GROUP ACTIONS

GROUP ACTIONS

Before "MODERN ALGEBRA," groups were collections of invertible transformations.

Permutations <u>permute</u> (some finite set)

Invertible linear transformations <u>move</u> vectors in a vector space

Galois groups (next term) <u>exchange</u> roots of a polynomial.

The general notion underlying these examples is that of a <u>group action</u>.

Definition An *action* of the group G on the set X is a map $a: G \times X \longrightarrow X$, $(g, x) \mapsto g \cdot x = g(x)$

where

1. $e \cdot x = x \quad \forall x \in X$
2. $(g_1 g_2) x = g_1 (g_2 x) \quad \forall g_1, g_2 \in G$, $x \in X$

Example. $G = S_n$, $X = \{1, \dots, n\}$.

The elements of S_n are determined by their action (permutation) of X.

Example: $G = GL(2,\mathbb{R})$ (invertible matrices)

$$X = \mathbb{R}^2 \qquad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad x = \begin{pmatrix} x \\ y \end{pmatrix}$$

$$g x = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} \qquad e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$(g_1 g_2) x = g_1 (g_2 x)$ by associativity of matrix multiplication.

Example: G any group, $X = N \trianglelefteq G$

$a(g,n) = g n g^{-2}$ conjugation action.

$N = G$ is especially important

EXAMPLE: RUBIK'S CUBE

EACH OF THE SIX FACES CAN BE ROTATED
90°, 180°, 270°, or 360° (the identity)

The group of transformations of the Rubik's cube is generated by 6 90° rotations, each of order 4.

Definition Let G act on X. Let $x, y \in X$. Say $x \sim_G y$ if $\exists\, g \in G,\ gx = y$

Proposition The relation $\sim_G$ is an equivalence relation.

Proof: **Reflexive**: $\forall\, x \in X \quad ex = x$

Symmetric If $gx = y$, then $y = g^{-1}x$

Transitive If $gx = y$, $hy = z$, then

$$(hg)x = h(gx) = hy = z \Rightarrow x \sim_G z.$$

The equivalence classes for $\sim_G$ are called <u>orbits</u>. The orbit containing $x \in X$ is written $\mathcal{O}_x$.

<u>Example</u> $G = GL(2,\mathbb{R})$ $X = \mathbb{R}^2$ Two orbits $\left\{\begin{pmatrix}0\\0\end{pmatrix}\right\}$ and everything else.

<u>Example</u>: $G = X$ acting on itself by conjugation. The orbits are conjugacy classes

---

<u>Definition</u>: The action of G on X is <u>transitive</u> if it has only one orbit

<u>Example</u>: S_n acting on $\{1, \dots, n\}$ is transitive

Definition: Let G act on X. The **stabilizer subgroup** of x, denoted G_x, is the set

$$G_x = \{g \in G \mid gx = x\}.$$

Lemma: This is a subgroup.

Proof: Exercise.

Challenge 1. Let $G = S_n$, $X = \{1, \dots, n\}$.

what is G_n = the stabilizer of the element n?

Challenge 2. Let $G = GL(2, \mathbb{R})$, $V = \mathbb{R}^2$;

$v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Determine the stabilizer subgroup G_v.

Theorem: Let G be a finite group acting on a set X. Then

$$|O_x| = |G|/|G_x|$$

Proof: We know that $|G|/|G_x|$ is the number of cosets of G_x in G. We define a bijection $\alpha: G/G_x \longrightarrow O_x$. To any $g \in G$ we let

$$\alpha(gG_x) = g(x).$$

1. α is well defined. If $gG_x = g'G_x$ then $\exists\, h \in G_x$, $g' = gh$. But $(gh)x = g(hx) = g(x)$ because $h \in G_x$

2. α is surjective. If $y \in \mathcal{O}_x$ then $\exists\, g \in G$, $gx = y$. Then $y = \alpha(gG_x)$.

