Group Actions (Represent!)

Some of our earliest examples of groups were from sets of functions $\{f : \mathbb{R} \to \mathbb{R}\}$ or $\{f : X \to X\}$ (given some set X). The identity element was the identity function $f(x) = x$ and the group law was composition of functions $fg = f \circ g$. For example, this is how we defined the symmetric groups.

However, focusing only on the group structure of functions neglects the important role played by the domain where functions act! In this section we'll finally look closely at how groups of functions interact with their domain.

If G is a group of functions $\{g : X \to X\}$, then we say the group G is **acting** on the set X; dually we say X is a ***G*-set** (or that X has a ***G*-action**). Rather than using the language of functions, the standard definition (below) expresses this relationship using the same format as group multiplication (hence μ).

Definition. An **action**[1] of a group G on a set X is a set map $\mu : G \times X \to X$ respecting group structure.

Written as a function.

- $\mu(e, x) = x$
- $\mu\big(g_1,\, \mu(g_2, x)\big) = \mu(g_1 g_2, x)$

Written multiplicatively.

- $e \cdot x = x$
- $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$

In this case we say X is a ***G*-set**,[2] and the map μ is a ***G*-action**. Instead of $\mu(g, x)$ or $g \cdot x$ we may just write gx. Our shorthand notation for "G acting on X" is $G \circlearrowright X$.

Remark. As suggested in the introduction, a G-action is equivalent to a compatible collection of set bijections $\{\phi_g : X \xrightarrow{\cong} X \mid g \in G\}$ by $\phi_g(x) = g \cdot x$.

Proposition. *A G-action $G \circlearrowright X$ is equivalent to a homomorphism $\Phi : G \to S_X$.*[3]

Proof. Given a G-action on X, define $\Phi(g) = \phi_g$ by $\phi_g(x) = g \cdot x$.

Each map ϕ_g is a bijection, since $\phi_g \circ \phi_{g^{-1}} = \phi_e$. Thus Φ maps to S_X, the set of bijections $X \to X$.

The map Φ is a homomorphism, because $\phi_{g_1} \circ \phi_{g_2} = \phi_{(g_1 g_2)}$.

In the other direction, given homomorphism $\Phi : G \to S_X$, define $g \cdot x = \Phi(g)(x)$. Then

$$g_1 \cdot (g_2 \cdot x) \;=\; \Phi(g_1)\big(\Phi(g_2)(x)\big) \;=\; \Phi(g_1) \circ \Phi(g_2)\,(x) \;=\; \Phi(g_1 g_2)(x) \;=\; (g_1 g_2) \cdot x.$$

Applying this with $g_1 = g_2^{-1}$ yields $e \cdot x = x$. $\square$

Example. The symmetric group S_n is defined by its action on $X = \{1, \ldots, n\}$.

S_n also acts on the set of subgroups of $\{1, \ldots, n\}$, i.e. the power set $X = \mathcal{P}\big(\{1, \ldots, n\}\big)$.

More interestingly, S_n acts on the set of subgroups of $\{1, \ldots, n\}$ of a specified size.

The action on subgroups of size 2 (pairs of numbers) is quite interesting and useful!

Example. The **trivial action** of G on X is given by $\mu(g, x) = x$.

Example. If $H < G$, then left multiplication defines a G-action on $X = \{H\text{-cosets}\}$.

We used this in our proof of the Lagrange Theorem.

Example. Two more important examples come from using $X = G$ itself.

- Left multiplication defines a G-action on the underlying set of G by $\mu(g, x) = gx$.
  This is called the **regular representation** of G.
- Conjugation defines a G-action on the underlying set of G by $\mu(g, x) = gxg^{-1}$.

[1] Some people may call this a **left** group action, since it is $G \times X \to X$ rather than $X \times G \to X$.

[2] In fancy generalizations this becomes a ***G*-module**.

[3] Such homomorphisms are called **representations** of G. These are the subject of much study!

