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 homomorphism $\phi : G \rightarrow \text{Perm}(S)$. If $\phi$ is injective, then the action is **faithful**.

Usually, if $x \in G$, $s \in S$, write $xs$ for $\phi(x)(s)$. Thus, we have a mapping $G \times S \rightarrow S$

$$(x, s) \mapsto xs$$

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) $\text{Stab}_G(s) = \{x \in G : xs = s\}$.

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

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

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

**Proof:** Let $H = \text{Stab}_G(s)$. 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** $\Theta : \text{Orb}_G(s) \rightarrow G/\text{Stab}_G(s)$, $\Theta(xs) = xH$. (not a homomorphism,

$$1-1$$

$$xs = ys \Rightarrow yx \in H \Rightarrow \Theta(yx) = H$$ ✓

**Clearly acts.**

$$\Theta(xH) = yH.$$ a group!
Remark: The kernel of an action is \( \ker \phi \). This is the set of elts \( \{ x : x \circ s = s \; \forall s \in S \} \).

Example: Take \( S = G \), define \( x \circ y = xy \).

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

Thus, \( G \) acts faithfully.

This is the left regular representation of \( G \).

**Thm 2.2 (Cayley):** Every group \( G \) is isomorphic to a transitive group of permutations acting on a set \( S \).

**Proof:** Let \( S = G \). We saw above that \( G \) acts on \( S \).

Transitivity: Start with \( y, z \in G \). Need \( x \in G \) s.t. \( x \circ y = z \).

Take \( x = z^{-1} \). \( x \circ y = z^{-1} \circ y = z \). \( \checkmark \)

Case: If \( |G| = n \), then \( G \rightarrow S_n \). "Isomorphic to a subgp of \( S_n \)."

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

Example: Take \( S = G \). \( G \) acts on \( S \) by conjugation: \( x \circ y = y^x = xyx^{-1} \), or \( \phi(x)y = y^x = xyx^{-1} \).

Check: \( x, y \in G \), \( z \in S \), then \( \phi(xy)z = z^{(xy)^z} = z^{y^{-1}x^{-1}} = (z^y)^{x^{-1}} = \phi(x)(z^y) \).

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

Action is faithful \( \iff Z(G) = 1 \).
Def: If $y \in G$, then $\text{Orb}_G(y)$ is the conjugacy class of $G$ containing $y$, denoted $c(y)$. 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 $|c(x)| = [G : C_G(x)]$.

Proof: Immediate from Prop 2.1 (orbit-stabilizer theorem).

Note: $|c(x)| = 1 \iff y^x y = x \iff y = y x \iff x \in Z(G)$.

Thus, $|G| = \sum |c(x)| = |Z(G)| + \sum \left[ \frac{|G|}{|C_G(x_i)|} \right]$

where $\{x_1, \ldots, x_k\}$ is a transversal of the size $\geq 2$ conjugacy 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 $|Z(G)| > 1$.

Proof: $p | |G| = p^n \implies p | [G : C_G(x_i)] \implies p | |Z(G)|$.

Let $S =$ set of subsets of $G$. Then, $G$ acts on $S$ by

$\phi(x)A = xAx^{-1} = A^x$ for $x \in G$, $A \in S$.

- The elements of $\text{Orb}_G(A)$ are the $G$-conjugates of $A$.
- $\text{Stab}_G(A)$ 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 $[G : N_G(A)]$. 

\[\]
Theorem 2.6 (The 2nd Isomorphism Theorem): Suppose \( H, K \leq G \) and \( K \triangleleft N_G(H) \). Then \( KH = HK \leq G \), \( H \triangleleft KH \), \( KN_H \triangleleft K \), and \( KH/H \cong K/(KN_H) \).

Proof: Note: \( KH = \{ kh : k \in K, h \in H \} \)

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

\[
k_1h_1(k_2h_2)^{-1} = k_1(h_1h_2^{-1})k_2^{-1} = k_1(k_2^{-1}k_2)(h_1h_2^{-1})k_2^{-1} \\
= (k_1k_2^{-1})k_2(h_1h_2^{-1})k_2^{-1}.
\]

\( \in K \cap H \) \( \Rightarrow \) \( K \cap H \leq N_G(H) \)

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

\( kh = k(hk^{-1}) \in KH \) \( \Rightarrow \) \( HK \subseteq KH \)

Show \( H \triangleleft KH \) \( khk^{-1} \in H \Rightarrow khk^{-1} \in KH \Rightarrow (khk^{-1})H \subseteq KH \)

Define \( f : K \longrightarrow KH/H \) \( f(k) = kh \).

Check: \( f \) is a homomorphism, \( f \) is onto.

\( \ker f = \{ k \in K : kh = H \} = KN_H \).

By FHT, \( K/\ker f = K/KN_H \cong KH/H \).

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

\( G \) acts on \( S \) by \( d(x)yH = xyH \).

\( x \in \text{kernel} \iff xyH = yH \iff y^{-1}xyH = H \forall y \in G \).

Thus, the kernel is \( K = \bigcap_{y \in G} yH \).

Action is faithful iff \( K = 1 \iff \bigcap_{y \in G} yH = 1 \).
Suppose \([G:H]=n\). Then this action is a homomorphism \(\phi: G \rightarrow \text{Perm}(S) \cong S_n\).

By FH T, \(G/K \cong \text{Im}(\phi)\), so \([G:K]|n!\) (by Lagrange's thm).

**Thm 2.7 (Cauchy):** Suppose \(G\) is a finite group, \(p\) a prime, and \(p|161\). Then \(G\) has an elt. of order \(p\).

**Proof:** Let \(S = \{(x_1, \ldots, x_p); x_1x_2\ldots x_p = 1\}\) \(\setminus\{ (1,1,\ldots,1)\}\).

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

Thus, \(|S| = |G|^{p-1} - 1\), so \(p|161|\).

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

\[\mathbb{Z}_p = \langle t \rangle \text{ and } t \cdot (x_1, x_2, \ldots, x_p) = (x_2, x_3, \ldots, x_p, x_1).\]

Note: \(x_1x_2\ldots x_p = 1 \iff x_1^{-1}(x_1x_2\ldots x_p) x_1 = x_2x_3\ldots x_p x_1 = 1\).

By Prop 2.1, every orbit has 1 or \(p\) elements. If all orbits had \(p\) els, then \(p|161\). But \(p|161\).

Therefore, there must be an orbit of size 1. Must be of the form \((x, x, \ldots, x)\), \(x \neq 1\). \(\Rightarrow x^p = 1\).

**Application:** Suppose \(|G| = 28\). Then \(\exists x \in G\) \(\text{ s.t. } |x| = 7\).

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

\(G\) acts on the left cosets of \(H\), so \(\exists \phi: G \rightarrow S_4\).

(size \(2^8\)) \rightarrow (size \(2^4\)).

Thus, \(K = \ker f \neq 1\). Recall: \(K = \cap \{xHx^{-1}; x \in G\} \leq H \Rightarrow K = H\).

In other words, \(xHx^{-1} = H \forall x \in G\) \(\Rightarrow H \triangleleft G\).
Example of a group action

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

$S$: \{ set of cycle binary 4-strings \}.

$G$ acts on $S$ by cyclic shift, or rotation.

E.g., $x_1 \rightarrow x_2 \rightarrow x_4 \rightarrow x_3 \rightarrow x_2$.