4. The Sylow Theorems

Recall Lagrange's thm: If $H \leq G$ and $|H| = m$, $|G| = n$, then $m \mid n$.

Does the converse hold? i.e, If $|G| = n$ and $m \mid n$, does there exist a subgroup of order m?

In general, no. But sometimes yes.

<u>Def:</u> Say $|G| = n < \infty$, p prime. Then a <u>p-Sylow subgroup</u> (or <u>Sylow p-subgroup</u>) is a subgroup $P \leq G$ s.t. $|P| = p^k$ is the highest power of p that divides $|G|$.

<u>Notation:</u> Write $p^k \| |G| \iff p^k \mid |G|$ but $p^{k+1} \nmid |G|$.

<u>Thm 4.1</u> (1st Sylow thm): Let $|G| < \infty$, p prime. Then G has a p-Sylow subgroup.

<u>Pf:</u> Induction on $|G|$. Suppose $|G| = p^k m$.

If $|G| = 1$ or $p \nmid |G|$, then $P = 1$ is p-Sylow.

Assume $p \mid |G| > 1$, and the thm holds for all smaller groups.

<u>Case 1:</u> $\exists\, H \lneq G$ s.t. $p \nmid [G:H]$. (Equivalently, $p^k \mid |H|$.)

By IHOP, H has a p-Sylow subgp $P \leq H$, which is also p-Sylow in G. ✓

<u>Case 2:</u> $\forall\, H \lneq G$, $p \mid [G:H]$. (Equivalently $p^k \nmid |H|$ for all $H \lneq G$).

We will show this can't happen.

By class equation: $|G| = |Z(G)| + \sum_{i=1}^{r} |cl(x_i)|$
$= |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]$

Since $p \mid |G|$ and $p \mid [G : C_G(x_i)]$ (by assumption), $p \mid |Z(G)|$.

By Cauchy, $\exists$ elt $x \in Z(G)$ of order p. Set $K = \langle x \rangle$.

Since $x \in Z(G)$, $K \trianglelefteq G$.

<u>Note</u>: Since $p^k \| |G|$, $p^{k-1} \| |G/K|$.

By IHOP, G/K has a p-Sylow subgp P_1 of order p^{k-1}.

$P_1 = P/K$, where $P \le G$ (By ~~Correspondence thm~~: Prop. 1.12 & Cor)

Also, $|P| = |P_1|\,|K| = p^k \Rightarrow P$ is p-Sylow in G ($\&$ $p \nmid [G:P]$) $\lightning$ $\square$

<u>Exercise</u> If $|G| = p^n$, p prime, then G has subgps

$$1 = G_0 \le G_1 \le \cdots \le G_n = G \quad \text{s.t. } [G_i : G_{i-1}] = p.$$

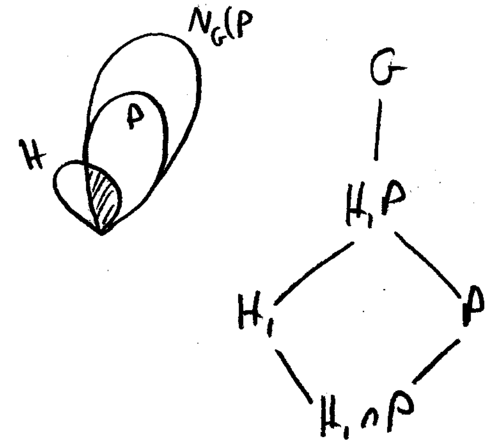
<u>Pf</u>: HW #3 (use induction, as above).

<u>Cor</u> If $p^i \mid |G|$, then G has a subgp of order p^i.

<u>Def</u>: If every elt of G has order a power of p, then G is a <u>p-group</u>.

<u>Exercise</u>: Show G is a finite p-group $\Longleftrightarrow |G| = p^n$.