Furthermore, if $H < G$ then the examples above give H-actions on G.

Example. Conjugation also defines a G-action on $X = \{\text{subgroups of } G\}$; because if H is a subgroup, then so is gHg^{-1}.

If a subgroup is normal, then $gHg^{-1} = H$ so the G-action will not change it. When something isn't changed or moved we say it is "fixed". We'll look into this in further detail below.

Cosets themselves generalize to a G-set version[4] called the orbit of an element.

Definition. If X is a G-set, then $x, y \in X$ are ***G*-equivalent**, $x \sim_G y$, if $y = g \cdot x$ for some $g \in G$.

Proposition. *This is an equivalence relation on X.*

Proof. Verify the equivalence relation axioms.

(Reflexive) $e \cdot x = x$ so $x \sim_G x$

(Symmetric) If $x \sim_G y$ then $y = g \cdot x$. Thus
$$g^{-1} \cdot y \;=\; g^{-1} g \cdot x \;=\; e \cdot x \;=\; x;$$
so $y \sim_G x$

(Transitive) If $x \sim_G y$ and $y \sim_G z$ then $y = g \cdot x$ and $z = g' \cdot y$. Thus
$$z \;=\; g' \cdot (g \cdot x) \;=\; (g'g) \cdot x;$$
so $x \sim_G z$. □

Definition. Given a G-set X, we define the following.[5]

- The **stabilizer** of an element $x \in X$ is $G_x = \{x \in X \mid g \cdot x = x\} \subset G$.
- The ***G*-orbit** of an element $x \in X$ is $Gx = [x] = \{y \in X \mid x \sim_G y\} \subset X$.

In later sections we will also want to use the following.

- The **fixed-points** of an element $g \in G$ is $X_g = \{x \in X \mid g \cdot x = x\} \subset X$.
- The **fixed-points** of the group is $X_G = \{x \in X \mid g \cdot x = x \text{ for all } g \in G\} \subset X$.

Example. The G-action on X is **free** if $g \cdot x = x$ only for $g = e$. In this case, all stabilizers and fixed points are trivial: $G_x = \{e\}$ and $X_g = \varnothing$ (for $g \neq e$). For example, the regular representation of a group is always free.

The G-action on X is **transitive** if every pair $x, y \in X$ has an element $g \in G$ so that $g \cdot x = y$. In this case, there is only one orbit; since $Gx = X$ for all $x \in X$. The regular representation is also transitive.

Proposition. *Stabilizers G_x are subgroups.*

Proof. Verify the subgroup axioms.

(Identity) $e \cdot x = x$ for all $x \in X$ so $e \in G_x$.

(Mult. Closed) If $g, h \in G_x$ then $g \cdot x = x$ and $h \cdot x = x$. Thus
$$(gh) \cdot x \;=\; g \cdot (h \cdot x) \;=\; g \cdot x \;=\; x;$$
so $gh \in G_x$.

[4] A "G-set version" of a statement is often called the "G-equivariant" version.

[5] In category theory and homotopical algebra, we use the opposite convention. Fixed points are superscripts X^g and orbits are subscripts X_g.

(Inv. Closed) If $g \in G_x$ then $g \cdot x = x$. Thus
$$x = e \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x;$$
so $g^{-1} \in G_x$. $\square$

The orbit of an element is where G can take it. The stabilizer subgroup of an element are the $g \in G$ that don't take it anywhere. These are clearly closely related. If two set elements are in the same orbit, then their stabilizers are conjugate.

Proposition. *If $y = g \cdot x$ then $G_y = gG_xg^{-1}$.*

Proof. Suppose $y = g \cdot x$.
($\supset$) If $h \in G_x$ then $h \cdot x = x$. So $ghg^{-1} \cdot y = ghg^{-1}g \cdot x = gh \cdot x = g \cdot x = y$.
($\subset$) If $k \in G_y$ then $k \cdot y = y$. So $g^{-1}kg \cdot x = g^{-1}k \cdot y = g^{-1} \cdot y = y$. Thus $g^{-1}G_yg \subset G_x$. $\square$

Corollary. *If $y = g \cdot x$ then $|G_y| = |G_x|$.*

In the other direction, if two group elements are in the same coset of a stabilizer, then they act on x in the same way.

