Lagrange's Theorem

Theorem: $(G,*)$ be a finite group of order n.

$G = \{g_1 \cdots g_n\}$

$H = \{h_1 \cdots h_k\} \leq G$ $(H,*)$ is a subgroup of order k.

Proof: $xH = xH$ $\quad x = y$ $\quad xH = yH$.

Equivalence class $\xrightarrow[\text{partition}]{}$ G into l equivalence class $[g] = gH$.

for any g: $|gH| = k$. $\Rightarrow n = k \cdot l$.

Another Proof:

$*$	h_1	$\cdots$	h_k
g_1H	g_1h_1	$\cdots$	g_1h_k
$\vdots$			
g_nH	g_nh_1	$\cdots$	g_nh_k

$g_iH = \{g_ih_1, g_ih_2 \cdots g_ih_k\}$

$|g_iH| = k$.

Ex. if $g_ih_2 = g_ih_4$

$g_i^{-1} \cdot g_i \cdot h_2 = g_i^{-1} \cdot g_i \cdot h_4 \Rightarrow h_2 = h_4$.

Assume I have g_iH, g_jH in my table.

Case 1: $g_iH \cap g_jH = \emptyset$ 

Case 2: $g_iH \cap g_jH \neq \emptyset$ 

Let $g_ih = g_j\tilde{h}$.

$g_ihh^{-1} = g_j\tilde{h} \cdot h^{-1}$

$g_iH \in g_j\tilde{h}h^{-1} \cdot H = g_jH$

Example mod 10

$G = \{1, 3, 7, 9\}$ $*_7$ (mod 10)

$H = \{1, 9\}$ $*_9$ (mod 10)

$*$ (mod 10)	1	9
1	1	9
3	3	7
7	7	3
9	9	1

$\{1,9\}$ $\{9,1\}$ identical.

$\{3,7\}$ $\{7,3\}$ identical.

The number of disjoint gH is $l = 2$.

$h \in H$ $h' \in H$

$\tilde{h} \in H$ $\tilde{h} \cdot h^{-1} \cdot h' \in H$.

$H = \{h_1 \cdots h_k\}$

$H' = \{h' \cdot h_1 \cdots h' \cdot h_k\}$

WTS $H \subseteq H'$ $h_i = h' \cdot \alpha$

$(h')^{-1} \cdot h_i = \alpha \in H$.

$H \supseteq H'$ $h' \cdot h_i \in H$.

$h' h_k \in H$

$H = H'$

Example mod 15 additive situation.

$0, 1, 2, \cdots 14$ $+$

$\forall x \exists y \ (x + y = 0 \pmod{15})$

↑ neutral element

productive situation $*$

no inverse element property. ↘ ~~0~~, 1, 2 --- 14

$\forall x \in G \ \exists y \in G \ (x \cdot y = 1 \pmod{15})$

$\forall x \in G \ x * 1 = 1 * x = x \pmod{15}$.

$2 * y = 1 \pmod{15} \Leftarrow y = 8$.

$(2)^{-1} = 8$.

$3 * y = 1 \pmod{15} \Leftarrow$ impossible.

$G = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$H = \{1, 2, 4, 8\}$.

	1	2	4	8
$1 \cdot H$	1	2	4	8
$14 \cdot H$	14	13	11	7

$G = 1 \cdot H \cup 3 \cdot H = \{1, 9, 3, 7\}$

$n = l \cdot k$

$4 = 2 \cdot 2$

Example. even permutation

Let A_n be a set of all even permutation.

A_n is a subgroup of S_n.

σ_1, σ_2 $\operatorname{sgn}(\sigma_1) = 1$

$\operatorname{sgn}(\sigma_2) = 1$.

$\operatorname{sgn}(\sigma_1 \cdot \sigma_2) = \operatorname{sgn}(\sigma_1) \operatorname{sgn}(\sigma_2) = 1$.

$\operatorname{sgn}(\varepsilon) = 1 = (-1)^0$

WTS $\sigma \in A_n$ $\sigma^{-1} \in A_n$

$\operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma^{-1})$

$= \operatorname{sgn}(\sigma \cdot \sigma^{-1}) = \operatorname{sgn}(\varepsilon) = 1$.

$1 \quad \therefore \operatorname{sgn}(\sigma^{-1}) = 1$

Claim $|A_n|$ divides $|S_n|$ $\frac{n!}{2}$

$H = A_n$

$G = S_n$

$*$	A_n
$\varepsilon \cdot A_n$	A_n
WTS $\sigma \cdot A_n$	A_n

σ even.

Let $A = \{h_1 \cdots h_4\}$.

$\sigma H = \{\sigma h_1, \sigma h_2 \cdots \sigma h_4\}$

WTS $H' \subseteq H$ and $H \subseteq H'$ $H = H'$

$h = \sigma \alpha$

$\sigma^{-1} \cdot h = \alpha = (\sigma^{-1} \cdot \sigma) \alpha = \alpha$

Turns out the number of disjoint

$(14) : l = 2$

$G = (1\cdots14)(7\cdots14) \Rightarrow n = l \cdot k$ (or $14\cdots17$)

$n = 8, l = 2, k = 4$

$\sigma \cdot A_n$ (odd)

Use of Lagrange's Theorem.

1. $2^{20} \pmod{17}$

$a = 2$ ⟸ prove this is a group.

$a, a^2 \cdots a^l \cdots a^k$.

$a^l = a^k \quad k > l$

$a^l \cdot a^{-l} = a^k \cdot a^{-l} \Rightarrow 1 = a^{k-l}$ ⟸ this makes a a cyclic group

$\{1, a \cdots a^{k-1}\}$

With lagrange's theorem, k divides 17.

$k = 1$ or $k = 17$

$k = 17$ $a^{17} \equiv 1 \pmod{17}$

$2^{20} = 2^{17} \cdot 2^3 \equiv 8 \pmod{17}$

Another approach. $2^{20} = (1024)^2$

↑ compute this div 17.

2. $2^{20} \equiv ? \pmod{15}$

$\{1, 2, 2^2, 2^3 \cdots\}$

Subgroup $|2^n| = \{5, 3, 15$

either $2^5 \equiv 1 \pmod{15}$

$2^3 \equiv 1 \pmod{15}$

$2^{15} \equiv 1 \pmod{15}$

Actually $32 \equiv 2 \pmod{15}$

$8 \equiv 8 \pmod{15}$

Such that guarantee $2^{15} \equiv 1 \pmod{15}$

$$2^{20} = 2^{15} \cdot 2^5 = 32 \pmod{15}$$
$$= 2 \pmod{15}$$

In the group of $\pmod{15}$, only $|H| = 3, 5, 15$

Suppose we consider all permutations of $(1, 2, 3)$.

$|S_3| = 6 = 3!$

$H \subseteq S_3 \quad |H| = 2, 3, \underline{\text{(not 6)}}$

$|A_3| = \frac{6}{2} = 3.$ ← when $|H| = 3$

$|H| = 2 \Rightarrow (\varepsilon, \sigma)$

$\therefore \sigma * \sigma * \sigma \quad \sigma * \sigma = \varepsilon$

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

or $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

or $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$