<u>Prop 4.2</u>: Let $P \leq G$ be a p-Sylow subgroup, & $H \leq G$ be a p-group. Then $H \cap N_G(P) = H \cap P$.



<u>Pf</u>: Let $H_1 = H \cap N_G(P)$.

Clearly, $H \cap P \leq H_1$, & $H_1 \leq N_G(P)$.

By Isom. thm (2.6), $H_1P/P \cong H_1/(H_1 \cap P)$

Since $H_1 \leq H$, H_1 is a p-group: $p^r = [H_1P : P] = [H_1 : H_1 \cap P]$

<u>Goal</u>: Show that $H_1P = P$, i.e., that $r = 0$.

$|H_1P| = [H_1P : P] \cdot |P| = p^r |P|$.

But H_1P is a p-group and P is p-Sylow, so

$p^k = |P| \leq |H_1P| \leq p^k \implies H_1P = P \implies H_1 \leq P$.

Thus $H_1 = H \cap N_G(P) \leq P \implies H \cap N_G(P) = H \cap P$. $\square$

<u>Thm 4.3</u> (2^{nd} Sylow thm): Let $|G| < \infty$, p prime, $P \leq G$ a p-Sylow subgp, and $H \leq G$ a p-group. Then $H \leq xPx^{-1}$ for some $x \in G$

(In particular, "all p-Sylow subgps are conjugate")

<u>Pf</u>: Let $S = \{xPx^{-1} : x \in G\}$.

H acts on S by conjugation: $h \bullet xPx^{-1} = hxPx^{-1}h^{-1}$.

Let $\mathcal{O}_1, \dots, \mathcal{O}_r$ be the orbits.

Pick $P_i \in \mathcal{O}_i$. Note that $\mathrm{Stab}_H(P_i) = \{h \in H : h^{-1}P_ih = P_i\} = H \cap N_G(P_i)$

$= H \cap P_i$ (Prop 4.2)

④

<u>Goal</u>: show that $|\mathcal{O}_i| = 1$ for some i.

Orbit-Stabilizer thm $\Rightarrow$ $|\mathcal{O}_i| = [H : \mathrm{Stab}_H(P_i)] = [H : H \cap P_i]$

<u>Note</u>: $|S| = |\{xPx^{-1} : x \in G\}|$

To count this, let G act on $\{xPx^{-1} : x \in G\}$ by conjugation.

This is clearly transitive (i.e., 1 orbit), & $\mathrm{Stab}_G(P) = \{x : xPx^{-1} = P\} = N_G(P)$

$|S| = [G : \mathrm{Stab}_G(P)] = [G : N_G(P)]$.

We now have: • $|S| = [G : N_G(P)]$

• $\underset{\text{p-Sylow}}{P} \leq N_G(P) \Rightarrow p \nmid [G : N_G(P)] \Rightarrow p \nmid |S|$.

Thus, $|S| = \sum_{i=1}^{r} |\mathcal{O}_i| = \sum_{i=1}^{r} \underbrace{[H : H \cap P_i]}_{= p^{k_i}} = \sum_{i=1}^{r} p^{k_i}$.

But $p \nmid |S| \Rightarrow |\mathcal{O}_i| = 1$ for some i.

For this i, $[H : H \cap P_i] = 1 \Rightarrow H = H \cap P_i \Rightarrow H \leq P_i$.

i.e., $H \leq x_i P x_i^{-1}$ for some $x_i \in G$. $\square$

<u>Cor</u>: If $|G| < \infty$ and $\exists!$ p-Sylow subgp $P \leq G$, then $P \trianglelefteq G$.

<u>Def</u>: If $|G| < \infty$, p prime, let n_p = # of p-Sylow subgps of G.

<u>Note</u>: G acts transitively on $S = \{xPx^{-1} : x \in G\}$, since all p-Sylow subgps are conjugate,

$n_p = |S| = [G : \mathrm{Stab}_G(P)] = [G : N_G(P)] \mid |G|$.