Proposition. *Group elements a, b are in the same coset of G_x if and only if $a \cdot x = b \cdot x$.*

Proof. ($\Rightarrow$) If a, b are in the same coset of G_x then $a = bg$ where $g \in G_x$. In this case
$a \cdot x = (bg) \cdot x = b \cdot (g \cdot x) = b \cdot x$.
($\Leftarrow$) If $a \cdot x = b \cdot x$ then $b^{-1}a \cdot x = e \cdot x = x$; so $b^{-1}a \in G_x$. This implies $aG_x = bG_x$. $\square$

The Orbit-Stabilizer Theorem is the "G-set version" of the Lagrange Theorem. The stabilizer G_x doesn't move x anywhere; and group elements in the same coset of G_x move x to the same position in its orbit Gx. Thus the orbit of x gets one new element from each coset of its stabilizer. Note that **stabilizers are usually not normal**, so the quotient $G \diagup G_x$ is probably not defined; thus we must leave statements at the level of coset counts (index).

Theorem [Orbit-Stabilizer]. *If X is a G-set, with everything finite, then the size of an element's orbit equals the index of its stabilizer subgroup, $|Gx| = [G : G_x]$.*

Proof. Define a set map $f : Gx \to \{\text{cosets of } G_x\}$ as follows. Given $y \in Gx$, let $f(y) = [g]$ where $y = g \cdot x$. This is well-defined because if $g_1 \cdot x = y = g_2 \cdot x$, then $g_2^{-1}g_1 \cdot x = x$; so $g_2^{-1}g_1 \in G_x$. Thus $[g_1] = [g_2]$.
We show this is a bijection.

(Surjective) This clear by construction. The left coset $[g]$ is the value of $f(g \cdot x)$.

(Injective) If $f(y_1) = f(y_2)$ then $[g_1] = [g_2]$ where $y_1 = g_1 \cdot x$ and $y_2 = g_2 \cdot x$. By the previous proposition, if g_1, g_2 are in the same G_x coset, then $y_1 = g_1 \cdot x = g_2 \cdot x = y_2$. $\square$

The following corollary is the main application of this formula.

Corollary. $|G| = |Gx| \cdot |G_x|$

Proof. By Lagrange's Theorem, the index is $[G : G_x] = \dfrac{|G|}{|G_x|}$. $\square$

Example. The dihedral group D_4 is the symmetries of a square. It consists of four rotations and four reflections (vertical, horizontal, and two diagonal). This group naturally acts on the set of vertices of a square.

- The orbit of each vertex is the full set of four vertices.
- The stabilizer of each vertex has two elements: the identity and the diagonal reflection fixing the vertex.
- Note that $\left|D_4\right| = 8 = 4 \cdot 2 = \left|\text{Orbit}\right| \cdot \left|\text{Stabilizer}\right|$

Example. The symmetric group S_4 acts on the set of subsets of $\{1, 2, 3, 4\}$.

- The orbit of a subset will be all subsets of the same size.
  For example the orbit of $\{1, 2\}$ is all 6 subsets of size 2.
- The stabilizer of an element will be all permutations which restrict to the subset.
  For example, the stabilizer of $\{1, 2\}$ is $\big\{e,\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4)\big\}$.
- Note that $\left|S_4\right| = 24 = 6 \cdot 4 = \left|\text{Orbit}\right| \cdot \left|\text{Stabilizer}\right|$

Example. The symmetric group S_3 acts on *itself* by conjugation $g \cdot x = gxg^{-1}$.

