Group Actions

Math 415B/515B

The notion of a group acting on a set is one which links abstract algebra to nearly every branch of mathematics. Group actions appear in geometry, linear algebra, and differential equations, to name a few. For this reason we will study them for a bit while taking a break from ring theory. Some of this material is covered in Chapter 7 of Gallian's book, but we will take a slightly more general approach. The applications to conjugacy classes of finite groups appear in Chapter 25 of Gallian, and Chapter 29 of Gallian has applications of group actions to geometry and symmetry.

Let G be a group and let X be a set. Let $\mathrm{Sym}(X)$ denote the group of all permutations of the elements of X. So, if X is a finite set and $|X| = n$, then $\mathrm{Sym}(X) \cong S_n$. We will give two equivalent definitions of G acting on X.

Definition 1. We say that G *acts on* X if there is a homomorphism $\phi : G \to \mathrm{Sym}(X)$.

One way of thinking of G acting on X is that elements of the group G may be "applied to" elements of X to give a new element of X. The next definition takes this point of view.

Definition 2. We say that G *acts on* X if there is a map

$$\cdot : G \times X \to X,$$

so that if $g \in G$ and $x \in X$, then $g \cdot x \in X$, such that:
(i) For every $g, h \in G$, $x \in X$, we have $(gh) \cdot x = g \cdot (h \cdot x)$,
(ii) For every $x \in X$, $e \cdot x = x$, where $e \in G$ is the identity.

Before giving examples, we need to show that the two above definitions actually define the same notion.

Theorem 1 *Definition 1 and Definition 2 are equivalent.*

Proof. First assume that G and X satisfy Definition 1, so that we have a homomorphism $\phi : G \to \mathrm{Sym}(X)$. We now show that G and X must also then satisfy Definition 2. We define a map $\cdot : G \times X \to X$ by $g \cdot x = \phi(g)(x)$. First, for every $g, h \in G$, $x \in X$, using the fact that ϕ is a homomorphism, we have

$$(gh) \cdot x = \phi(gh)(x) = (\phi(g) \circ \phi(h))(x) = \phi(g)(\phi(h)(x)) = g \cdot (h \cdot x),$$

so that $\cdot$ satisfies condition (i) of Definition 2. Also, since ϕ is a homomorphism, $\phi(e)$ is the trivial permutation, where $e \in G$ is the identity element. So $e \cdot x = \phi(e)(x) = x$, which is condition (ii) of Definition 2. Thus G and X satisfy Definition 2.

Now suppose G and X satisfy Definition 2, so that we have a map

$$\cdot : G \times X \to X$$

which satisfies (i) and (ii). We define a map $\phi : G \to \mathrm{Sym}(X)$ by $\phi(g)(x) = g \cdot x$. We first show that this is well-defined, that is, $\phi(g)$ is actually a one-to-one and onto map from X to itself. To show that $\phi(g)$ is onto, let $x \in X$, and consider $g^{-1} \cdot x \in X$. Then we have

$$\phi(g)(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e \cdot x = x,$$

so $\phi(g)$ is onto. To show that $\phi(g)$ is one-to-one, suppose that we have $\phi(g)(x) = \phi(g)(y)$ for $x, y \in X$, so that $g \cdot x = g \cdot y$. Using both conditions (i) and (ii) of Definition 2, we have

$$g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) \Rightarrow (g^{-1}g) \cdot x = (g^{-1}g) \cdot y \Rightarrow e \cdot x = e \cdot y \Rightarrow x = y.$$

Finally, we show that ϕ is a homomorphism. Let $g, h \in G$, $x \in X$. We have

$$\phi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))(x).$$

Thus, G and X satisfy Definition 1. □

Now that we have a few ways of thinking about group actions, let's see some examples.

Example 1. As mentioned before, we may take $X = \{1, 2, \ldots, n\}$, $G = S_n = \mathrm{Sym}(X)$, and $\phi : S_n \to S_n$ to be the identity map.

Example 2. Let $X = \mathbb{R}^n$ and $G = \mathrm{GL}(n, \mathbb{R})$, and for $A \in G$, $v \in X$, define $A \cdot v = Av$. That is, we let G act on X as linear transformations.

Example 3. Let X be a unit cube sitting in $\mathbb{R}^3$, and let G be the group of symmetries of X, which acts on X again as linear transformations on $\mathbb{R}^3$.

Example 4. Let X be a group H, and let G also be the same group H, where H acts on itself by left multiplication. That is, for $h \in X = H$ and $g \in G = H$, define $g \cdot h = gh$. This action was used to show that every group is isomorphic to a group of permutations (Cayley's Theorem, in Chapter 6 of Gallian's book).

Before defining more terms, we'll first see a nice application to finite group theory.

