in S} |\mathrm{stab}(s)|.$$

Proof: Count checkmarks in the fixed point table.

Groups acting on themselves!

Groups acting on “themselves”

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 (i.e., its set of elements) 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.

(Please put the word “right” in a salt shaker and shake it all over those bullet points.)

Groups acting on subgroups by conjugation

Any group G acts on its set S of subgroups, $S = \{H \mid H \leq G\}$ by **right-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:

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

- 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 fixator of g are the subgroups that g normalizes:

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

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

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

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

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

Groups acting on subgroups by conjugation

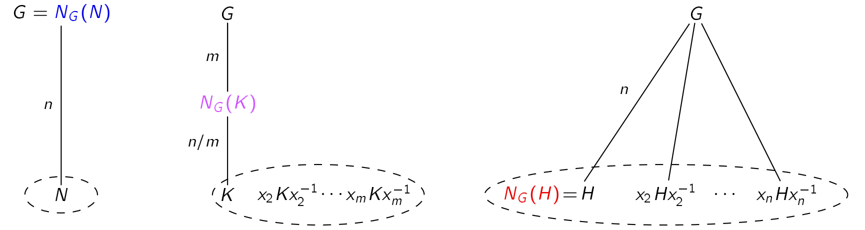
Let's apply our two theorems:

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

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

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

$$\#\text{conjugacy classes of subgroups of } G = \mathbb{E}\big[\#\text{ subgroups } g \text{ normalizes}\big].$$



normal — $\left|\mathrm{cl}_G(N)\right| = 1$

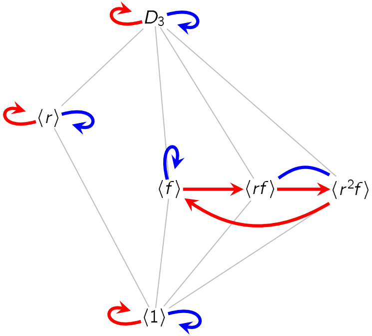
moderately unnormal — $1 < \left|\mathrm{cl}_G(K)\right| < [G : K]$

fully unnormal — $\left|\mathrm{cl}_G(H)\right| = [G : H]$; as large as possible

Groups acting on subgroups by conjugation

Here is an example of $G = D_3$ acting on its subgroups by a homomorphism $\tau : D_3 \to \mathrm{Perm}(S) \cong S_6$.

$$
\begin{array}{rcllllll}
\tau(1) & = & \langle 1 \rangle & \langle r \rangle & \langle f \rangle & \langle rf \rangle & \langle r^2 f \rangle & D_3 \\
\color{red}{\tau(r)} & \color{red}{=} & \color{red}{\langle 1 \rangle} & \color{red}{\langle r \rangle} & \color{red}{\langle f \rangle} & \color{red}{\langle rf \rangle} & \color{red}{\langle r^2 f \rangle} & D_3 \\
\tau(r^2) & = & \langle 1 \rangle & \langle r \rangle & \langle f \rangle & \langle rf \rangle & \langle r^2 f \rangle & D_3 \\
\color{blue}{\tau(f)} & \color{blue}{=} & \color{blue}{\langle 1 \rangle} & \color{blue}{\langle r \rangle} & \color{blue}{\langle f \rangle} & \color{blue}{\langle rf \rangle} & \color{blue}{\langle r^2 f \rangle} & D_3 \\
\tau(rf) & = & \langle 1 \rangle & \langle r \rangle & \langle f \rangle & \langle rf \rangle & \langle r^2 f \rangle & D_3 \\
\tau(r^2 f) & = & \langle 1 \rangle & \langle r \rangle & \langle f \rangle & \langle rf \rangle & \langle r^2 f \rangle & D_3
\end{array}
$$



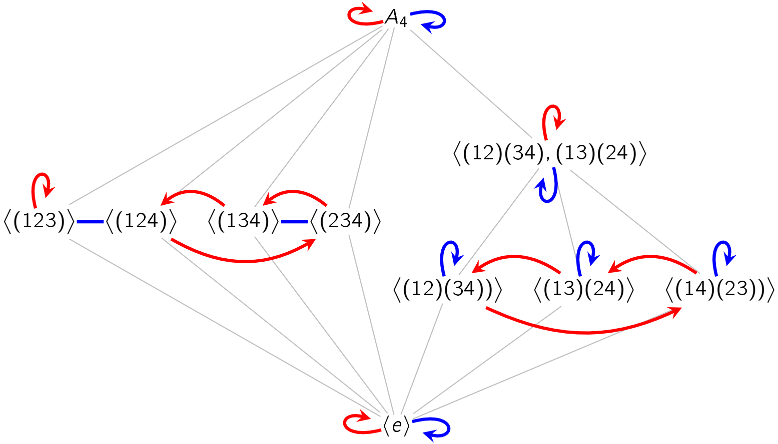
Observations

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

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

Groups acting on subgroups by conjugation

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



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

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

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 $|\operatorname{Orb}(\phi)| = 60/|A_4| = 5$ conjugacy classes.

A summary

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

More applications of group actions!

Here is where we did a fun example in class

In class we talked about SA_8 acting on itself by conjugation:

- we drew an action diagram,
- we drew boxes around each orbit,
- we looked at fixators,
- we looked at fixed points, which was $Z(SA_8) = \langle r^2 \rangle$,
- and we said that $|SA_8| = (4 \cdot 1) + 2 + 2 + 2 + 2 + 2 + 2$.

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:

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

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

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

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

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

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

Clearly, $(e, \ldots, e) \in P$ is a fixed point.

The $|G|^{p-1} - 1$ other elements in P sit in orbits of size 1 or p.

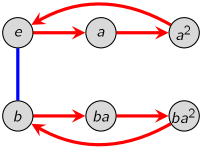
Since $p \nmid |G|^{p-1} - 1$, there must be other orbits of size 1. Thus, some $(x, \ldots, x) \in P$, with $x \neq e$ satisfies $x^p = e$. $\square$

Classification of groups of order 6

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

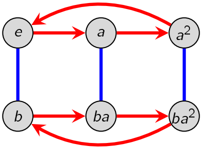
- an element a of order 3
- an element b of order 2.

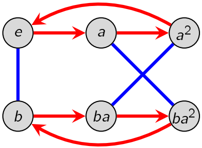
Clearly, $G = \langle a, b \rangle$, and so G must have the following "partial Cayley graph":



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

Exercise. Suppose that $|G| = pq$, where $p < q$ are primes and p doesn't divide $q - 1$. Prove that G is cyclic.