- Orbits are all elements of the same length:
  - Orbit of identity: $\{e\}$
  - Orbit of 2-cycles: $\big\{(1\ 2),\ (1\ 3),\ (2\ 3)\big\}$
  - Orbit of 3-cycles: $\big\{(1\ 2\ 3),\ (1\ 3\ 2)\big\}$
- The stabilizer of an element will be the elements which commute with it.
  - Everything commutes with e
  - Swaps commute only with themselves (Orbit of size 3; Stabilizer of size 2)
  - $(1\ 2\ 3)$ and $(1\ 3\ 2)$ commute with each other and e (Orbit of size 2; Stabilizer of size 3)

The Class Equation.

The orbits of its G-action partition a G-set. Thus

$$\left|X\right| \;=\; \left|X_G\right| \;+\; \left|Gx_1\right| \;+\; \cdots \;+\; \left|Gx_r\right|$$

where X_G is the set of elements that are fixed by all of G, and the Gx_i are the distinct nontrivial orbits of other elements in X. According to the orbit-stabilizer theorem we can also write this in terms of stabilizer subgroups.

$$\left|X\right| \;=\; \left|X_G\right| \;+\; \left[G : G_{x_1}\right] \;+\; \cdots \;+\; \left[G : G_{x_r}\right]$$

By the corollary of the orbit stabilizer theorem, all of these numbers divide $\left|G\right|$. Also each $\left|Gx_i\right| > 1$, because the trivial orbits are included in $\left|X_G\right|$.

The class equation is this same formula applied to the conjugation action of G on itself $\mu(g, x) = gxg^{-1}$. In this case, X_G becomes the **center** of the group $Z(G)$, the orbits become the **conjugacy classes** of elements, and the stabilizer subgroups are the **centralizer subgroups** $C(x_i) = \{g \mid gx_i = x_ig\}$.

Definition. The **class equation** for a group G is an expression for $|G|$ as a sum

$$\left|G\right| \;=\; \left|Z(G)\right| \;+\; n_1 \;+\; \cdots \;+\; n_r$$

- $Z(G) = \{g \mid gh = hg \text{ for all } h \in G\}$ is the center of G
- $n_i = \left[G : C(x_i)\right]$ is the index of a distinct centralizer subgroup $C(x_i) = \{g \mid gx_i = x_ig\}$

Following are two quick examples of the **POWER** of the class equation.

Proposition. *If G has order p^n where p is prime, then $Z(G) \neq \{e\}$.*

Proof. By the class equation $p^n = |G| = |Z(G)| + n_1 + \cdots + n_r$. The n_i are nontrivial divisors of p^n, so they are multiples of p. Thus $|Z(G)|$ must also be a multiple of p. In particular $|Z(G)| \neq 1$. □

Proposition. *If G has order p^2 where p is prime, then G is abelian.*

Proof. From the proof of the previous proposition, we know that $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$ then we are done.

Suppose by way of contradiction that $|G| = p$ and consider $G \big/ Z(G)$. If $|G| = p$ then $\left|G \big/ Z(G)\right| = p$ by Lagrange, and thus is cyclic $G \big/ Z(G) = \left\langle [a] \right\rangle$. Thus $g, h \in G$ have $[g] = [a]^i$ and $[h] = [a]^j$ for some i, j. So $g = a^ix$ and $h = a^jy$ for some $x, y \in Z(G)$. In this case

$$gh \;=\; a^ix\,a^jy \;=\; a^ia^jxy \;=\; a^ja^iyx \;=\; a^jy\,a^ix \;=\; hg$$

Therefore G is abelian. □

Burnside's Count.

Burnside's Count says that the number of distinct orbits of a G-action is equal to the average number of fixed points for elements in G.

Theorem [Burnside]. *Let X be a G-set (with everything finite) with k distinct G-orbits. Then*

$$k \;=\; \frac{1}{|G|} \sum_{g \in G} |X_g|$$