

Group Actions
Math 100A UCSD Fall 2001

Cayley's theorem says every finite group G can be embedded into a symmetric group. The proof of this theorem involved a clever idea, namely associating to each g in G the left multiplication function $\ell_g: G \rightarrow G$, where $\ell_g(x) = gx$. Each ℓ_g is a permutation of G , with inverse $\ell_{g^{-1}}$, and associating g to ℓ_g converts *elements* of G into *permutations* of G . The set $\text{Perm}(G)$ of all permutations of G is a group (under composition). Since $\ell_{g_1} \circ \ell_{g_2} = \ell_{g_1 g_2}$ (that is, $g_1(g_2 x) = (g_1 g_2)x$ for all $x \in G$), associating g to ℓ_g gives a group homomorphism

$$G \rightarrow \text{Perm}(G),$$

which is one-to-one (ℓ_g determines g since $\ell_g(e) = g$) and thus gives the sought after embedding of G into a symmetric group (when $\#G = m$, we have $\text{Perm}(G) \cong S_m$).

This homomorphism from G to $\text{Perm}(G)$ lets us view any group as a group of permutations of itself. Allowing an abstract group to be a group of permutations in other ways is a powerful tool in analyzing the group, and Cayley's theorem was simply the first example of the use of this idea. We now discuss this idea, called a group action, more generally.

An *action* of a group G on a set X is, by definition, a homomorphism from G to the group of permutations of X ,

$$G \rightarrow \text{Perm}(X).$$

There are three basic ways we will make a group G act: left multiplication on G , conjugation on G , and left multiplication on a coset space G/H . All of these will now be described in detail.

Example 1. G acts on G by left multiplication. Send G to $\text{Perm}(G)$ by associating with g the function ℓ_g , where $\ell_g(x) = gx$. This example was used already in the proof of Cayley's theorem, and we have already seen that $\ell_{g_1} \circ \ell_{g_2} = \ell_{g_1 g_2}$.

Example 2. G acts on G by conjugation. Send G to $\text{Perm}(G)$ by associating with g the function 'conjugation by g ,' denoted γ_g , where

$$\gamma_g(x) = gxg^{-1}$$

for $x \in G$. This is a permutation of G , with inverse $\gamma_{g^{-1}}$. Note for any $x \in G$ that

$$\begin{aligned}(\gamma_{g_1} \circ \gamma_{g_2})(x) &= \gamma_{g_1}(\gamma_{g_2}(x)) \\ &= g_1(g_2 x g_2^{-1}) g_1^{-1} \\ &= (g_1 g_2)x(g_1 g_2)^{-1} \\ &= \gamma_{g_1 g_2}(x),\end{aligned}$$

so $\gamma_{g_1} \circ \gamma_{g_2} = \gamma_{g_1 g_2}$.

While the left multiplication action of G on itself (Example 1) associates different group elements with different permutations, the conjugation action often makes two group elements act identically. That is, different elements of G may conjugate in the same way. To take an extreme example, when G is abelian all conjugations are the identity function ($gxg^{-1} = x$ for all x). Stating this in the language of homomorphisms, we allow a group action $G \rightarrow \text{Perm}(X)$ not to be injective.

Example 3. For a subgroup $H \subset G$, let G act on the left coset space $G/H = \{aH : a \in G\}$ by left multiplication. (We do *not* care whether or not $H \triangleleft G$, as we are just thinking about G/H as a set.) Send G to $\text{Perm}(G/H)$ by associating each $g \in G$ with the function $\ell_g : G/H \rightarrow G/H$ given by

$$\ell_g(aH) = gaH.$$

For example, take $G = D_4$ and $H = \{I, F\}$. Below is a table illustrating how left multiplication by F , R , and FR permute the left cosets in $G/H = \{H, RH, R^2H, R^3H\}$. For example, ℓ_F is a transposition of RH and R^3H . (Or, as one says, F acts like a transposition.) That $\ell_F \circ \ell_R = \ell_{FR}$ can be seen explicitly, for instance $(\ell_F \circ \ell_R)(R^2H) = \ell_F(R^3H) = FR^3H = \ell_{FR}(R^2H)$.

