Lecture XVII: Applications of Sylow Theorems III

Sylow Theorems: G finite group, $p \mid |G|$ prime. Then,

(1) Sylow p-groups exist

(2) Sylow p-subgroups are unique up to conjugation

(3) $n_p = \#$ Sylow p-subgroups of G $\quad n_p \equiv 1 \mod (p)$ $\quad \&$ $\quad n_p \mid |G|$.

Corollary: $n_p = 1$ & G not a p-group $\Rightarrow$ any Sylow p-subgroup of G is normal.

§17.1 Simple groups:

Definition: A group G is called simple if it has no non-trivial, proper, normal subgroups.

Proposition: Any p-group G of size $|G| > p$ is not simple.

Q: How can we ensure a finite non p-group is not simple? There are 3 main tricks.

- **First trick:** Show $n_p = 1$ for some p via Sylow Thm (3)

  Example 1: $|G| = 28 \Rightarrow G$ is not simple because $n_7 = 1$.

- **Second trick:** Use $G \circlearrowright \mathrm{Syl}_p(G)$ by conjugation & show $\ker \varphi \neq \{e\}, G$ for $\varphi : G \longrightarrow \mathrm{Aut}_{Set}(\mathrm{Syl}_p(G)) \subseteq S_{n_p}$ $\quad \varphi(g) = \mathrm{Conj}(g)$.

  Example 2: Prove that there are no simple groups of order 224.

  Solution: Write $|G| = 224 = 2^5 \cdot 7 \Rightarrow$ only Sylow 2- and 7-subgroups.

  - $n_2 \equiv 1 \pmod 2$ $\quad \&$ $\quad n_2 \mid 7$ $\quad \Rightarrow$ $\boxed{n_2 = 1 \text{ or } 7}$
  - $n_7 \equiv 1 \pmod 7$ $\quad \&$ $\quad n_7 \mid 32$ $\quad \Rightarrow$ $n_7 = 1$ or 8

  - If $n_2 = 1$, we conclude G is not simple. (! Sylow 2-subgroup is normal)
  - If $n_2 = 7$, we use $G \circlearrowright \mathrm{Syl}_2(G) =: X$ by conjugation $\quad |X| = 7$.

    We have a group homomorphism induced by this action

$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Aut}_{Set}(X) \subseteq S_7 \\ g &\longmapsto \mathrm{Conj}(g) \end{aligned}$$

If φ is injective, then $G \simeq \mathrm{Im}\,\varphi \leq S_7$ So $|G| = |\mathrm{Im}\,\varphi| \mid |S_7| = 7!$,
ie $224 \mid 7! \iff 32 \mid 6! = 16 \cdot 9 \cdot 5$ Contr!

$\Rightarrow \varphi$ is not injective, so $\{e\} \neq \mathrm{Ker}\,\varphi \trianglelefteq G$.

• Claim: $\mathrm{Ker}\,\varphi \neq G$ because $\exists g \in G$: $\mathrm{Conj}(g)(P_0) = g P_0 g^{-1} \notin P_0$ $(P_0 \ntrianglelefteq G)$ for any $P_0 \in \mathrm{Syl}_2(G)$.

We conclude: $\mathrm{Ker}\,\varphi \neq \{e\}, G$ & $\mathrm{Ker}\,\varphi \triangleleft G$, ie G is NOT simple.

• Third trick: Show $n_p = 1$ for some p by overcounting.

Example 3: Prove that there are no simple groups of order 56.

Solution: Write $|G| = 56 = 2^3 \cdot 7 \Rightarrow$ only Sylow 2- and 7-subgroups.

