2. Permutation groups and group actions

Def: Let G be a group, and S be a set. A group action of G on S is a homom. $\phi: G \longrightarrow \mathrm{Perm}(S)$.

If ϕ is injective, then the action is faithful.

Usually, if $x \in G$, $s \in S$, write $x \cdot s$ for xs instead of $\phi(x)(s)$.

Thus, we have a mapping
$$G \times S \longrightarrow S$$
$$(x,s) \longmapsto xs$$
satisfying

(i) $(xy)s = x(ys)$

(ii) $1s = s$. for all $x,y \in G$, $s \in S$.

Note: This is another way to define an action.

Def: If G acts on S, then the stabilizer of $s \in S$ is the set (secretly, a subgroup) $\mathrm{Stab}_G(s) = \{x \in G : xs = s\}$.

The orbit of s is $\mathrm{Orb}_G(s) = \{xs : x \in G\}$.

Def: If $\mathrm{Orb}_G(s) = S$, then G acts transitively on S.

Prop 2.1: If G acts on S, and $s \in S$, then $\mathrm{Stab}_G(s) \leq G$ and $[G : \mathrm{Stab}_G(s)] = |\mathrm{Orb}_G(s)|$.

Pf: Let $H = \mathrm{Stab}_G(s)$. If $x,y \in H$ then $ys = s \Rightarrow s = y^{-1}s$.

So, $(xy^{-1})s = x(y^{-1}s) = xs = s \Rightarrow xy^{-1} \in H \Rightarrow H \leq G$. ✓

Define $\Theta: \mathrm{Orb}_G(s) \longrightarrow G/\mathrm{Stab}_G(s)$, $\Theta(xs) = xH$ (not a homom; $\mathrm{Orb}_G(s)$ isn't a group!)

1-1: $xs = ys \Rightarrow y^{-1}x \in H \Rightarrow \Theta(y^{-1}x) = H$ ✓
$\Rightarrow xH = yH$.

Clearly onto. $\square$

<u>Remark</u>: The <u>kernel</u> of an action is $\ker \phi$. This is the set of elts $\{x : x \cdot s = s \ \forall s \in S\}$.

<u>Example</u>: Take $S = G$, define $x \cdot y = xy$.

The kernel is $\{x \in G : xy = y \ \forall y \in G\} = 1$.

Thus, G acts faithfully.

This is the <u>left regular representation</u> of G.

<u>Thm 2.2</u> (Cayley): Every group G is isomorphic to a transitive group of permutations acting on a set S.

<u>Pf</u>: Let $S = G$. We saw above that G acts on S.

<u>Transitivity</u>: Start with $y, z \in G$. Need $x \in G$ s.t. $x \cdot y = z$

Take $x = zy^{-1}$. $x \cdot y = zy^{-1} \cdot y = z$. ✓ $\square$

<u>Cor</u>: If $|G| = n$, then $G \hookrightarrow S_n$. "isomorphic to a subgp of S_n".

<u>Def</u>: If G is a group, and $x, y \in G$, then the <u>conjugate</u> of x by y is $x^y := y^{-1}xy$. <u>Note</u>: $x^{yz} = (x^y)^z$.

<u>Example</u> Take $S = G$. G acts on S by conjugation:

$x \cdot y = y^{x^{-1}} = xyx^{-1}$, or $\phi(x)y = y^{x^{-1}} = xyx^{-1}$

<u>Check</u>: $x, y \in G$, $z \in S$, then $\phi(xy)z = z^{(xy)^{-1}} = z^{y^{-1}x^{-1}} = (z^{y^{-1}})^{x^{-1}}$

$= \phi(x)(z^{y^{-1}}) = \phi(x)\phi(y)z$.

$\ker \phi = \{x \in G : y = xyx^{-1} \ \forall y \in G\} = Z(G)$.

Action is faithful $\Longleftrightarrow Z(G) = 1$.

Def: If $y \in G$, then $\mathrm{Orb}_G(y)$ is the conjugacy class of G containing y, denoted $cl(y)$. The stabilizer of $y \in G$ is $\{x \in G : xy = yx\}$, called the centralizer of y in G, denoted $C_G(y)$.