3. α is injective. Suppose

$$\alpha(gG_x) = \alpha(hG_x) \Rightarrow g(x) = h(x).$$

Then

$$(h^{-2}g)(x) = h^{-2}(h(x)) = x$$

so $h^{-2}g \in G_x \Rightarrow gG_x = hG_x$.

Thus

$$|G|/|G_x| = |G/G_x| = |\mathcal{O}_x|.$$

$\square$

G acting on X.

$$X_G = \{x \in X \mid g(x) = x \ \ \forall g \in G\}$$

= set of orbits consisting of a single element.

$X = G$, $\quad g(h) = ghg^{-1}$ conjugation action.

$$X_G = \{h \in G = X \mid ghg^{-1} = h \ \ \forall g \in G\}$$

$ghg^{-1} = h \iff gh = hg \ \ \forall g \in G \quad X_G = Z_G$

Conjugation. $G \curvearrowright X$.

$$g(h) = ghg^{-1}.$$

What is G_e? (stabilizer)

What is $\mathcal{O}_e$? $geg^{-1} = gg^{-1} = e$

$|\mathcal{O}_e| = 1$. $G_e = G$

$geg^{-1} = e \ \forall g \in G$.

$$\frac{|G|}{|G_e|} = |\mathcal{O}_e|$$

$\shortparallel$

1

Another action of G on G $\quad X = G$

$G \times G \to G \qquad g(h) = g \cdot h.$

What are the orbits?

Answer: the action is <u>transitive</u>:

$g(e) = g \cdot e = g. \implies e \sim_G g \ \forall g$

So the orbit $\mathcal{O}_e = G. \quad \Big| \quad \underset{\substack{\shortparallel \\ g}}{g(e)} = e$

G_e = stabilizer of e.

$= \{e\} \qquad |G| / |G_e| = |\mathcal{O}_e| = |G|$

Corollary (the orbit equation). Suppose G is a finite group acting on a finite set X. Then orbits = fixed points $\cup \{O_{x_1}, \dots O_{x_n}\}$

$$|X| = |X_G| + \sum_{i=1}^{n} [G : G_{x_i}] ,$$ where

$X_G = \{x \in X \mid gx = x \ \forall g \in G\}$ is the fixed point set of G

and $\{x_i\}$ are representatives of distinct orbits that are not fixed points, $i = 1, \dots, n$.

Example: $X = G$, with conjugation. Then $X_G = Z(G)$ is the center of G.

Proof of the orbit equation:

$$X = \text{fixed points} \amalg \underbrace{\text{orbits that are not fixed points}}^{n \text{ orbits}}$$

In each orbit on the right, choose an element x_i.

$$X = \underset{\text{fixed points}}{X_G} \amalg \mathcal{O}_{x_1} \amalg \mathcal{O}_{x_2} \amalg \dots \amalg \mathcal{O}_{x_n}$$

$$|X| = |X_G| + |\mathcal{O}_{x_1}| + \dots + |\mathcal{O}_{x_n}|$$

$$|X| = |X_G| + \sum_{i=1}^{n} |\mathcal{O}_{x_i}|$$

But $|\mathcal{O}_{x_i}| = |G| / |G_{x_i}| = [G : G_{x_i}]$

so

$$|X| = |X_G| + \sum_{i=1}^{n} [G : G_{x_i}]$$

$\square$

Conjugation action next time.

Theorem: Let G be a finite group. Then
$$|G| = |Z_G| + \sum_{i=1}^{n} |G/C_{h_i}|$$

where h_i runs through representatives of conjugacy classes not in the center and C_{h_i} is the centralizer.

Proof: $h \in X_G \iff \forall g \in G \quad ghg^{-1} = h$

$\iff \forall g \in G \quad gh = hg \iff h \in Z(G)$.

