12/09

Cosets and Lagrange's Theorem.

Suppose G is a finite group and H is a subgroup of G

We define a relation $\sim$ on G by

$a \sim b \iff a^{-1}b \in H$

Lagrange's Theorem

If G is a finite group and $H \leq G$, then $|H| \mid |G|$ (or) $\exists\, c \in \mathbb{N}$ such that $|G| = c|H|$

'$\sim$' is an equivalence relation (Past exercise!)

Let $a \in G$ and C_a be the equivalence class of a

$$C_a = \{x \in G \mid a \sim x\}$$
$$= \{x \in G \mid a^{-1}x \in H\}$$
$$= \{x \in G \mid x = ah \text{ for some } h \in H\}$$
$$= \{ah \mid h \in H\}$$
$$= aH$$

Definition

If G is a group and $H \leq G$, then aH is called a left coset of H.

Then $G = \bigsqcup_{a \in G} C_a$

↳ Disjoint union

$\Rightarrow |G| = \sum_{a \in G} |C_a|$

Let $a, b \in G$, we show that there is a bijection

$\phi : aH \to bH$

We will prove this by showing $\phi : H \to aH$ exists

Define $\phi : H \longrightarrow aH$
$h \mapsto ah$

ϕ is a bijection!

(i) $\phi(h_1) = \phi(h_2)$

$ah_1 = h_2$

$\Rightarrow h_1 = h_2$

So, ϕ is injective

(ii) Take $x \in aH$, then $x = ah$ for some $h \in H$

Then $\phi(h) = ah = x$

So, ϕ is surjective

So, we have

$$|G| = \sum_{a \in G} |C_a|$$

$$|G| = |H| \text{ (\# equivalence classes)}$$

Hence, Lagrange's theorem is proved.

- Equivalence classes are left cosets of H in G

So,

$$|G| = |H| \text{ (\# left cosets of } H \text{ in } G)$$

If $H \leq G$, then the index of H in G, denoted by $[G:H]$ is defined to be the number of left cosets of H in G.

Right cosets :- $Ha := \{ha \mid h \in H\}$

Similar calculation follows

$\Rightarrow$ # left cosets = # right cosets of H

Converse of Lagrange's theorem

If $d \mid |G|$, then $\exists H \leq G$ s.t $|H| \mid |G|$ and $|H| = d$

It is not true !!

Proof (by counterexample)

Let A_4 be the alternating group on $\{1, 2, 3, 4\}$

$|A_4| = 12 \ (\frac{4!}{2})$

- Suppose it is possible that $H \leq A_4$ and $|H| = 6$

← Claim :- For any $\sigma \in G$, $\sigma^2 \in H$

If $\sigma \in G$ → $\sigma \in H$ / $\sigma \notin H$

If $\sigma \in H \Rightarrow \sigma^2 \in H$

Then $G = H \sqcup \sigma H$

$G = H \sqcup aH$ for some $a \in G$

Claim :- $G = H \sqcup aH \quad \forall a \in G \setminus H$

$a \in G \setminus H$

$aH = H \iff a \in H$

If $\sigma^2 H = \sigma H$ then $\sigma \in H$ $(\Rightarrow \Leftarrow)$

$\Rightarrow \sigma^2 H = H$

$\Rightarrow \sigma^2 \in H$

Let $\sigma \in A_4$ be a 3-cycle

Then $o(\sigma) = 3$

$\Rightarrow \sigma^3 = Id$

$\Rightarrow \sigma = \sigma^4 = (\sigma^2)^2 \in H$

$\Rightarrow \sigma \in H$

All 3-cycles $\in H$ $[\Rightarrow\Leftarrow$ because $|H| = 6 \neq 8]$

Corollary

If G is a finite group and $a \in G$, then

$o(a) \mid |G|$

Let $H = \langle a \rangle$

Then $|H| = o(a)$

$\Rightarrow o(a) \mid G$

Corollary

If G is a finite group and $a \in G$ then

$a^{o(G)} = 1$

since $o(a) \mid o(G)$

$o(G) = c\, o(a)$

$a^{o(G)} = a^{c\, o(a)}$

$= (a^{o(a)})^c = 1$

Euler's Theorem

$a^{\phi(n)} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$

Let $U_n = \{ [a] \mid \gcd(a,n) = 1 \}$

$|U_n| = \phi(n)$

For any $[a] \in U_n$, $[a]^{\phi(n)} \equiv [1]$ in $U(n)$

Thus $a^{\phi(n)} \equiv 1 \pmod{n}$

Fermat's Little Theorem

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

Wilson's Theorem

$(p-1)! \equiv (-1) \pmod{p}$

(proof Exercise!)

Proposition

Let G, G' be finite groups and $\phi : G \to G'$ be a homomorphism.

Then $|G| = |\ker \phi| \, |\operatorname{Im} \phi|$

(Recall)

$\ker \varphi = \{ g \in G \mid \varphi(g) = I_{G'} \}$

$\operatorname{Im} \varphi = \{ g' \in G' \mid \varphi(g) = g' \text{ for some } g \in G \}$

Define a relation $\sim$ on G as follows

$a \sim b \iff \phi(a) \; \phi(b)$

Equivalence class $C_a : \{ x \in G \mid \phi(x) = \phi(a) \}$

$= \{ x \in G \mid [\phi(a)]^{-1} \phi(x) = I_{G'} \}$

$= \{ x \in G \mid \phi(a^{-1}) \phi(x) = I_{G'} \}$

$= \{ x \in G \mid \phi(a^{-1} x) = I_{G'} \}$

$= \{ x \in G \mid a^{-1} x \in \ker \phi \}$

(Exercise!)

If $\phi : G \to G'$ is group homomorphism, then $\ker \phi \leq G$

$= \{ x \in G \mid x \in a \ker \phi \}$

$= a \ker \phi$

$\Rightarrow |C_a| = |\ker \phi|$

$$|G| = \sum_{a \in G} |C_a|$$

$$= \sum_{a \in G} |\ker \phi|$$

$$= |\ker \phi| |\operatorname{Im} \phi|$$

Example

$SL_n(\mathbb{F}_q) = \{ M \in GL_n(\mathbb{F}_q) \mid \det(M) = 1 \}$

$\det : GL_n(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^{\times}$

$|GL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)| \, |\mathbb{F}_q^{\times}|$

$(q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = |SL_n(\mathbb{F}_q)| \, (q-1)$

Multiplicative property of index

If G is a finite group and H, K are subgroups of G s.t $K \leq H \leq G$

Then $[G:K] = [G:H][H:K]$

Proof

$[G:H] = s$, $[H:K] = t$ $\qquad G = \bigsqcup_{i=1}^{s} g_i H$

Prove $G = \bigsqcup_{\substack{i=1 \\ j=1}}^{\substack{t \\ s}} g_i h_j K$ where $H = \bigsqcup_{j=1}^{t} h_j K$