Prop 2.3: If G is a group, $x \in G$, then $|cl(x)| = [G : C_G(x)]$.

Pf: Immediate from Prop 2.1 (orbit-stabilizer thm). $\square$

Note: $|cl(x)| = 1 \Leftrightarrow y^{-1}xy = x \ \forall y \Rightarrow xy = yx \Rightarrow x \in Z(G)$.

Thus, $$|G| = \sum |cl(x)| = |Z(G)| + \underbrace{\sum_{i=1}^{k} [G : C_G(x_i)]}_{}$$

where $\{x_1, \ldots, x_k\}$ is a transversal of the size ≥ 2 conj. classes

This is the class equation.

Note: $|Z(G)|$ and $[G : C_G(x_i)]$ divide $|G|$.

Prop 2.4 If $|G| = p^n$ (p prime), then $|Z(G)| > 1$.

Pf. $p \mid [G : C_G(x_i)]$ and $p \mid |G| \Rightarrow p \mid |Z(G)| > 1$. $\square$

Let S = Set of subsets of G. Then, G acts on S by $\phi(x) A = xAx^{-1} = A^{x^{-1}}$ for $x \in G$, $A \in S$.

- The elements of $\mathrm{Orb}_G(A)$ are the G-conjugates of A.
- $\mathrm{Stab}_G(A)$ is the normalizer of A in G, denoted $N_G(A)$

Prop 2.5: The number of distinct G-conjugates of A in G is $[G : N_G(A)]$

$\boxed{4}$

Thm 2.6 (The [2^{nd}] Isomorphism theorem): Suppose $H, K \leq G$, and $K \leq N_G(H)$. Then $KH = HK \leq G$, $H \trianglelefteq KH$, $K \cap H \trianglelefteq K$, and $KH/H \cong K/(K\cap H)$.

$$\begin{tikzcd}[column sep=small]
 & G \arrow[d, dash] & \\
 & HK \arrow[dl, dash] \arrow[dr, dash] & \\
H \arrow[dr, dash] & & K \arrow[dl, dash] \\
 & H\cap K &
\end{tikzcd}$$

Pf: Note: $KH = \{ kh : k \in K, h \in H\}$

Show $KH \leq G$: Consider $k_1h_1, k_2h_2 \in KH$.

$$k_1h_1(k_2h_2)^{-1} = k_1(h_1h_2^{-1})k_2^{-1} = k_1(k_2^{-1}k_2)(h_1h_2^{-1})k_2^{-1}$$

$$= \underbrace{(k_1k_2^{-1})}_{\in K}\ \underbrace{k_2(h_1h_2^{-1})k_2^{-1}}_{\in H \text{ b/c } k \in N_G(H)}. \quad \checkmark$$

Show $KH = HK$ $\quad kh = (khk^{-1})k \in HK \Rightarrow KH \subseteq HK$

$\quad hk = k(k^{-1}hk) \in KH \quad HK \subseteq KH$ $\checkmark$

Show $H \trianglelefteq KH$ $\quad khk^{-1} \in H \Rightarrow khk^{-1} \in KH \Rightarrow kHk^{-1} \subseteq KH$ $\checkmark$.

Define $f : K \longrightarrow KH/H$, $f(k) = kH$.

Check: f is a homom, f is onto.

$\ker f = \{ k \in K : kH = H\} = K \cap H$.

By FHT, $K/\ker f = K/K\cap H \cong KH/H$. $\square$

Let G be a group, $H \leq G$, $S = \{xH : x \in G\}$.

G acts on S, by $\phi(x)\,yH = xyH$.

$x \in$ kernel iff $xyH = yH \Leftrightarrow y^{-1}xy \in H$ $\forall y \in G$.

Thus, the kernel is $K = \bigcap_{y \in G} yHy^{-1}$.

Action is faithful iff $K = 1 \Leftrightarrow \bigcap_{y \in G} y^{-1}Hy = 1$.

Suppose $[G:H]=n$. Then this action is a homom.

$\phi: G \longrightarrow Perm(S) \cong S_n$.

By FHT, $G/K \cong Im(\phi)$, so $[G:K] \mid n!$ (By Lagrange's thm).