• $n_2 \equiv 1 \pmod 2$ & $n_2 \mid 7 \Rightarrow n_2 = 1$ or 7

• $n_7 \equiv 1 \pmod 7$ & $n_7 \mid 8 \Rightarrow \boxed{n_7 = 1 \text{ or } 8}$

If $n_7 = 1$, we are done (G cannot be simple by Sylow Thm (2))

If $n_7 = 8$, write $\mathrm{Syl}_7(G) = \{P_1, \ldots, P_8\}$

Each P_i has 7 elements. In particular, $P_i \cap P_j \neq \{e\}$ $\forall i \neq j$ because $|P_i \cap P_j| \neq 7$ and $|P_i \cap P_j| \mid 7$.

$\Rightarrow$ We have $(7-1)8 = 48$ elements of order 7

↳ don't count $e \in P_i$

We are left with $56 - 48 = 8$ elements: e & 7 more, none of them has order 7.

As any $Q \in \mathrm{Syl}_2(G)$ has size 8, we are forced to have $n_2 = 1$ because $|G \setminus \bigcup_{i=1}^{8} (P_i \setminus \{e\})| = 8$ & $Q \subseteq G \setminus \bigcup_{i=1}^{8} (P_i \setminus \{e\})$. Then, $Q \triangleleft G$, $Q \neq \{e\}, G$

so G is not simple. □

§17.2 Sylow subgroups of D_{2m} for m odd:

We assume m is odd, then $|D_m| = 2m \Rightarrow p = 2$ or $p \mid m$

• Any Sylow 2-subgroup has order 2.

$D_{2m} = \{ \boxed{e, r, r^2, \dots, r^{m-1}}$ → normal subgroup of D_{2m} $= \langle r \rangle \simeq \mathbb{Z}/m\mathbb{Z}$

$\boxed{s, sr, sr^2, \dots, sr^{m-1}} \}$ all elements of order 2

m is odd, so $\text{ord}(r^j) \neq 2 \ \forall j$

Proposition 1: $|\text{Syl}_2(D_{2m})| = m$ when m is odd.

Proof: $\text{Syl}_2(D_{2m}) = \{\{e, sr^j\} : j = 0, \dots, m-1\}$ has m elements, all distinct

- Let p be any odd prime dividing m and pick $Q \in \text{Syl}_p(D_{2m})$.

Since $2 \nmid |Q|$, no element of Q can have order 2. This implies $Q \subseteq \underbrace{\langle r \rangle}_{\substack{\text{abelian} \\ \simeq \mathbb{Z}/m\mathbb{Z}}} \trianglelefteq D_{2m}$

Since $p \mid m \Rightarrow p \mid |\langle r \rangle|$ so $Q \in \text{Syl}_p(\underbrace{\langle r \rangle}_{\simeq \mathbb{Z}/m\mathbb{Z}})$

Proposition 2: $|\text{Syl}_p(D_{2m})| = 1$ when m is odd & $p \neq 2$

Proof: $\text{Syl}_p(\mathbb{Z}/m\mathbb{Z}) = 1$ because the group is abelian.

If $Q_1, Q_2 \in \text{Syl}_p(D_{2m})$ then they are both Sylow p-subgroups of $\mathbb{Z}/m\mathbb{Z}$ because they both lie in $\langle r \rangle$ and have the correct size. Then, $Q_1, Q_2 \in \text{Sylow}_p(D_{2m})$ yields $Q_1 = Q_2$.

§17.3 Sylow subgroups of D_{2m} for m even:

We assume m is even, and write $m = 2^a k$ for k odd.

$\Rightarrow 2m = 2^{a+1} m$ with $a \geq 1$

GOAL: Compute Sylow subgroups of $D_{2^{a+1}m}$ for $a \geq 1$ and m odd.

Example: $m = 3$, $a = 1$ $\quad |D_{12}| = 1 \quad D_{12} = \langle s, r \mid s^2 = r^6 = e, srs = r^{-1} \rangle$

$r^3 \in D_{12}$ has order 2 and it is a central element (HW1). So it must be in all Sylow 2-subgroups. To get such a subgroup, we need another element of order 2.