Thm 4.4 (3^{rd} Sylow thm): $n_p \equiv 1 \pmod p$

PF: let $P \leq G$ be p-Sylow, and let $S = \{xPx^{-1} : x \in G\}$

let P act on S by conjugation, with orbits $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$.

Note: $\{P\}$ is a size-1 orbit (say it's $\mathcal{O}_1$).

Goal: $p \mid |\mathcal{O}_i| \quad \forall i \geq 2$.

If $P_i \in \mathcal{O}_i$ for $i \geq 2$, then $P_i \neq P$, and

$\mathrm{Stab}_P(P_i) = \{x \in P : xP_ix^{-1} = P_i\} = P \cap N_G(P_i) = P \cap P_i \neq P$ (Prop 4.2).

Thus $|\mathcal{O}_i| = [P : P \cap P_i]$ is divisible by p if $2 \leq i \leq r$ ✓

Now, $|S| = |\mathcal{O}_1| + \sum_{i=2}^{r} |\mathcal{O}_i| \equiv 1 + \underbrace{\sum_{i=2}^{r} |\mathcal{O}_i|}_{\text{divisible by } p} \equiv 1 \pmod p$ □

Note: If $|G| = p^k m$, where $p \nmid m$, then $n_p \nmid p \Rightarrow n_p \mid m$.

In summary, $\boxed{\begin{array}{l} n_p \equiv 1 \pmod p \\ n_p \mid m \mid |G| \end{array}}$

Note: G acts transitively on $\{xPx^{-1} : x \in G\}$ if $P \leq G$ is p-Sylow,

thus $n_p = |\{xPx^{-1}\}| = [G : \mathrm{Stab}_G(P)] = \boxed{[G : N_G(P)] = n_p}$

Applications of Sylow theorems

[1] Suppose $|G| = 28 = 2^2 \cdot 7$.

Then $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 4 \Rightarrow n_7 = 1$.

Thus $\exists!$ 7-Sylow subgroup $P \lhd G$, and G is not simple.

[2] Suppose $|G| = pq$, both primes $q < p$, $\underbrace{p \not\equiv 1 \pmod q}_{\text{will use to show } G \text{ cyclic}}$

$n_p \equiv 1 \pmod p \Rightarrow n_p = 1 + kp \mid q \Rightarrow k = 0$ & $\boxed{n_p = 1}$ (since $q < p$).

Thus $\exists!$ p-Sylow subgp $P \lhd G$.

$n_q \equiv 1 \pmod p \Rightarrow n_q = 1 + mq \mid p \Rightarrow 1 + mp = 1$ or $\underbrace{1 + mq = p}_{\substack{\text{impossible, since} \\ p \not\equiv 1 \pmod q}}$

Thus $n_q = 1 + mq = 1 \Rightarrow m = 0$ & $\boxed{n_q = 1}$

Thus $\exists!$ q-Sylow subgp $Q \lhd G$.

Say $P = \langle x \rangle$, $Q = \langle y \rangle$.

$$x^{-1}\underbrace{y^{-1}xy}_{\in P} = \underbrace{x^{-1}y^{-1}x}_{\in Q}y \in P \cap Q = 1 \Rightarrow x^{-1}y^{-1}xy = 1 \Rightarrow xy = yx.$$

Thus, $|xy| = pq$ and $G = \langle xy \rangle$ is cyclic.

[3] Suppose $|G| = 56 = 2^3 \cdot 7$. $n_7 \equiv 1 \pmod 7$ & $n_7 \mid 8 \Rightarrow n_7 = 1$ or 8.

If $n_7 = 1$, then G is not simple.

If $n_7 = 8$, then $\exists\ 8 \cdot 6 = 48$ elts in G of order 7.

But that leaves 8 elements in the 2-Sylow subgps (which have order 8).

Therefore, $n_2 = 1$, so G is not simple.

4 Say $|G| = p^2 q$ (See D & F p. 144).

Claim: G is not simple.