Thm 2.7 (Cauchy): Suppose G is a finite group, p a prime, and $p \mid |G|$. Then G has an elt. of order p.

Pf: Let $S = \{(x_1, \dots, x_p) : x_1 x_2 \cdots x_p = 1\} \setminus \{(1,1,\dots,1)\}$.

Note: We may choose $x_1, \dots, x_{p-1}$ at will. Then x_p is forced.

Thus, $|S| = |G|^{p-1} - 1$, so $p \nmid |S|$.

The group $\mathbb{Z}_p$ acts on S by cyclic shift:

$\mathbb{Z}_p = \langle \sigma \rangle$ and $\sigma \cdot (x_1, x_2, \dots, x_p) = (x_2, x_3, \dots, x_p, x_1)$.

Note: $x_1 x_2 \cdots x_p = 1 \iff x_1^{-1}(x_1 x_2 \cdots x_p) x_1 = x_2 x_3 \cdots x_p x_1 = 1$.

By Prop 2.1, every orbit has 1 or p elements.

If all orbits had p elts, then $p \mid |S|$. But $p \nmid |S|$.

Therefore, there must be an orbit of size 1.

Must be of the form $(x, x, \dots, x)$, $x \neq 1$. $\Rightarrow x^p = 1$. $\square$

Application: Suppose $|G| = 28$. Then $\exists\, x \in G$ with $|x| = 7$.

Let $H = \langle x \rangle$, so $|H| = 7$.

G acts on the left cosets of H, so $\exists\, \phi: G \longrightarrow S_4$.

size 28 size 24

Thus, $K = \ker f \neq 1$. Recall: $K = \bigcap \{xHx^{-1} : x \in G\} \leq H \Rightarrow K = H$.

In other words, $xHx^{-1} = H \;\; \forall x \in G \Rightarrow H \trianglelefteq G$.

Example of a group action

let $G = \mathbb{Z}_4 = \{1, r, r^2, r^3\}$

$S = \{$ set of cyclic binary 4-strings $\}$.

G acts on S by cyclic shift, or rotation.

e.g., $\begin{matrix} x_1 & - & x_2 \\ | & & | \\ x_4 & - & x_3 \end{matrix} \longrightarrow \begin{matrix} x_4 & x_1 \\ x_3 & x_2 \end{matrix}$

$= |\mathrm{Orb}_G(s)|$ by Orb-stab thm (Prop 2.1)

Orbits:	size	$\mathrm{Stab}_{\mathbb{Z}_4}(s)$	$[\mathbb{Z}_4 : \mathrm{Stab}_{\mathbb{Z}_4}(s)]$
$\begin{smallmatrix}0&0\\0&0\end{smallmatrix}$	1	$\{1, r, r^2, r^3\}$	$4/4 = 1$
$\begin{smallmatrix}1&1\\1&1\end{smallmatrix}$	1	$\{1, r, r^2, r^3\}$	$4/4 = 1$
$\begin{smallmatrix}1&0\\0&1\end{smallmatrix} \rightleftarrows \begin{smallmatrix}0&1\\1&0\end{smallmatrix}$	2	$\{1, r^2\}$	$4/2 = 2$
$\begin{smallmatrix}1&0\\0&0\end{smallmatrix} \to \begin{smallmatrix}0&1\\0&0\end{smallmatrix} \to \begin{smallmatrix}0&0\\0&1\end{smallmatrix} \to \begin{smallmatrix}0&0\\1&0\end{smallmatrix}$	4	1	$4/1 = 4$
$\begin{smallmatrix}1&1\\0&0\end{smallmatrix} \to \begin{smallmatrix}0&1\\0&1\end{smallmatrix} \to \begin{smallmatrix}0&0\\1&1\end{smallmatrix} \to \begin{smallmatrix}1&0\\1&0\end{smallmatrix}$	4	1	$4/1 = 4$
$\begin{smallmatrix}1&1\\0&1\end{smallmatrix} \to \begin{smallmatrix}0&1\\1&1\end{smallmatrix} \to \begin{smallmatrix}1&0\\1&1\end{smallmatrix} \to \begin{smallmatrix}1&1\\1&0\end{smallmatrix}$	4	1	$4/1 = 1$