Group Theory
Week #7, Lecture #26

Setup: • G finite group
• p prime, $p \mid G$
• $|G| = p^k m$, $p \nmid m$

Lemma If P is a normal p-Sylow subgroup of G, then P contains every p-subgroup of G.

Proof • Let $H \leq G$, $|H| = p^r$ for some $r \geq 1$. Let $\boxed{a \in H}$. Then the order of a divides the order of H (by Lagrange), and so $o(a)$ is also a power of p.

- Since $P \trianglelefteq G$ by assumption, we may view the left coset aP as an element of the factor group, G/P.
- Note that $(aP)^{o(a)} = a^{o(a)}P = eP = P$.

  Thus, $o(aP)$ divides $o(a)$, and so it is also a power of p.
- On the other hand,

  $o(aP) \mid |G/P| = [G:P] = m$ (again by Lagrange),

  which is coprime to p (since $P \in Syl_p(G)$)
- Hence: $\boxed{o(aP) = 1}$, which means $aP = P$, or, $\boxed{a \in P}$

  This shows $H \leq P$

$\boxed{\text{QED}}$

Theorem (Sylow II) All p-Sylow subgroups of G are conjugate.

Proof Let $P \in Syl_p(G)$. Let

$\{$all p-Sylow subgroups of $G\}$ — also p-Sylow!

$$Syl_p(G) \supseteq \boxed{S = \{\text{conjugate subgroups of } P\} = \{Q \leq G : Q = gPg^{-1}, \text{ for some } g \in G\}}$$

and consider the conjugation action of the group P on the set S

$$P \times S \longrightarrow S \qquad (x, Q) \longrightarrow xQx^{-1}$$

Ex 1 If $P \trianglelefteq G$, then $gPg^{-1} = P$, $\forall g \in G$, and so $S = \{P\}$

Ex 2 If $G = S_3$, $p = 2$, and $P = \langle (1,2) \rangle \cong \mathbb{Z}_2$, then

$S = \{\langle (1,2)\rangle, \langle (1,3)\rangle, \langle (2,3)\rangle\}$

(12) (12)

(the generator (12) of P fixes P and interchanges the other 2-sylow subgroups)

Step 1 (a) Suppose Q is fixed by P, i.e., $P \leq N(Q)$. Then:

- $|Q| = |P| = p^k$ (Conjugate subgroups have same order)
- $p \nmid m = [G:Q]$ (by assumption)
- $[G:Q] = [G:N(Q)] \cdot [N(Q):Q]$ (by properties of index)

Hence: $\boxed{p \nmid [N(Q):Q]} \Rightarrow \boxed{Q \in Syl_p(N(Q))}$

But we also know that $\boxed{Q \trianglelefteq N(Q)}$ (always the case!)

Hence, by the Lemma: $\circledast$ $\boxed{Q \text{ contains all } p\text{-subgroups of } N(Q)}$

(b) Now recall our assumption in Step 1: $P \leq N(Q)$

Thus, by $\circledast$: $P \leq Q$ (since P is a p-group)

But $|P| = |Q|$, and thus $\boxed{P = Q}$

So we showed: $(\cdot)$ $\boxed{S^P = \{P\}}$ (the only $Q \in S$ fixed by conj. action of P is P)

(c) We use now the Class Equation for p-groups acting on sets:

$$\boxed{|S| \equiv |S^P| \pmod p}$$

But $|S^P| = 1$ by $(\cdot)$, and so we conclude that

$$\boxed{|S| \equiv 1 \pmod p} \quad (\cdot\cdot)$$

Step 2. Now let Q be any p-Sylow subgroup of G, and consider the conjugation action of Q on the same set S as above.

- Again by the Class Equation for p-group actions:

$$\underset{\underset{1}{\parallel\!|}\,(\cdot\cdot)}{|S|} \equiv |S^Q| \pmod p$$

$\leftarrow$ by Step 1

- So $|S^Q| \equiv 1 \pmod p$, in particular, $S^Q \neq \emptyset$.
  Hence, $\exists K \in S^Q$ such that $xKx^{-1} = K$, $\forall x \in Q$, ie.,
  $\boxed{Q \subseteq N(K)}$ (**)

- But $K \trianglelefteq N(K)$ [always!], and also $|K| = |P| = p^k$
  since $K \in S$ is a conjugate of P

  and so $\boxed{K \text{ is a normal p-Sylow subgroup of } N(K)}$ (***)

- Applying the Lemma to (**) and (***), we get:
  $\boxed{Q \subset K}$ $\leftarrow$ (Q is a p-group in $N(K)$, K normal p-Sylow in $N(K)$)

- But again $|Q| = |K| = p^k \Rightarrow \boxed{Q = K}$

- Finally, recall $K \in S^Q \subset S = \{\text{conjugates of } P\}$, and so
  Q is also a conjugate of P.