x	H	RH	R^2H	R^3H
$\ell_F(x)$	H	R^3H	R^2H	RH
$\ell_R(x)$	RH	R^2H	R^3H	H
$\ell_{FR}(x)$	R^3H	R^2H	RH	H

Returning to the general case,

$$\begin{aligned} (\ell_{g_1} \circ \ell_{g_2})(aH) &= \ell_{g_1}(\ell_{g_2}(aH)) \\ &= g_1(g_2aH) \\ &= g_1g_2aH \\ &= \ell_{g_1g_2}(aH), \end{aligned}$$

so left multiplication on cosets does define an action of G on G/H . The inverse of ℓ_g is $\ell_{g^{-1}}$. (That the notation ℓ_g used here matches that of our first example should not cause confusion, as long as you keep in mind whether G is acting by left multiplication on elements or on cosets. In fact, the first example is just a special case of this current example when the subgroup H is trivial.)

To prove theorems about group actions, we need to agree on a notation to express an arbitrary permutation arising from a group action. While the permutations in our examples have been written as ℓ_g or γ_g , when we discuss an arbitrary group action of G on a set X , we will denote the permutation of X corresponding to g as π_g . (In mathematics, π is used as a notation for many things besides 3.14159...; here it denotes a permutation.) The condition that $\pi : G \rightarrow \text{Perm}(X)$ is a homomorphism means

$$\pi_{g_1} \circ \pi_{g_2} = \pi_{g_1g_2}.$$

Equivalently, for every $x \in X$ we must have

$$\pi_{g_1}(\pi_{g_2}(x)) = \pi_{g_1 g_2}(x),$$

and we have already seen how such an identity is verified in our basic examples.

Keep in mind that when a group G acts on a set X , the set X is often not a group. But $\text{Perm}(X)$ is a group, and the action is a homomorphism from the group G to the group $\text{Perm}(X)$.

To get used to this notation, the fact that a homomorphism of groups sends the identity to the identity and sends inverses to inverses means π_e is the identity permutation of X (the permutation which fixes all points) and $\pi_g^{-1} = \pi_{g^{-1}}$ for any g . Of course, you can verify these in the concrete examples we know (e.g., $\ell_g^{-1} = \ell_{g^{-1}}$).

Every action has three important aspects: its orbits, its stabilizers, and its fixed points.

For each $x \in X$, its *orbit* is

$$\mathcal{O}_x = \{\pi_g(x) : g \in G\} \subset X$$

and its *stabilizer* is

$$\text{Stab}_x = \{g \in G : \pi_g(x) = x\} \subset G.$$

We call x a *fixed point* for the action when $\pi_g(x) = x$ for all $g \in G$, that is, when $\mathcal{O}_x = \{x\}$ (or equivalently, when $\text{Stab}_x = G$).

Writing the definition of orbits and stabilizers in words, the orbit of a point is a *geometric* concept: it is the set of all points which x can be moved to by the group action. On the other hand, the stabilizer of a point is an *algebraic* concept: it is the set of group elements which fix the point.

To suggest a mental picture, we will often refer to the elements of X as *points* (if $X = G$, then we think about elements of G as permutations when they act on G and as points when they are acted upon) and we will refer to the size of an orbit as its *length*.

Notational Remark: When trying to think about a set as a geometric object, it is helpful to refer to its elements as ‘points,’ no matter what they might really be. For example, when we think about G/H as a set on which G acts (by left multiplication), it is useful to think about the cosets of H , which are the elements of G/H , as the ‘points’ in G/H . At the same time, though, a coset is a subset of G . There is a tension between these two interpretations: is a left coset of H a point in G/H or a subset of G ? It is both, and it is important to be able to think about a coset in both ways. To get around this largely psychological problem, we will adopt the following notational convention sometimes when using the action of G on G/H : we write a coset aH as $\{aH\}$ if we want to indicate we are viewing aH as a

‘point’ in G/H . When the coset is considered to be a subset of G , we avoid the braces and just write aH .

All of our applications of group actions to group theory will flow from the relations between orbits, stabilizers, and fixed points, which we now illustrate in our three basic examples of group actions.