Case 1: $p > q$. Let $P \leq G$ be p-Sylow. Then $[G:P] = q$, the smallest prime dividing $|G|$ $\Rightarrow$ $P \trianglelefteq G$ (see HW #2).

Case 2: $p < q$. Assume $n_q > 1$. Then $n_q = 1 + tq \mid p^2 \Rightarrow n_q = p$ or p^2.

Since $p < q$, $n_q \neq p \Rightarrow n_q = p^2$.

Thus, $tq + 1 = p^2 \Rightarrow tq = (p-1)(p+1)$

q prime $\Rightarrow$ $\underbrace{q \mid p-1}_{\text{impossible since } p<q}$ or $\underbrace{q \mid p+1}$.

$\Rightarrow q = p+1 \Rightarrow p = 2,\ q = 3. \Rightarrow |G| = 12$

It remains to show that if $|G| = 12$, then G is not simple.

$12 = 2^2 \cdot 3 \Rightarrow n_2 = 1$ or 3

Assume $n_2 = 3$, and $P < G$ be 2-Sylow.

Then $[G:P] = 3$.

If G were simple, then it has no subgroup of index 2.

But then any subgroup of index 3 is normal (see HW #2)

Hence G can't be simple.

<u>Prop 4.5</u>: If G is simple & $|G| = 60 = 2^2 \cdot 3 \cdot 5$, then $G \cong A_5$.

<u>Pf:</u> Recall HW 2: G can't have a subgroup of index ≤ 4.

(e.g., if $[G:H] = 4$, then since $60 \nmid 4!$, $\exists\, \phi: G \longrightarrow S_4$ & $\ker\phi \trianglelefteq G$).

$n_5 \equiv 1 \pmod 5$ & $n_5 \mid 12 \implies \boxed{n_5 = 6}$

$n_3 \equiv 1 \pmod 3$ & $n_5 \mid 20 \implies \boxed{n_3 = 10}$

$n_2 \equiv 1 \pmod 2$ & $n_2 \mid 15 \implies \boxed{n_2 = 3, 5, \text{ or } 15}$

If $n_2 = 3$ then $[G : N_G(P)] = 3$ (where $P \leq G$ is 2-Sylow) $\lightning$

<u>If $n_2 = 5$</u>, then $[G : N_G(P)] = 5$.

$G \curvearrowright G/N_G(P)$, so $\exists\, \phi: G \hookrightarrow S_5$

If $\phi(G) \not\leq A_5$, then $[\phi(G) : A_5 \cap \phi(G)] = 2$ (see HW #2).

Then $A_5 \cap \phi(G) \trianglelefteq \phi(G) \implies \phi^{-1}(A_5 \cap \phi(G)) \trianglelefteq G$ (Correspondence thm/ Prop 1.12)

So $\phi: G \hookrightarrow A_5 \implies G \cong A_5$.

Next, <u>suppose $n_2 = 15$</u>.
If all 2-Sylow subgroups intersect trivially, then $\exists\, (4-1)\cdot 15 = 45$ non-identity elts in them (of order 2 or 4).
But the 5-Sylow subgps contain $(5-1)\cdot 6 = 24$ elts of order 5.

But $45 + 24 > 60$ $\lightning$.
So $\exists\, P, Q \leq G$, 2-Sylow, such that $|P \cap Q| = 2$.

Let $M = N_G(P \cap Q)$.

$$\left.\begin{array}{l} \bullet\ P, Q \leq M \Rightarrow 4 \mid |M|. \\ \bullet\ P \cup Q \subseteq M \Rightarrow |M| > 4. \\ \bullet\ M \neq G \ \&\ [G:M] \leq 5 \end{array}\right\} \Rightarrow |M| = 12, \ \&\ [G:M] = 5.$$

Again, $G \curvearrowright G/M$, and the same argument shows

$\exists\, \phi : G \hookrightarrow A_5 \Rightarrow G \cong A_5$ $\lightning$