Group Actions

Math 430 - Spring 2011

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. Group actions are a fundamental tool in pure group theory as well, and one of our main applications will be the Sylow Theorems (Sections 36 and 37 in Fraleigh). These notes should be used as a supplement to Section 16 of Fraleigh's book. Some of the notation here will differ from the notation in Fraleigh, but we will attempt to point out whenever this happens.

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 (written as S_X in Fraleigh). 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

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

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

If the group G acts on the set X, we will call X a *G-set.* Note that Fraleigh often writes gx for $g * x$, where $g \in G$ and $x \in X$.

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

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

so that $*$ 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 $e * x = \phi(e)(x) = x$, 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

$$* : G \times X \to X$$

which satisfies (i) and (ii). We define a map $\phi : G \to \text{Sym}(X)$ by $\phi(g)(x) = g * x$. 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 $g^{-1} * x \in X$. Then we have

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

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 $g * x = g * y$. Using both conditions (i) and (ii) of Definition 2, we have

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

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

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

Thus, G and X satisfy Definition 1. $\square$

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 $A * v = Av$. 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 $g * h = gh$. This action was used to show that every group is isomorphic to a group of permutations (Cayley's Theorem, in Section 8 of Fraleigh).

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 the proof of Lagrange's Theorem (Section 10 of Fraleigh), we have $|X| = [G : H] = p$, and so $\mathrm{Sym}(X) \cong S_p$. We define an action of G on X by $g * aH = gaH$, 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. This satisfies Definition 2, since for any $g_1, g_2, a \in G$, we have $(g_1 g_2) * aH = g_1 g_2 aH$ and $e * aH = aH$. 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 $g * H = gH \neq H$, 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 $\mathrm{im}(\phi) = \phi(G)$ 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 $p!$, and p^2 does not divide $p!$, 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 $\mathrm{stab}_G(x)$, is the set of elements $g \in G$ such that $g * x = x$. In symbols,

$$\mathrm{stab}_G(x) = \{g \in G \mid g * x = x\}.$$

In Fraleigh, this is called the *isotropy subgroup of x*, and is written G_x (we show below that this is actually a subgroup of G).

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

$$\mathrm{orb}_G(x) = \{g * x \mid g \in G\}.$$

Fraleigh uses the notation Gx for the orbit of x under 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 $\mathrm{stab}_G(5) = G$, and $\mathrm{orb}_G(5) = \{5\}$. We also have

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

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

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 $g * a = gag^{-1}$. We first check that this satisfies

Definition 2. First, we have $e * a = eae^{-1} = a$. Now let $g, h, a \in G$. Then we have

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

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 is called 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 is the *centralizer of a in G*, also written $C_G(a)$. The next Lemma shows us that stabilizers of group actions are always subgroups, and so in particular, centralizers of elements of groups are 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 $e * x = x$, 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 $g * x = x$, we have

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

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

$$(gh) * x = g * (h * x) = g * x = x,$$

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 group which acts on X. For any $x \in X$, we have*

$$|\text{orb}_G(x)| = [G : \text{stab}_G(x)],$$

which means that the cardinalities are equal even when these are infinite sets. If G is a finite group, then

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

Proof. Fix $x \in X$. From Lemma 1, $\text{stab}_G(x)$ is a subgroup of G, and we recall that$[G : H]$ denotes the cardinality of the set of left cosets of H in G. 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 $f(g*x) = gH$. First, we check that f is well-defined, and at the same time check that f is injective. If $g_1, g_2 \in G$, $g_1 * x = g_2 * x \in \text{orb}_G(x)$ if and only if $(g_2^{-1}g_1) * x = x$, iff $g_2^{-1}g_1 \in \text{stab}_G(x) = H$, which is equivalent to $g_2H = g_1H$. So $g_1 * x = g_2 * x$ if and only if $f(g_1 * x) = f(g_2 * x)$, and f is well-defined and injective. Also f is onto, since for any $gH \in \mathcal{K}$, $f(g * x) = gH$. Thus, f gives a one-to-one correspondence, and so

$$|\text{orb}_G(x)| = |\mathcal{K}| = [G : \text{stab}_G(x)].$$

When G is finite, it follows from the proof of Lagrange's Theorem that $[G : \text{stab}_G(x)] = |G|/|\text{stab}_G(x)|$ So, in this case, $|G| = |\text{stab}_G(x)|\ |\text{orb}_G(x)|$. $\square$

Next, we connect the concept of a group action with the important notion of an equivalence relation.

Theorem 4 *Let G be a group which acts on a set X, and for $x, y \in X$, define $x \sim y$ to mean that there is a $g \in G$ such that $g * x = y$. Then $\sim$ is an equivalence relation on X, and the equivalence class of $x \in X$ is* $\text{orb}_G(x)$.

Proof. We must check that $\sim$ satisfies the reflexive, symmetric, and transitive properties. First, for any $x \in X$, we have $e * x = x$, where e is the identity in G, and so $x \sim x$ and the reflective property holds. Next, if $x \sim y$, then there is a $g \in G$ such that $g * x = y$. It follows from Definition 2 that we then have $g^{-1} * y = x$, so that $y \sim x$ and the symmetric property holds. Now assume $x \sim y$ and $y \sim z$, where $g * x = y$ and $h * y = z$. Then from Definition 2, $h * (g * x) = (hg) * x = z$, and so $x \sim z$ and transitivity holds. So, $\sim$ is an equivalence relation.

From the definition of an equivalence class, if $x \in X$, then the class of x is the set $\{y \in X \mid x \sim y\} = \{y \in X \mid y = g * x \text{ for some } g \in G\}$. This is exactly the definition of the orbit of x under G. $\square$

We conclude with one more application to group theory, this time to the conjugacy classes of a group, as introduced in Example 6 above. Note that if G is a group and $z \in G$ is in the center of G, then the conjugacy class of z is just $\{z\}$.

Theorem 5 (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 $\mathrm{cl}(x)$ 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 $\mathrm{orb}_G(x) = \mathrm{cl}(x)$, and $\mathrm{stab}_G(x) = C_G(a)$. From Theorem 3, we have, for each $x \in G$,

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

Since from Theorem 4 the conjugacy classes of G are just equivalence classes, we have that 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

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

We also know that $b \in Z(G)$ exactly when $gbg^{-1} = b$ for every $g \in G$, which happens exactly when $|\mathrm{cl}(b)| = 1$. So, $\sum_{z \in Z(G)} |\mathrm{cl}(z)| = |Z(G)|$. 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. □