$\{e, s, r^3, sr^3\} = \{e, sr^3, r^3, s\}$, $\quad \{e, sr, r^3, sr^4\} = \{e, sr^4, r^3, sr\}$, $\quad \{e, sr^2, r^3, sr^5\} = \{e, sr^5, r^3, sr^2\}$

ie "mod out by $\underbrace{\langle r^3 \rangle}_{= Z(D_{12})} \simeq \mathbb{Z}/2\mathbb{Z}$" and then count. $\Rightarrow n_2(D_{12}) = 3$.

Same idea works in general:

Proposition 1: $\left|Syl_2(D_{2^{a+1}m})\right| = m$ if m is odd and $a \geq 1$.

Proof: $Z(D_{2^{a+1}m}) = \langle r^{2^{a-1}m} \rangle$ has order 2 and lies in every Sylow 2-subgroup because of $Z(D_{2^{a+1}m}) \trianglelefteq D_{2^{a+1}m}$ & Sylow (2).

We consider the projection
$$\begin{array}{ccc} D_{2^{a+1}m} & \xrightarrow{\pi} & D_{2^{a+1}m}/\langle r^{2^{a-1}m}\rangle \simeq D_{2^a m} \\ s & \longmapsto & \bar{s} \\ r & \longmapsto & \bar{r} \end{array}$$

because $\bar{s} = \pi(s)$ has order 2
$\bar{r} = \pi(r)$ has order $2^{a-1}m$
$\pi(s)\pi(r)\pi(s) = \pi(r^{-1})$

These describe the relations of $D_{2^a m}$.

$|\mathrm{Im}\,\pi| = 2^{a+1}m/2 = 2^a m$ & $|\mathrm{Ker}\, f| = 2$

Claim: π induces a bijection $Syl_2(D_{2^{a+1}m}) \xrightarrow{\sim} Syl_2(D_{2^a m})$

Proof: $H \in Syl_2(D_{2^{a+1}m}) \Rightarrow |H| = 2^{a+1}$ & $r^{2^{a-1}m} \in H$ by construction

$\Rightarrow \pi(H) = H/\langle r^{2^{a-1}m}\rangle \leq D_{2^a m}$ by 2^{nd} Iso Theorem.

Since $\left|H/\langle r^{2^{a-1}m}\rangle\right| = 2^{a+1}/2 = 2^a$ we get $\pi(H) \in Syl_2(D_{2^a m})$.

Conversely, every subgroup $\bar{H}$ 2-subgroup of $D_{2^a m}$ has order 2^a and by 2^{nd} Iso Theorem, it induces $H = \pi^{-1}(\bar{H}) \leq D_{2^{a+1}m}$ with $H \supseteq \mathrm{Ker}\,\pi = \langle r^{2^{a-1}m}\rangle$.
Since $|H| = |\bar{H}|\cdot|\mathrm{Ker}\,\pi| = 2^{a+1}$ we have $H \in Syl_2(D_{2^{a+1}m})$.

The map π induces a 1-to-1 correspondence between these sets by the 2^{nd} Iso Thm because every $H \in Syl_2(D_{2^{a+1}m})$ contains $\mathrm{Ker}\,\pi$. □

We finish the proof by induction on $a+1 \geq 2$, combined with the Claim, to show
$$|Syl_2(D_{2^{a+1}m})| = |Syl_2(D_{4m})| = |Syl_2(D_{2m})|$$
In turn, $|Syl_2(D_{2m})| = m$ by Proposition 1 § 12.2

Proposition 2: $|Syl_p(D_{2^a m})| = 1$ when m is odd, $a \geq 1$ & $p \neq 2$

<u>Proof:</u> Fix $Q \in Syl_p(D_{2^a m})$. Since $2 \nmid |Q|$ Q cannot contain any element of order 2. Thus $Q \subseteq \langle r \rangle$ which is abelian. Thus $Q \in Syl_p(\langle r \rangle)$ Since $|Syl_p(\langle r \rangle)| = 1$, the result follows. $\square$