Proof of Sylow Theorem using Grp Actions

Recall

G: finite grp

$|G| = n = p^{\alpha} \cdot m$

$p \nmid m$

(Sylow Thm)

a) Sylow p-subgrp exists.

b) All Sylow p-subgrps are conjugate to each other.

(if H_1, H_2 are both Sylow p-subgrps, then

$\exists\, \sigma \in G$ s.t $\sigma H_1 \sigma^{-1} = H_2$

c) Denote n_p to be # of Sylow p-subgrps.

① $n_p \mid m$

② $n_p \equiv 1 \pmod p$

Proof of Sylow a):

$$G \curvearrowright X = \{ \overset{\text{subset}}{S} \subseteq G \mid |S| = p^{\alpha} \}.$$

$$g * S = g \cdot S$$

$$|X| = \binom{p^{\alpha} \cdot m}{p^{\alpha}}$$

We claim that. when $p \nmid m$ $\binom{p^{\alpha} \cdot m}{p^{\alpha}} \not\equiv 0 \pmod p$.

Ex ↑: Hint: count powers of p in numerator and denominator.

$$\frac{p^{\alpha} \cdot m\,(p^{\alpha} \cdot m - 1) \cdots\cdots (p^{\alpha} \cdot m - p^{\alpha} + 1)}{p^{\alpha} \cdot (p^{\alpha} - 1) \cdots\cdots 1}$$

By Stabilizer - Orbit Formula.

$$|X| = \sum_{O} |O| = \sum_{O} \frac{|G|}{|Stab(x)|} \not\equiv 0 \pmod p$$

pick $x \in O$

If $\forall x \in X$ $|Stab(x)|$ is exactly contains $p^{\alpha-1}$ in the size. as the factor at p. then. it contradicts with. $|X| \not\equiv 0 \pmod p$)

$\Rightarrow \exists O$ s.t. $p^{\alpha} \mid |Stab(x)|$

$x = S \subseteq G$ is a certain subset of G

$H = Stab(x)$ $\longrightarrow$ $S = \{ s_1, \cdots, s_{p^{\alpha}} \}$

$|S| = p^{\alpha}$ $\qquad Stab(s_i) = \{ h \in H \mid h \cdot s_i = s_i \}$
$= \{e\}$

$$\underset{p^{\alpha}}{\overset{\|}{|S|}} = \sum_{O} |O| = \sum_{O} \frac{|H|}{|Stab(s_i)|} = \sum_{O} |H| = \underline{|H|} \cdot |O|$$

$s_i \in O$

$\Rightarrow |H| \mid p^{\alpha}$

$\Rightarrow |H| = p^{\alpha}$.

$\square$.

Proof of Sylow (b).

Suppose H_1 H_2 are two Sylow p subgrps,

$$H_1 \curvearrowright X = \{ \text{left cosets of } H_2 \}$$

$$h_1 * gH_2 = (h_1 g) \cdot H_2$$

$$\begin{tikzcd} H \arrow[r] \arrow[rr, bend left] & G \arrow[r] & Per(X) \end{tikzcd}$$

$$|X| = \frac{|G|}{|H_2|} = m \not\equiv 0 \pmod p$$

$$\Vert$$

$$\sum_{O} |O| = \sum_{O} \frac{|H_1|}{\underset{x \in O}{|Stab(x)|}} \not\equiv 0 \pmod p$$

$\Rightarrow \exists\, O$ s.t. $Stab(x) = H_1$

$$\Updownarrow$$

suppose $x = g \cdot H_2$

$$H_1 \cdot gH_2 = gH_2$$

$$\Updownarrow$$

$$g^{-1} H_1 \cdot g H_2 = H_2$$

$$\Updownarrow$$

$$g^{-1} H_1 g \subseteq H_2$$

$$\Downarrow$$

$$g^{-1} H_1 \cdot g = H_2 \quad \text{since } |H_1| = |H_2|$$

$\square$.

Proof of Sylow (c)

$$G \curvearrowright X = \{ \text{all Sylow } p\text{-subgrps} \}$$

$$g * H = gHg^{-1}$$

by Sylow (b). G acts transitively on X.

$$|X| = |O| = \frac{|G|}{|\mathrm{Stab}(x)|} = d \mid m.$$

$\forall x \in X$

Say $x = H$

$\mathrm{Stab}(H) = \{ g \in G \mid g \cdot H g^{-1} = H \}$ = normalizer of H

$\Updownarrow$

the largest subgrp M of G s.t. $H \triangleleft M$.