Example 1. When G acts on itself by left multiplication,

- there is one orbit ($g = \ell_g(e) \in \mathcal{O}_e$),
- $\text{Stab}_x = \{g : gx = x\} = \{e\}$ is trivial,
- there are no fixed points (if $\#G > 1$).

Example 2. When G acts on itself by conjugation,

- the orbit of a is $\mathcal{O}_a = \{gag^{-1} : g \in G\}$, which is the conjugacy class of a .
- $\text{Stab}_a = \{g : gag^{-1} = a\} = \{g : ga = ag\}$ is the centralizer of a .
- a is a fixed point when it commutes with all elements of G , and thus the fixed points of conjugation form the center of G .

Example 3. When G acts on G/H by left multiplication,

- there is one orbit ($\{gH\} = \ell_g(\{H\}) \in \mathcal{O}_{\{H\}}$),
- $\text{Stab}_{\{H\}} = \{g : gH = H\} = H$,
- $\text{Stab}_{\{aH\}} = \{g : gaH = aH\} = \{g : a^{-1}ga \in H\} = aHa^{-1}$,
- there are no fixed points (if $H \neq G$).

These examples illustrate several facts: an action need not have any fixed points (Example 1 with nontrivial G), different orbits can have different lengths (Example 2 with $G = S_3$), and the points in a common orbit don’t have to share the same stabilizer (Example 3, if H is a non-normal subgroup).

Theorem 1. *Let G act on X , with each g in G corresponding to the permutation π_g of X .*

a) *Different orbits are disjoint.*

b) *For each x , Stab_x is a subgroup of G and $\text{Stab}_{\pi_g(x)} = g \text{Stab}_x g^{-1}$.*

c) *$\pi_g(x) = \pi_{g'}(x)$ if and only if g and g' lie in the same left coset of Stab_x .*

In particular, we have

$$\#\mathcal{O}_x = [G : \text{Stab}_x].$$

The last equation, relating the length of an orbit to the size of a stabilizer for a point in the orbit, is called the *orbit-stabilizer formula*. As an example, when S_3 acts on itself by conjugation, the orbit of (12) is its conjugacy class $\{(12), (13), (23)\}$ and the stabilizer of (12) is its centralizer $\{(1), (12)\}$. Note $\#[(12)] = [S_3 : \{(1), (12)\}]$.

Proof. a) Just as in the proof that different cosets of a subgroup are disjoint, the way we prove different orbits are disjoint is to prove that two orbits which

overlap must coincide. Suppose \mathcal{O}_x and \mathcal{O}_y have a common element z :

$$z = \pi_{g_1}(x), \quad z = \pi_{g_2}(y).$$

We want to show $\mathcal{O}_x = \mathcal{O}_y$. It suffices to show $\mathcal{O}_x \subset \mathcal{O}_y$. (Then switch the roles of x and y to get the reverse inclusion.)

For any point $u \in \mathcal{O}_x$, write $u = \pi_g(x)$ for some $g \in G$. Since $x = \pi_g^{-1}(z)$,

$$u = \pi_g(\pi_g^{-1}(z)) = \pi_g(\pi_{g_1^{-1}}(z)) = \pi_{gg_1^{-1}}(z) = \pi_{gg_1^{-1}}(\pi_{g_2}(y)) = \pi_{gg_1^{-1}g_2}(y),$$

which shows us that $u \in \mathcal{O}_y$. Therefore $\mathcal{O}_x \subset \mathcal{O}_y$.

b) To see that Stab_x is a subgroup of G , we have $e \in \text{Stab}_x$ since π_e is the identity permutation. Moreover, if $g_1, g_2 \in \text{Stab}_x$ then

$$\pi_{g_1g_2}(x) = \pi_{g_1}(\pi_{g_2}(x)) = \pi_{g_1}(x) = x,$$

so $g_1g_2 \in \text{Stab}_x$. Thus Stab_x is closed under multiplication. Lastly,

$$\pi_g(x) = x \implies x = \pi_g^{-1}(x) = \pi_{g^{-1}}(x),$$

so Stab_x is closed under inversion.

