Lecture 8: Sylow Theorems II

Last time: Discussed Sylow Thms

Fix $p>0$ prime & write $n=p^r m$ with $(m:p)=1$.

Let G be a group of order n.

Definition: A subgroup $P<G$ of order p^r is called a Sylow p-subgp of G

Sylow Theorems: (A) Sylow p-subgroups exist.

(B1) If $H<G$ is a p-group, then there exists a Sylow p-subgroup $P<G$ with $H\subseteq P$.

(B2) Any two Sylow p-subgroups $P,Q<G$ are conjugate to each other (ie $\exists\, g\in G$ with $Q=gPg^{-1}$)

(C) Let n_p = number of Sylow p-subgroups of G. Then (i) $n_p\equiv 1 \bmod (p)$
(ii) $n_p \mid m$

Obs 1: (A) can be strengthen to arbitrary powers of p: (see HW3)

(A') There exists subgroups H of G with $|H|=p^i$ for all $i=0,\ldots,r$.

Obs 2: original proof of Sylow (A) went through permutations & matrices / $\mathbb{F}_p$:
(see HW3)

Step 1:
$$G \hookrightarrow \underset{\mathrm{Aut}_{Set}(G)}{\overset{\|}{S_n}} \hookrightarrow GL_n(\mathbb{F}_p)$$
$$g \longmapsto L_g$$
$$\sigma \longmapsto (P_\sigma)_{ij}=\begin{cases}1 & \text{if } \sigma(i)=j\\ 0 & \text{else}\end{cases}$$

Step 2: $GL_n(\mathbb{F}_p)$ has a Sylow p-group $=\left\{\begin{pmatrix}1 & & a_{ij}\\ & \ddots & \\ 0 & & 1\end{pmatrix} : a_{ij}\in\mathbb{F}_p \ 1\leq i<j\leq n\right\}$

Here, $|GL_n(\mathbb{F}_n)| = p^{\frac{n(n-1)}{2}}\, \Pi$ where $(p:\Pi)=1$

(Last time: $n=2$ & $p=5$).

Step 3 (**HEART**) If $G<H$ $p \mid |G|$ & H has a Sylow p-subgp, so does G.

Obs 3: Can count n_p for $GL_n(\mathbb{F}_q)$ for any finite field $\mathbb{F}_q$ of char p $(q=p^k)$
(see HW3)
$$n_p = \prod_{k=1}^{n}(q^{k-1}+q^{k-2}+\cdots+1) =: [n!]_q \quad (q\text{-factorial number!})$$

(Last time $n=2$ & $q=p=5$, we got $n_5=6=1(5+1)=[2!]_5$)

§1. Application 1: Classifying simple groups

Sylow Theorems are often used for classification of finite groups. In particular, they can help us find one nontrivial, proper normal subgp.
(If so, $e \neq H \lhd G \rightsquigarrow G/H$ is group of smaller order ....)

Definition: A group G is simple if it has no nontrivial proper, normal subgroup.

Lemma: Assume G has a unique Sylow p-subgroup P, $p \mid G$ & G is not a p-gp. Then, $P \lhd G$

Proof: By Thm (B2), gPg^{-1} is also a Sylow p-subgroup $\forall g \in G$.
Since $n_p = 1$, we conclude $gPg^{-1} = P$ $\forall g \in G$, so $P \lhd G$. $\square$

Proposition 1: There are no simple groups of order 28

Pf/ $|G| = 28 = 2^2 7 \underset{\text{Thm (C)}}{\rightsquigarrow} \left.\begin{array}{l} n_7 \equiv 1 \mod 7 \\ n_7 \mid 4 \end{array}\right\} \Rightarrow \boxed{n_7 = 1}$

By the Lemma, the Sylow 7-subgroup P of G is normal, proper & nontrivial. So G is not simple.

Proposition 2: There are no simple groups of order 224.

Pf/ $|G| = 224 = 2^5 \cdot 7 \underset{\text{Thm (C)}}{\Longrightarrow} \left.\begin{array}{l} \cdot\ n_2 \equiv 1 \mod 2 \\ \quad n_2 \mid 7 \end{array}\right\} \Rightarrow \boxed{n_2 = 1 \text{ or } 7}$

CASE 1: $n_2 = 1$ Then by the Lemma Sylow 2-subgroup $P \lhd G$
But $e \neq P$, $P \neq G$ so G is not simple!