Observe

$H \subseteq \mathrm{Stab}(H) \subseteq G$

$\Rightarrow$ ① $n_p \mid m$.

Let H be a Sylow p-subgrp.

$$H \overset{\text{conj.}}{\curvearrowright} X = \{ \text{all Sylow-}p \text{ subgrp} \}$$

$n_p = \sum_O |O|$

For example: the orbit of H is H ✓.

$\mathrm{Stab}(H) = H$

$|O| = 1$

$hHh^{-1} = H$

For other Sylow-p subgrp, say $H_1 \neq H \in X$.

$$\mathrm{Stab}(H_1) = \{ h \in H \mid h \cdot H_1 \cdot h^{-1} = H_1 \} = H \cap \mathrm{Norm}(H_1)$$

Our goal is to show that $n_p \equiv 1 \bmod p$.

Notice that. $\dfrac{|H|}{|\mathrm{Stab}(x)|}$ is a divisor of $|H|$.

which is $\not\equiv 0 \bmod p$ only when $\mathrm{Stab}(x) = H$.

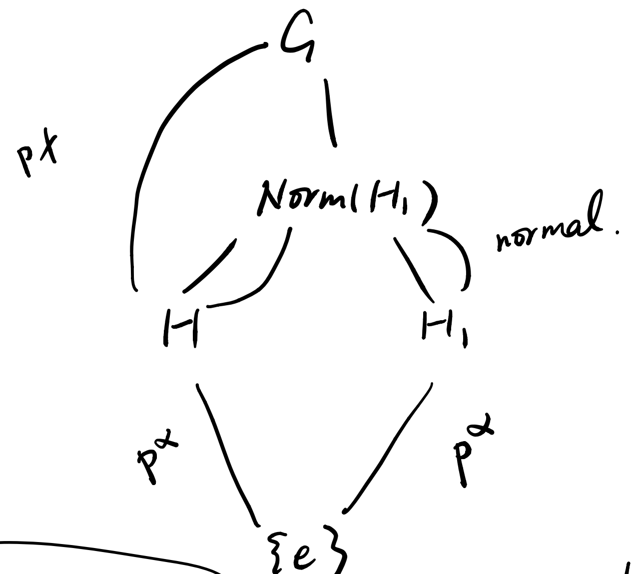
$\Downarrow$

$|O| = 1$

If $\mathrm{Stab}(H_1) = H$ then. $H \cap \mathrm{Norm}(H_1) = H$

$\Downarrow$

$H \subseteq \mathrm{Norm}(H_1)$



H, H_1 are both Sylow-p subgrps of $\mathrm{Norm}(H_1)$

but Sylow (b) tells us that H and H_1 are conjugate to each other in $\mathrm{Norm}(H_1)$, condicts with $H_1 \triangleleft \mathrm{Norm}(H_1)$

$\exists \sigma \in \mathrm{Norm}(H_1)$ $\sigma H_1 \sigma^{-1} = H$

$\sigma H_1 \sigma^{-1} = H_1 \ \forall \sigma \in \mathrm{Norm}(H_1)$

$\Rightarrow H = H_1$

$$\Rightarrow \sum_{O} |O| = 1 + \sum_{\substack{O \\ H \notin O}} |O| = 1 + \sum_{O} \text{positive } p\text{-powers} \equiv 1 \bmod p.$$

$\square$

Example: Find all grps with order 15.

$15 = 5 \times 3$. $\quad G_5 = (\mathbb{Z}_5, +)$

$G_3 = (\mathbb{Z}_3, +)$

How many. $G_5 = ?$ $\quad \begin{cases} n_5 \equiv 1 \mod 5 \\ n_5 \mid 3 \end{cases} \Rightarrow n_5 = 1$

$\begin{cases} n_3 \equiv 1 \mod 3 \\ n_3 \mid 5 \end{cases} \Rightarrow n_3 = 1$

We have found all subgrps of G.

Lemma: If N, H are both normal in G. and

1) $N \cap H = \{e\}$.

2) $N \cdot H = G$.

then $G = N \times H$.

Ans: $G = C_5 \times C_3 = C_{15}$.

$|G| = n = P_1 \cdot P_2$ where. $\quad P_1 \not\equiv 1 \mod P_2$. $\quad (P_1 \neq P_2)$

$P_2 \not\equiv 1 \mod P_1$

then $G = C_{P_1 \cdot P_2}$