Theorem 2 *Let G be a finite group, and let H be a subgroup of G such that $[G : H] = p$, where p is the smallest prime dividing $|G|$. Then H is a normal subgroup of G.*

Proof. We let X be the set of left cosets of H in G. From a Corollary of Lagrange's Theorem, we have $|X| = [G : H] = p$, and so $\mathrm{Sym}(X) \cong S_p$. We define an action of G on X by $g \cdot aH = gaH$, for $g \in G$ and $aH \in X$. That is, we let G act on the left cosets of H in G by left multiplication. To check that this satisfies Definition 2 is immediate, since for any $g_1, g_2, a \in G$, we have $(g_1 g_2) \cdot aH = g_1 g_2 aH$ and $e \cdot aH = aH$. From Theorem 1, and since $\mathrm{Sym}(X) \cong S_p$, we have a homomorphism $\phi : G \to S_p$.

For any $g \in G, g \notin H$, we have $g \cdot H = gH \neq H$, and so $\phi(g)$ cannot be the trivial permutation of left cosets of H in G, that is, $g \notin \ker(\phi)$ when $g \notin H$. We must therefore have $\ker(\phi) \leq H$. From the first isomorphism theorem for groups, we have $G/\ker(\phi) \cong \mathrm{im}(\phi)$, where $\mathrm{im}(\phi)$ is a subgroup of S_p. So we have

$$\frac{|G|}{|\ker(\phi)|} = |G/\ker(\phi)| \Big| |S_p| = p!.$$

Note that p is the largest prime dividing $p!$, while p is the smallest prime dividing $|G|$. Since $\ker(\phi) \leq H$ and H is a proper subgroup of G, we cannot

have $G = \ker(\phi)$, that is, $[G : \ker(\phi)] \neq 1$. The only possibility is that $|G/\ker(\phi)| = [G : \ker(\phi)] = p$, since this is the only divisor of $|G|$ which divides $p!$. We now have

$$[G : \ker(\phi)] = \frac{|G|}{|\ker(\phi)|} = p = [G : H] = \frac{|G|}{|H|},$$

so that $|H| = |\ker(\phi)|$. Since $\ker(\phi) \subseteq H$, we must have $H = \ker(\phi)$, which is a normal subgroup of G. $\square$

We now define a few important terms relevant to group actions.

Definition 3. Let G be a group which acts on the set X. For $x \in X$, the *stabilizer of x in G*, written $\text{stab}_G(x)$, is the set of elements $g \in G$ such that $g \cdot x = x$. In symbols,

$$\text{stab}_G(x) = \{g \in G \mid g \cdot x = x\}.$$

For $x \in X$, the *orbit of x under G*, written $\text{orb}_G(x)$, is the set of all elements in X of the form $g \cdot x$ for $g \in G$. In symbols,

$$\text{orb}_G(x) = \{g \cdot x \mid g \in G\}.$$

Example 5. Let $G = \{(1), (1\ 2), (3\ 4\ 6), (3\ 6\ 4), (1\ 2)(3\ 4\ 6), (1\ 2)(3\ 6\ 4)\}$, and let $\phi : G \to S_6$, $\phi(\alpha) = \alpha$, be the natural injection, as G is a subgroup of S_6. Then G acts on $\{1, 2, 3, 4, 5, 6\}$. First note that since 5 is fixed by every element of G, we have $\text{stab}_G(5) = G$, and $\text{orb}_G(5) = \{5\}$. We also have

$$\text{stab}_G(3) = \text{stab}_G(4) = \text{stab}_G(6) = \langle(1\ 2)\rangle, \quad \text{stab}_G(1) = \text{stab}_G(2) = \langle(3\ 4\ 6)\rangle,$$

$$\text{orb}_G(3) = \text{orb}_G(4) = \text{orb}_G(6) = \{3, 4, 6\}, \quad \text{orb}_G(1) = \text{orb}_G(2) = \{1, 2\}.$$

Example 6. Let G be any group, and we let G act on itself by conjugation. That is, for $g, a \in G$, we define $g \cdot a = gag^{-1}$. We first check that this satisfies Definition 2. First, we have $e \cdot a = eae^{-1} = a$. Now let $g, h, a \in G$. Then we have

$$(gh) \cdot a = gha(gh)^{-1} = ghah^{-1}g^{-1} = g \cdot (h \cdot a),$$

so this is indeed a group action. If we fix an $a \in G$, we see that the orbit of a is

$$\text{orb}_G(a) = \{gag^{-1} \mid g \in G\},$$

which we've seen before defined as the conjugacy class of a in G. If we look at the stabilizer of a in G, we have

$$\text{stab}_G(a) = \{g \in G \mid gag^{-1} = a\},$$

which we've also seen before defined as the centralizer of a in G, also written $C_G(a)$. We've shown that the centralizers of elements in G are subgroups of G, and the next Lemma shows us that stabilizers of group actions are always subgroups.

Lemma 1 *If G acts on X, and $x \in X$, then $\text{stab}_G(x)$ is a subgroup of G.*

Proof. Let $x \in X$. Since $e \cdot x = x$, we know that $e \in \text{stab}_G(x)$, and so the stabilizer of x in G is nonempty. Now suppose $g, h \in \text{stab}_G(x)$. Since $g \cdot x = x$, we have

$$g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x \Rightarrow (g^{-1}g) \cdot x = g^{-1} \cdot x \Rightarrow e \cdot x = g^{-1} \cdot x \Rightarrow g^{-1} \cdot x = x.$$

So, $g^{-1} \in \text{stab}_G(x)$. We also have

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x,$$

so $gh \in \text{stab}_G(x)$. Thus $\text{stab}_G(x) \leq G$. $\square$

The next result is the most important basic result in the theory of group actions.

