Abstract Algebra
Lecture 22
Monday, 11/22/2010

The third best trick in mathematics: count sounthing two ways. The tenth best trick in mathematics: pull something out that won't work anywhere else.

1 Group Actions

Defn: A **group action** of a group G on a set A is a function

$$f : G \times A \to A$$

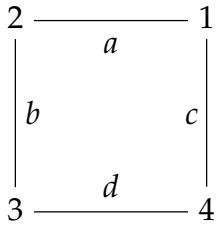
which satisfies the following properties:

- $f(1, a) = a$
- $f(g, f(h, a)) = f(gh, a)$.

We will denote this as $1 \cdot a = f(1, a)$ and $g \cdot (h \cdot a) = (gh) \cdot a$.

Ex: Invertible $n \times n$ matrices act on size n vectors by multiplication. The group of units in a field also acts on vectors.

Ex: Recall our old friend $D_4 = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \rho_1, \rho_2, \rho_3, \rho_4\}$, the dihedral group of symmetries of a square.



If we label the vertices and edges of the square as shown above, then we have

$$\sigma_3 \cdot 2 = 1 \qquad \rho_2 \cdot 4 = 3$$

$$\sigma_1 \cdot c = a \qquad \rho_2 \cdot d = d$$

and so on.

Theorem: An action of G on A is equivalent to a homomorphism from G to S_A, the symmetric group on A.

Proof: Let $f : G \times A \to A$ be an action. Define $\phi : G \to S_A$ by $\phi(g)(a) = g \cdot a$. Why is $\phi(g)$ a permutation? Because $\phi(g)$ is a bijective map from A to itself. We can see this since $\phi(g^{-1})$ is its inverse: $\phi(g^{-1}) \circ \phi(g)(a) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1_G \cdot a = a$. Is ϕ a homomorphism? Yes, because $\phi(gh)(a) = (gh) \cdot a = g \cdot (h \cdot a) = \phi(g) \circ \phi(h)(a)$. ∎

Ex: Consider D_4 acting on the edges of a square. This gives the homomorphism:

$$\begin{aligned} \sigma_0 &\mapsto e & \rho_1 &\mapsto (ac)(bd) \\ \sigma_1 &\mapsto (abcd) & \rho_2 &\mapsto (bc) \\ \sigma_2 &\mapsto (ad)(bc) & \rho_3 &\mapsto (ab)(cd) \\ \sigma_3 &\mapsto (acdb) & \rho_4 &\mapsto (ad) \end{aligned}$$

Theorem: Let G act on A. Then:

1. The **kernel** of the action, defined as
$$\{g \in G \mid g \cdot a = a \forall a \in A\}$$
is a normal subgroup of G.
2. For every $a \in A$, the set
$$G_a = \{g \in G \mid g \cdot a = a\}$$
is a subroup of G.

Proof: The group in part (1) is the kernel of the corresponding homomorphism. For part (2), let $g, h \in G_a$. Then $(gh) \cdot a = g \cdot (h \cdot a) = a$. The proof of closure under inverses is left for the reader. ∎

Theorem: Cayley's Theorem. Every group G is isomorphic to a subgroup of a symetric group. Specifically, S_G.

Proof: Let the group G act on the set G by left multiplication: $g \cdot h = gh$. This gives a homomorphism from G to S_G. We want to show that this homomorphism is injective. So asume g is in the kernel of this map. This means $g \cdot h = h$ for all $h \in G$. So $gh = h$, so g is the identity. Since the kernel of the homomorphism is just the identity, the map is injective. ∎

But what does a group action tell us about a set? For starters, it gives an equivalence relation on elements of the set: $x \sim y \iff x = g \cdot y$. We call these equivalence classes **orbits**.

Theorem: If a finite group G acts on A, then the sizes of the orbits divide $|G|$. Specificaly, $|G| = |G_a| \cdot |\text{Orb}(a)|$.

Proof: We claim that $xG_a = yG_a$ if and only if $x \cdot a = y \cdot a$. If $x \cdot a = y \cdot a$, then $a = (x^{-1}y) \cdot a$. So $x^{-1}y \in G_a$, which gives $x^{-1}yG_a = G_a$. Hence $yG_a = xG_a$. Each step works backwards. Thus the map

$$\{g \cdot a \mid g \in G\} \to \{g \cdot G_a \mid g \in G\}$$

defined by

$$g \cdot a \mapsto g \cdot G_a$$

is a well-defined bijection. Thus, there are as many cosets as there are elements of the orbit, so Lagrange's Theorem gives the desired result. ∎

What happens if $|G| = p^a$? The equivalence classes on A have sizes that are powers of p. Let n_i be the number of orbits of size p^i. Now, $|A| = n_0 + n_1 p + n_2 p^2 + \cdots n_a p^a$. So then $|A| \equiv n_0 \mod p$. We introduce notation such that $|A| = |A_G| \mod p$, where $A_G = \{a \in A \mid g \cdot a = a \forall g \in G\}$ (the set of elements that aren't moved by anything).

Theorem: Cauchy's Theorem. Let G be a group and p a prime with $p \big| |G|$. Then G contains an element of order p.

Proof: Let $X = \{(g_1, g_2, \ldots, g_p) \mid g_1 g_2 \cdots g_p = 1, g_i \in G\}$. Notice $g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$. So $|X| = |G|^{p-1} \equiv 0 \mod p$. Consider $\langle (123 \ldots p) \rangle \subseteq S_p$. We have $|\langle (123 \ldots p) \rangle| = p$. This group acts on X:

$$(123 \ldots p) \cdot (g_1, g_2, \ldots, g_p) = (g_p, g_1, g_2, \ldots, g_{p-1}).$$

Check: does $g_p(g_1 g_2 \cdots g_{p-1}) = 1$? Yes, since $g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$. Now, what is X_G? What are the things fixed by the action of this group? If $(g_1, g_2, \ldots, g_p) \in X_G$, then $(g_1, g_2, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1})$, so $g_1 = g_2 = \cdots = g_p$. So, $X_G = \{(g, g, \ldots, g) \mid g^p = 1\}$. Also, X_G is nonempty, since at least $(1, 1, \ldots, 1) \in X_G$. But we know that $|X| \equiv 0 \mod p$, so we also have $|X_G| \equiv 0 \mod p$. And since X_G has at least the identity, it must have at least p elements. So there is some $g \in G$ such that $g \neq 1$ and $(g, g, \ldots, g) \in X_G$. Then g has order p. ∎