The relation between the stabilizer at two points in an orbit is given by

$$\begin{aligned} h \in \text{Stab}_{\pi_g(x)} &\iff \pi_h(\pi_g(x)) = \pi_g(x) \\ &\iff \pi_{hg}(x) = \pi_g(x) \\ &\iff \pi_g^{-1}(\pi_{hg}(x)) = x \\ &\iff \pi_{g^{-1}}(\pi_{hg}(x)) = x \\ &\iff \pi_{g^{-1}hg}(x) = x \\ &\iff g^{-1}hg \in \text{Stab}_x \\ &\iff h \in g \text{Stab}_x g^{-1}, \end{aligned}$$

so $\text{Stab}_{\pi_g(x)} = g \text{Stab}_x g^{-1}$.

c) The condition $\pi_g(x) = \pi_{g'}(x)$ is equivalent to $x = \pi_g^{-1}(\pi_{g'}(x)) = \pi_{g^{-1}g'}(x)$, which means $g^{-1}g' \in \text{Stab}_x$, or $g' \in g \text{Stab}_x$. Therefore g and g' act in the same way on x if and only if g' and g lie in the same left coset of Stab_x (Remember that for any subgroup H , $g' \in gH$ if and only if $g'H = gH$.)

Since \mathcal{O}_x consists of the points $\pi_g(x)$ for varying g , and group elements act in the same way on x if and only if they lie in the same left coset of Stab_x , different points in \mathcal{O}_x correspond to different left cosets of Stab_x . Thus $\#\mathcal{O}_x$ is the number of left cosets of Stab_x in G , which is the index $[G : \text{Stab}_x]$. \square

The following two corollaries are reinterpretations of parts of Theorem 1, and the proofs are left to the reader.

Corollary 1. *Let G act on X , where G is finite.*

a) *The length of every orbit divides the size of G .*

b) *Points in a common orbit have conjugate stabilizers, and in particular the size of the stabilizer is the same for all points in an orbit.*

For example, the size of any conjugacy class in a group divides the size of the group, since conjugacy classes are orbits of the conjugation action.

Corollary 2. *Let G act on X , where G and X are finite. Let the different orbits of X be represented by x_1, \dots, x_t . Then*

$$\#X = \sum_{i=1}^t \#\mathcal{O}_{x_i} = \sum_{i=1}^t [G : \text{Stab}_{x_i}].$$

The action of a group of prime power size has special features. When $\#G = p^k$ for a prime p , we call G a p -group. For example, D_4 is a 2-group. Because all subgroups of a p -group have p -power index, the length of an orbit under an action by a p -group is a multiple of p unless the point is a fixed point, when its orbit has length 1. This leads to the following important congruence connecting the size of a set and the number of fixed points in it under the action by a p -group.

Theorem 2 (Fixed Point Congruence). *Let G be a finite p -group acting on a finite set X . Then*

$$\#X \equiv \#\{\text{fixed points}\} \pmod{p}.$$

Proof. Let the different orbits in X be represented by x_1, \dots, x_t , so Corollary 2 leads to

$$(1) \quad \#X = \sum_{i=1}^t \#\mathcal{O}_{x_i}.$$

Since $\#\mathcal{O}_{x_i} = [G : \text{Stab}_{x_i}]$ and $\#G$ is a power of p , $\#\mathcal{O}_{x_i} \equiv 0 \pmod{p}$ unless $\text{Stab}_{x_i} = G$, in which case \mathcal{O}_{x_i} has length 1, i.e., x_i is a fixed point. Thus when we reduce both sides of (1) modulo p , all terms on the right side vanish except for a contribution of 1 for each fixed point. That implies

$$\#X \equiv \#\{\text{fixed points}\} \pmod{p}.$$

□

Keep in mind that the congruence in Theorem 2 holds only for actions by groups with p -power size. When a group of size 6 acts, we don't get a congruence mod 2 or mod 3. But when a group of size 9 acts, then we get a congruence mod 3.

Corollary 3. *Let G be a finite p -group acting on a finite set X . If $\#X$ is not divisible by p , then there is at least one fixed point in X . If $\#X$ is divisible by p , then the number of fixed points is a multiple of p .*

In the second case, the number of fixed points might be 0. If we happen to know that there is at least one fixed point, then in the second case we know there are at least p fixed points.

