# MAT3004 Lecture 8: Cosets, Lagrange's Theorem, and Group Actions

## 1 Recall: Subgroups and Cosets

For a subgroup $H \leq G$:

- Define relation: $a \sim b \iff a^{-1}b \in H$.
- This equivalence relation gives the equivalence class:

$$[a] = aH = \{ah \mid h \in H\} \quad (\textbf{Left Coset})$$

---

- Similarly, define: $a \sim_R b \iff ba^{-1} \in H$.
- This gives:

$$[a]_R = Ha = \{ha \mid h \in H\} \quad (\textbf{Right Coset})$$

Therefore, the group $G$ is partitioned into a disjoint union of left cosets:

$$G = \bigsqcup_{i \in I} a_i H$$

**Theorem 1** (Lagrange)**.** *If $|G| < \infty$, then $|H|$ divides $|G|$ (written as $|H| \mid |G|$).*

## 2 Proof of Lagrange's Theorem

*Proof.* Since $|G| < \infty$, we can write $G$ as a finite disjoint union of cosets:

$$G = a_1 H \sqcup \cdots \sqcup a_m H$$

Without loss of generality (WLOG), assume $a_1 H = eH = H$.

**Claim 1.** *$|a_i H| = |H|$ for all $i$.*

*Proof of claim:* Let $f : H \to a_i H$ be the map defined by $f(h) = a_i h$.
Then:

1. $f$ is obviously surjective by definition of $a_i H$.

2. $f$ is injective: Suppose $f(h) = f(h')$.

$$\begin{aligned} &\implies a_i h = a_i h' \\ &\implies a_i^{-1}(a_i h) = a_i^{-1}(a_i h') \\ &\implies e \cdot h = e \cdot h' \implies h = h' \end{aligned}$$

$\therefore f$ is bijective, which implies $|H| = |a_i H|$.
Using equation $(*)$, we have:

$$\begin{aligned} |G| &= |a_1 H| + \cdots + |a_m H| \\ &= |H| + \cdots + |H| \quad (m \text{ times}) \\ &= m|H| \end{aligned}$$

Thus, $|H|$ divides $|G|$. □

**Definition 1.** *We write $[G : H]$ as the number of disjoint left cosets of $H$ in $G$.*

If $|G| < \infty$, then:

$$[G : H] = m = \frac{|G|}{|H|}$$

# 3 Corollaries

**Corollary 1.** *For any $g \in G$, the order of the element divides the group order: ord$(g) \mid |G|$.*

*Proof.* Take $H = \langle g \rangle \leq G$. Then $\text{ord}(g) = |H|$. By Lagrange's Theorem, $|H| \mid |G|$. □

**Example 1.** *If $|G| = 8$, then ord$(g) \in \{1, 2, 4, 8\}$.*

**Corollary 2.** *If $|G| = p$ ($p$ is prime), then $G \cong \mathbb{Z}_p$. (Reference: HW5)*

**Corollary 3** (Fermat's Little Theorem)**.** *Let $p$ be a prime. For any integer $a$ such that $p \nmid a$ (i.e., $[a] \in (\mathbb{Z}/p\mathbb{Z})^\times$),*

$$a^{p-1} \equiv 1 \pmod{p}$$

*(e.g., $p = 13, 3^{12} \equiv 1 \pmod{13}, 5^{12} \equiv 1 \pmod{13}$)*

*Proof.* Consider the multiplicative group $G = \mathbb{Z}_p^\times$. The order of the group is $|G| = p - 1$. For any $a \in \mathbb{Z}$ with $p \nmid a$, we have $[a] \in \mathbb{Z}_p^\times$.

By Corollary 1, $\text{ord}([a]) = k$, where $k \mid (p-1)$. $\implies k \cdot l = p - 1$ for some $l \in \mathbb{N}$.
Then:

$$[a]^{p-1} = [a]^{k \cdot l} = ([a]^k)^l = [1]^l = [1]$$

$\therefore [a^{p-1}]_p = [1]_p \implies a^{p-1} \equiv 1 \pmod{p}$. □

# 4 Group Actions

Intuitively, a group action represents "moving" elements in a set $X$ by group elements $g \in G$.