QED

Theorem (Sylow III) For each prime $p \mid |G| = p^k m$, the number $n_p = n_p(G)$ of p-Sylow subgroups of G satisfies:

$$\boxed{\begin{array}{ll} \cdot\ n_p \equiv 1 & (\text{mod } p) \\ \cdot\ n_p \mid m & \end{array}}$$

Proof Let $P \in Syl_p(G)$, and $S = \{gPg^{-1} : g \in G\}$.
By Sylow II: $\boxed{S = Syl_p(G)}$, and so $\boxed{n_p = |S|}$

Step 1 Consider the conjugation action of P on S.
By Class Eq for p-groups: $|S| \equiv |S^P| \pmod p$

$\therefore$ $\boxed{n_p \equiv 1 \pmod p}$ ✓

Step 2 Now consider the conjugation action of G on S.
By Sylow II, the orbit $G\cdot P$ is all of S. Hence:

$$\boxed{n_p = |S| = |G\cdot P| \underset{\substack{\uparrow \\ \text{Orbit-Stabilizer Thm}}}{=} [G:G_P] \underset{\substack{\uparrow \\ \text{by def of normalizer}}}{=} [G:N(P)]} \quad (*)$$

Now:

$$m \underset{\substack{\uparrow \\ P \text{ is } p\text{-Sylow}}}{=} [G:P] = [G:N(P)]\cdot[N(P):P] \underset{\substack{\uparrow \\ \text{by } (*)}}{=} n_p \cdot [N(P):P]$$

$\therefore \boxed{n_p \mid m}$ ✓

QED

Remarks / consequences of Sylow I–III

① If $n_p = 1$, then there is a single p-Sylow subgroup, and that subgroup must be normal (and conversely):

$$\boxed{n_p(G) = 1 \iff \left(\mathrm{Syl}_p(G) = \{P\} \;\&\; P \trianglelefteq G\right)}$$

$$\left(\begin{array}{l} P \ntrianglelefteq G \iff \exists g \in G \text{ s.t. } gPg^{-1} \neq P \\ \qquad\qquad\qquad \Updownarrow \qquad\qquad \uparrow \text{Sylow II} \\ \qquad\qquad\quad |S| > 1, \text{ i.e., } n_p \neq 1 \end{array} \right)$$

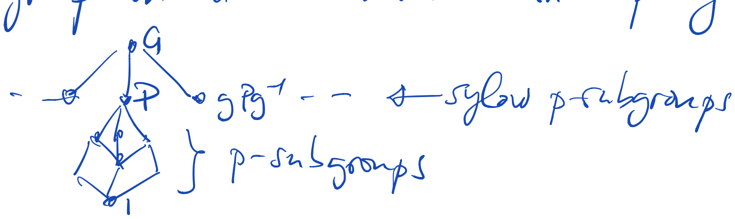
② To re-emphasize the point of Sylow II:

$$\boxed{\mathrm{Syl}_p(G) = \{\text{conjugates of } P \text{ in } G\}}$$

(where P is any p-Sylow subgroup, which exists by Sylow I)

③ Every p-subgroup in G is contained in a p-Sylow.

schematic:



That is, p-Sylow subgroups are maximal among all p-subgroups of G (but not necessarily among all subgroups)

Examples / Applications

- One of the main apps. of Sylow theory is to show that certain large classes of finite groups are <u>not</u> simple, i.e., contain no non-trivial, proper normal subgroups.

- Basic idea: try to find $p \mid |G|$ such that $n_p = 1$, which then implies $\exists P \trianglelefteq G$ (by rem 1) and so done. (Usually start with largest $p \mid G$)

- Otherwise, determine a short list of $\{n_p : p \mid G\}$ and use other facts from group theory to find $1 \neq N \underset{\neq}{\trianglelefteq} G$.

Ex 1 $|G| = 100 = 2^2 \cdot 5^2$ not simple

Sylow III: $n_5 \equiv 1 \pmod 5$ & $n_5 \mid 4$

$\Updownarrow$

$n_5 = 1, 2, \text{or } 4$

$\therefore n_5 = 1$

Hence G is not simple (by Rem. 1)

Ex 2 $|G| = 28 = 2^2 \cdot 7$ not simple

$n_7 \equiv 1 \pmod 7$ & $n_7 \mid 4 \Rightarrow n_7 = 1$ ✓

Ex 3 $|G| = 24 = 2^3 \cdot 3$ not simple

- $n_3 \equiv 1 \pmod 3$ & $n_3 \mid 8 \implies n_3 = 1$ or 4

  ($n_3 \in \{1,2,4,8\}$)