Moreover, for any $h \in G$, the stabilizer

$$G_h = \{g \in G \mid ghg^{-1} = h\}$$

$$= C_h = \{g \in G \mid gh = hg\}$$

the centralizer of h

The orbit equation in this case is called the class equation

$$|G| = |Z(G)| + \sum_{h_i} [G : C_{h_i}]$$

$$|G| = |Z(G)| + \sum_{h_i} [G : C_{h_i}]$$

Example: In $G = S_n$, $n > 2$, we know $Z(S_n) = \{e\}$ and the conjugacy classes are in bijection with the partitions of n (cycle lengths).

Judson says this is (almost) an NP complete problem.

Theorem: Let G be a p-group where p is a prime. Then $|Z(G)| \geq p$.

Proof: We have

$$|G| = |Z(G)| + \sum_{h_i} [G : C_{h_i}].$$

Each C_{h_i} is a subgroup of G, hence is a p-group. And $|G| \equiv 0 \ (p)$, $|C_{h_i}| < |G|$

$\Rightarrow p \mid [G : C_{h_i}]$, $p \mid |G|$. Thus $p \mid |Z(G)|$.

<u>Corollary</u>: Let $|G| = p^2$ for some p. Then G is abelian.

<u>Proof</u>: We know $|Z(G)| \geq p$. Let $h \in G$, $h \notin Z(G)$. Then the group H generated by h and $Z(G)$ is of order $> p$ but divides $p^2 \Rightarrow H = G$. But h commutes with $Z(G)$, so H is an abelian group $\Rightarrow$ G is abelian.

A theorem of Cauchy

Theorem

Let G be a finite group of order n and let p be a prime dividing n. Then G has an element of order p.

Proof.

We use the Class Equation, where the x_i are representatives of conjugacy classes not in the center:

$$|G| = |Z(G)| + \sum_i [G : C_{x_i}]$$

Assume the theorem is true for groups of order less than n. If p divides the order of one of the C_{x_i}, then by induction C_{x_i} has an element g of order p, because $|C_{x_i}| < |G| = n$. But $g \in C_{x_i} \subseteq G$, so we are done. □

Proof of Cauchy's theorem, continued

Proof.

So we assume p divides no C_{x_i}. Then $p | [G : C_{x_i}] = |G|/|C_{x_i}|$ for all i.

Now p divides

$$|G| - \sum_i [G : C_{x_i}] = |Z(G)|$$

because it divides each term on the left-hand side. Thus p divides $|Z(G)|$. But then $|Z(G)|$ has an element of order p, by the classification of finite abelian groups. □

Proof of Cauchy's theorem, continued

Proof.

So we assume p divides no C_{x_i}. Then $p | [G : C_{x_i}] = |G|/|C_{x_i}|$ for all i. Now p divides

$$|G| - \sum_i [G : C_{x_i}] = |Z(G)|$$

because it divides each term on the left-hand side. Thus p divides $|Z(G)|$. But then $|Z(G)|$ has an element of order p, by the classification of finite abelian groups. □

Proof of Cauchy's theorem, continued

Proof.

So we assume p divides no C_{x_i}. Then $p|[G : C_{x_i}] = |G|/|C_{x_i}|$ for all i. Now p divides

$$|G| - \sum_i [G : C_{x_i}] = |Z(G)|$$

because it divides each term on the left-hand side. Thus p divides $|Z(G)|$. But then $|Z(G)|$ has an element of order p, by the classification of finite abelian groups. $\square$

The group of transformations of Rubik's cube has order

$$43{,}252{,}003{,}274{,}489{,}856{,}000$$

$$= 2^{27} 3^{14} 5^3 \cdot 7^2 \cdot 11$$

It is a SEMIDIRECT PRODUCT

$$(\mathbb{Z}_3^7 \times \mathbb{Z}_2^{11}) \rtimes ((A_8 \times A_{12}) \rtimes \mathbb{Z}_2)$$

AND IT ACTS BY PERMUTING TWO SUBSETS OF THE 26 BLOCKS:

- THE 8 CORNERS
- THE 12 EDGES

HENCE A_8, and A_{12}

THE 6 CENTERS OF EACH FACE **DON'T MOVE**.

CAN'T PERMUTE TWO CORNERS LEAVING THE OTHERS ALONE.