**Definition 2.** *Let $G$ be a group and $X$ be a set. A $G$-**action on** $X$ is a map:*

$$G \times X \to X$$

$$(g, x) \mapsto g \cdot x$$

*Satisfying two axioms:*

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

## 4.1 Examples

1. **Symmetric Group:** $G = S_n$, $X = X_n = \{1, 2, \ldots, n\}$.

$$\sigma \cdot x = \sigma(x) \quad \text{for } x = 1, 2, \ldots, n$$

2. **Dihedral Group:** $G = D_n$, $X = X_n$ (vertices of a regular polygon).

   - $r \cdot x = \begin{cases} x+1 & \text{if } x < n \\ 1 & \text{if } x = n \end{cases}$ (Rotation)
   - $s \cdot x = \begin{cases} 1 & \text{if } x = 1 \\ n+2-x & \text{if } x > 1 \end{cases}$ (Reflection)

3. **Rotation Group:** $G = SO(2) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \middle| \theta \in \mathbb{R} \right\}$

   Let $X = S^2 = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \middle| x^2 + y^2 + z^2 = 1 \right\}$ (The Sphere).

   The action is defined by rotation (e.g., around the z-axis):

$$r_\theta \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

# 5 Action Homomorphism

**Proposition 1.** *For any $G$-action on $X$, the map*

$$\sigma : G \to Aut(X)$$

*is a group homomorphism. Here, $Aut(X) := \{\phi : X \to X \mid \phi \text{ is bijective}\}$ is the group of permutations of $X$. The map is defined by $g \mapsto \sigma_g$, where $\sigma_g(x) := g \cdot x$.*

*Proof.* **1. Well-defined ($\sigma(g) \in \mathbf{Aut}(X)$):** Given $g \in G$, is the map $\sigma_g : X \to X$ bijective? Yes, its inverse is $\sigma_{g^{-1}}$.

$$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(x) &= \sigma_{g^{-1}}(g \cdot x) \\ &= g^{-1} \cdot (g \cdot x) \\ &= (g^{-1}g) \cdot x \\ &= e \cdot x = x\end{aligned}$$

Thus $(\sigma_{g^{-1}} \circ \sigma_g) = \mathrm{id}_X$, and similarly $(\sigma_g \circ \sigma_{g^{-1}}) = \mathrm{id}_X$. Therefore, $\sigma_g$ is bijective.

**2. Homomorphism Property:** Check $\sigma(g_1 g_2) = \sigma(g_1)\sigma(g_2)$. For any $x \in X$:

$$\text{LHS: } \sigma(g_1 g_2)(x) = (g_1 g_2) \cdot x$$
$$\text{RHS: } \sigma_{g_1}(\sigma_{g_2}(x)) = g_1 \cdot (g_2 \cdot x)$$

By the definition of group action (axiom 2), these are equal. □ □

# 6 Orbits and Stabilizers

**Definition 3.** *Let $G$ act on $X$. For an element $x \in X$:*

*(i) The **orbit** of $x$ is:*

$$O_x := \{g \cdot x \mid g \in G\} \subseteq X$$

*(ii) The **stabilizer** of $x$ is:*

$$G_x := \{g \in G \mid g \cdot x = x\} \subseteq G$$

**Example 2** (Sphere Action). $G = SO(2)$, $X = S^2$ *(rotation around z-axis).*

- *If $x$ is the North/South pole, the orbit is a single point: $O_x = \{x\}$.*
- *If $x$ is elsewhere, $O_x$ is the latitude circle containing $x$.*
- *Stabilizer for $x$ on equator: $G_x = \{I\}$ (trivial).*
- *Stabilizer for North Pole $n$: $G_n = G$ (entire group fixes the pole).*

**Example 3** (Pentagon). $G = D_5$, $X = \{1, 2, 3, 4, 5\}$.

- *Orbit of vertex 1: $O_1 = \{1, 2, 3, 4, 5\} = X$. (The action is transitive).*
- *Stabilizer of vertex 1: $G_1 = \{e, s\}$, where $s$ is the reflection across the axis passing through 1.*

**Remark 1.** *1. The relation $x \sim y \iff y \in O_x$ is an equivalence relation on $X$. Thus, $X$ is partitioned by orbits: $X = \bigsqcup(\text{distinct orbits})$.*

*2. For any $x \in X$, the stabilizer $G_x$ is a subgroup of $G$ ($G_x \leq G$). Therefore, if $G$ is finite, $|G_x|$ divides $|G|$ by Lagrange's Theorem.*