- $n_2 \equiv 1 \pmod 2$ & $n_2 \mid 3 \implies n_2 = 1$ or 3

[Aside: $|S_4| = 24$ and $n_2 = 3$, $n_3 = 4$
so has no normal sylows
but it is still not simple – it has normal, non-Sylow subgroups
Note: $Syl_2(S_4)$ & $Syl_3(S_4)$ computed last time]

If $n_2 = 1 \to$ done

Suppose $n_2 = 3$, so $\mathcal{S} = Syl_2(G) = \{P, Q, R\}$

2-Sylows, all conjugate (of size 8)

Consider the conjugation action of G on $\mathcal{S}$. By Sylow II: $\boxed{G \cdot P = \mathcal{S}}$ (*)

(the action is transitive, i.e., it has a single orbit)

This action has an associated hom,

$$\boxed{\varphi : G \longrightarrow Sym(\mathcal{S}) = S_3}$$

But

$$|G| = 24 > 6 = 3! = |S_3|$$

so $K := ker(\varphi) \neq \{e\}$ (otherwise, $G \cong \varphi(G)$, a subgroup of S_3)

But also $K \neq G$, since otherwise φ is the trivial hom, and so the action of G on $\mathcal{S}$ is trivial, i.e. $G \cdot x = \{x\}$, for all $x \in \mathcal{S}$. But this contradicts (*), which says $G \cdot P = \mathcal{S}$, so orbits have size 3, not 1.

$\therefore 1 \neq K \underset{\neq}{\trianglelefteq} G$ is a nontrivial, proper subgroup

QED

Ex 4 $|G| = 72 = 8\cdot 9 = 2^3\cdot 3^2$ not simple

- $n_3 \equiv 1 \pmod 3$ & $n_3 | 8$ $\Longrightarrow n_3 = 1$ or 4
- $n_2 \equiv 1 \pmod 2$ & $n_2 | 9$ $\Longrightarrow n_2 = 1, 3,$ or 9
- If either $n_2 = 1$ or $n_3 = 1$ — done (by Remark)
- If $n_3 = 4$, then get transitive rep from Sylow II, with $S = \{P, Q, R, T\}$

$$\varphi : G \longrightarrow Sym(S) = S_4$$

But $|G| = 72 > 24 = 4! = |S_4|$

so $K := \ker(\varphi) \trianglelefteq G$ is nontrivial, and also proper subgroup, by transitivity of the action — done

---

Note: The method from Examples 3 & 4 works if $|G| = p^k\cdot m$ and $p^k\cdot m > m!$

Ex 5 $|G| = 12 = 2^2\cdot 3$ not simple

- $n_3 \equiv 1 \pmod 3$ & $n_3 | 4$ $\Longrightarrow n_3 = 1$ or 4
- $n_2 \equiv 1 \pmod 2$ & $n_2 | 3$ $\Longrightarrow n_2 = 1$ or 3

note: · for $p = 3$, $m = 4$: $12 \not> 4!$ — so neither of the above methods works!

· for $p = 2$, $m = 3$: $12 > 3!$ — so second method works — try it!

Suppose $n_3 = 4$. Then all 3-Sylows are cyclic of order 3 (since every group of order p is cyclic), and so they cannot intersect except at e.

So $t_3 = 4\cdot(3-1) = 8$

Hence, there are only 4 elements left in G (the identity & 3 others); so they must comprise a 2-Sylow subgroup, which must be unique, i.e., $n_2 = 1$

Ex 6 $|G| = 30 = 2 \cdot 3 \cdot 5$

- $n_2 \equiv 1 \pmod{2}$, $n_2 \mid 15 \Rightarrow n_2 = 1, 3, 5,$ or 15
- $n_3 \equiv 1 \pmod{3}$, $n_3 \mid 10 \Rightarrow n_3 = 1$ or 10
- $n_5 \equiv 1 \pmod{5}$, $n_5 \mid 6 \Rightarrow n_5 = 1$ or 6

- Suppose $n_3 \neq 1$ i.e., $n_3 = 10$

  if P & Q are distinct 3-Sylows (of order 3), then

  $P \cap Q = \{e\}$ (since $|P \cap Q| \mid 3$ and $P \cap Q \neq P$)

  so $t_3 = 10 \cdot 2 = 20$

- Suppose also that $n_5 \neq 1$, i.e., $n_5 = 6$. Then

  $t_5 = 6 \cdot 4 = 24$

  Thus, if $n_3 \neq 1$ & $n_5 \neq 1$, then

  $t_3 + t_5 = 20 + 24 = 44 > 30$ — contradiction

$\therefore$ Either $n_3 = 1$ or $n_5 = 1$ QED