Proof. When $\#X$ is not divisible by p , neither is the number of fixed points (by the fixed point congruence), so the number of fixed points can't equal 0 (after all, $p|0$) and thus is ≥ 1 . On the other hand, when $\#X$ is divisible by p , then the fixed point congruence shows the number of fixed points is $\equiv 0 \pmod p$, so this number is a multiple of p . \square

So you don't finish this handout without seeing how the fixed point congruence leads to results in pure group theory, we prove one result about p -groups with the aid of this congruence.

Theorem 3. *Let $\#G = p^k > 1$. Then G has a nontrivial center. That is, there is at least one nonidentity element of G which commutes with every element of G .*

Proof. The condition that a commutes with every element of G can be written as $a = gag^{-1}$ for all g , so a is fixed by all conjugations. The main idea of the proof is therefore to consider the action of G on itself by conjugation and count the fixed points.

We denote the center, as usual, by $Z(G)$. Since G is a p -group, the fixed point congruence implies

$$\#X \equiv \#Z(G) \pmod p.$$

In this case $X = G$ (conjugation is an action of G on itself), and since $\#G$ is a power of p this congruence implies

$$0 \equiv \#Z(G) \pmod p,$$

so $\#Z(G)$ is divisible by p . We know $Z(G)$ is a subgroup of G , containing at least the identity. Since we've shown p divides $\#Z(G)$, $Z(G)$ contains at least p elements, so in particular $Z(G) \neq \{e\}$. \square

Of course, in any concrete p -group you can check that the center is nontrivial: the center of D_4 is $\{I, R^2\}$, the center of $\mathbf{Z}/p^5\mathbf{Z}$ is $\mathbf{Z}/p^5\mathbf{Z}$, and the center of the Heisenberg group over $\mathbf{Z}/p\mathbf{Z}$ is the matrices of the form

$$\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where $b \in \mathbf{Z}/p\mathbf{Z}$. However, to prove that the center of an arbitrary p -group is nontrivial, some kind of uniform argument is needed which applies to all p -groups, and the proof we gave in Theorem 3, using group actions, is such an argument.

We conclude this handout with an application of left multiplication on cosets. In the handout on the index of a subgroup, the following two results were proved (by different methods):

- If H is a subgroup with $[G : H] = 2$, then $H \triangleleft G$.
- If $\#G = p^k$ and $[G : H] = p$, then $H \triangleleft G$.

Now we prove a result which includes both of these as special cases.

Theorem 4. *Let G be a finite group with $\#G > 1$, and p be the smallest prime factor of G . Any subgroup of G with index p is a normal subgroup.*

Check for yourself that Theorem 4 covers both of the results above. While group actions don't play a role in the statement of Theorem 4, they will play a role in its proof.

Proof. Let H be a subgroup of G with index p , so G/H is a set with size p . We will prove $H \triangleleft G$ by showing H is the kernel of a homomorphism. (We know kernels are always normal subgroups.)

Let G act on G/H by left multiplication, which gives an action

$$G \rightarrow \text{Perm}(G/H) \cong S_p,$$

that sends each g in G to the permutation ℓ_g of G/H .

We look at the kernel K of this action. To say $g \in K$ means ℓ_g is the identity permutation, or g fixes all the left cosets: $g(aH) = aH$ for all cosets aH . One of the cosets is H itself, and if $g \notin H$, then $gH \neq H$, so g doesn't fix all the cosets and thus $g \notin K$. Therefore $K \subset H$.

By the fundamental homomorphism theorem, G/K is isomorphic to a subgroup of S_p , so $\#(G/K) \mid p!$ by Lagrange. Since $[G : H] = p$ and $K \subset H \subset G$, we write

$$\#(G/K) = [G : K] = [G : H][H : K] = p[H : K],$$

so the relation $\#(G/K) \mid p!$ simplifies to

$$[H : K] \mid (p-1)!.$$

Since $[H : K]$ is a factor of $\#G$, its smallest prime factor is p . But this index divides $(p-1)!$, so therefore it doesn't have any prime factors. That means $[H : K] = 1$, or $H = K$. In particular, H is the kernel of a homomorphism, so H is a normal subgroup. \square