Theorem 3 (Orbit-Stabilizer Lemma) *Suppose G is a finite group which acts on X. For any $x \in X$, we have*

$$|G| = |\text{stab}_G(x)| \, |\text{orb}_G(x)|.$$

Proof. Fix $x \in X$. From Lemma 1, $\text{stab}_G(x)$ is a subgroup of G, and it follows from Lagrange's Theorem that the number of left cosets of $H = \text{stab}_G(x)$ in G is $[G : H] = |G|/|H|$. Let $\mathcal{K}$ denote the set of left cosets of H in G. Define a function

$$f : \text{orb}_G(x) \to \mathcal{K},$$

by $f(g \cdot x) = gH$. First, we check that f is well-defined, and at the same time check that f is injective. If $g_1, g_2 \in G$, $g_1 \cdot x = g_2 \cdot x \in \text{orb}_G(x)$ if and only if $(g_2^{-1}g_1) \cdot x = x$, iff $g_2^{-1}g_1 \in \text{stab}_G(x) = H$, which is equivalent to $g_2H = g_1H$.

So $g_1 \cdot x = g_2 \cdot x$ if and only if $f(g_1 \cdot x) = f(g_2 \cdot x)$, and f is well-defined and injective. It is immediate that f is onto, since for any $gH \in \mathcal{K}$, $f(g \cdot x) = gH$.

Now, f gives a one-to-one correspondence between elements of $\text{orb}_G(x)$ and the left cosets of $\text{stab}_G(x)$ in G. Thus, these are equal in number, and we have

$$|\text{orb}_G(x)| = |\mathcal{K}| = \frac{|G|}{|\text{stab}_G(x)|},$$

which gives the desired result. □

There are several examples of the Orbit-Stabilizer Lemma applied to groups of symmetries of geometric objects given in Chapter 7 of Gallian, which you should read. The following application comes from Example 6 above, and appears in Chapter 25 of Gallian.

Theorem 4 (Class Formula) *Let G be a finite group, let $Z(G)$ be the center of G, and let A be a collection of distinct representatives of conjugacy classes of G which are not in $Z(G)$. Then we have*

$$|G| = |Z(G)| + \sum_{a \in A} [G : C_G(a)].$$

Proof. For any $x \in G$, let $\text{cl}(x)$ denote the conjugacy class of x in G. From Example 6 above, we let G act on itself by conjugation, and for any $x \in G$, we have $\text{orb}_G(x) = \text{cl}(x)$, and $\text{stab}_G(x) = C_G(a)$. From Theorem 3, we have, for each $x \in G$,

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

We showed in Math 415A that the relation of elements being conjugate in G is an equivalence relation, and so conjugacy classes form a partition of G. So, the union of distinct conjugacy classes of G gives G. Let B be a set of representatives of distinct conjugacy classes of G, and we have

$$|G| = \sum_{b \in B} |\text{cl}(b)| = \sum_{b \in B} [G : C_G(b)]. \tag{1}$$

We also know that $b \in Z(G)$ exactly when $gbg^{-1} = b$ for every $g \in G$, which happens exactly when $|\text{cl}(b)| = 1$. So, $\sum_{z \in Z(G)} |\text{cl}(z)| = |Z(G)|$. If we choose A to be a set of representatives of conjugacy classes which are not in $Z(G)$, splitting (1) into a sum over $Z(G)$ and a sum over A gives the result. □

PROBLEMS:

1. Let p be prime, let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and let G be the following subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$:

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p \right\}.$$

Let $X = \mathbb{F}_p^2$ be the set of 2×1 vectors with entries from $\mathbb{F}_p$, that is,

$$\mathbb{F}_p^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid x, y \in \mathbb{F}_p \right\}.$$

(a): For $g \in G$ and $v \in X$, define $g \cdot v = gv$, where gv is matrix-vector multiplication. Show that this satisfies Definition 2 of a group action.
(b): Show that for every $v \in X$, we have $|\mathrm{orb}_G(v)| = 1$ or p.
(c): If $v = \begin{pmatrix} x \\ y \end{pmatrix}$, show that $\mathrm{stab}_G(v) = G$ if and only if $y = 0$.

2. Let G be a group which acts on a set X, and for $x, y \in X$, define $x \sim y$ if there is a $g \in G$ such that $g \cdot x = y$. Prove that $\sim$ is an equivalence relation on X, and the equivalence class of $x \in X$ is $\mathrm{orb}_G(x)$.

3. Let G be a finite group such that $|G| = p^k$, for some prime p and integer $k \geq 1$. Use Theorem 4 to show that the center of G is nontrivial, that is, that $Z(G)$ contains more than just the identity element e.

4. Use Problem 3 above and Theorem 9.3 in Gallian to show that any group of order p^2, where p is prime, is abelian.