CASE 2: $n_2 = 7$ so $\cdot\ |Syl_2(G)| = 7$.

By Thm (B2) $G \circlearrowright Syl_2(G)$ by conjugation.

Thus, we have a group homomorphism:

$$\varphi : G \longrightarrow \mathrm{Aut}_{set}\, Syl_2(G) = S_7$$

sizes: 224 $\qquad$ $7! = 5040$

<u>Claim 1</u>: φ is not injective

Pf/ If so $G \simeq \mathrm{Im}\,\varphi < S_7$ so $224 \mid 5040$ Contra!
($2^5 \nmid 5040$)

<u>Claim 2</u>: φ is not trivial

Pf/ $\mathrm{Ker}\,\varphi = G$ means $G \circlearrowright Syl_2(G)$ is a trivial action, but we know it's transitive & $|Syl_2 G| \neq 1$. Contra!

<u>Conclusion</u> $\mathrm{Ker}(\varphi) \trianglelefteq G$, $\mathrm{Ker}(\varphi) \neq e, G$, so G is not simple. $\square$

- The last usual trick is to overcount when some $n_p > 1$.

<u>Proposition 3</u>: There are no simple groups of order 56.

Pf/ $|G| = 56 = 2^3 \cdot 7$. $\underset{\text{Thm (C)}}{\Longrightarrow}$ $\left.\begin{array}{l} \bullet\ n_7 \equiv 1 \bmod 7 \\ \bullet\ n_7 \mid 8 \end{array}\right\} \Rightarrow \boxed{n_7 = 1 \text{ or } 8}$

- <u>CASE 1</u>: $n_7 = 1$ Then G is not simple ($P \in Syl_7(G)$ works)
- <u>CASE 2</u>: $n_7 = 8$ Write $Syl_7(G) = \{P_1, \dots, P_8\}$.

- Each P_i has 7 elements.
- $P_i \cap P_j = \{e\}$ if $i \neq j$ (any $x \in P_i \cap P_j$, $x \neq e$ will generate both P_i & P_j).

$\Rightarrow \bigcup_{i=1}^{8} P_i$ has $(7-1)\,8 = 48$ elements of order 7.

Then, $H = (G \setminus \bigcup_{i=1}^{8} P_i) \cup \{e\}$ has $56 - 48 = 8$ elements.

- <u>Claim</u>: H is a Sylow 2-subgroup of G, so $n_2 = 1$ & G is not simple

If $Q \in Syl_2(G)$, then $Q \cap P_i = \{e\}$ (orders are coprime)
So $Q \subseteq H$ but $|Q| = |H| = 8$ so $Q = H$ $\square$

<u>Obs</u>: One example featuring all tricks (in HW3):
If $|G| = 60 = 2^2 \cdot 3 \cdot 5$ & G is simple, then $n_5 = 6$, $n_3 = 10$ & $n_2 = 5$.

§.2 Classification of groups of order p^2:

Lemma: If $H \neq \{e\}$ is a p-group, then its center $Z(H)$ is nontrivial

Pf/ Consider $H \circlearrowright H$ by conjugation, then $|H^H| \equiv |H| \equiv 0 \pmod p$
$H^H = \{x \in H : hxh^{-1} = x \ \forall h \in H\} = Z(H)$ $\Rightarrow$ $p \mid |Z(H)|$ $\square$

Obs: $Z(H) \lhd H$ is a normal abelian subgroup.

We can prove that groups of order p^2 are abelian & we can classify them:

Proposition: If $|G| = p^2$, then G is abelian. Furthermore,

$$G \simeq \mathbb{Z}/p^2\mathbb{Z} \text{ or } \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Pf/ By our Lemma $|Z(G)| = p$ or p^2. In the latter case, $G = Z(G)$ & G is abelian. In the former case $|G/Z(G)| = p$ so $G/Z(G) \simeq \mathbb{Z}/p\mathbb{Z}$ is cyclic. But HW1 Problem 18 implies G is abelian so $|Z(G)| \neq p$.
Contr!

To finish, we show the classification of G

CASE 1: $\exists\, g \in G$ of order p^2. Then $\boxed{G = \langle g \rangle \simeq \mathbb{Z}/p^2\mathbb{Z}}$.

CASE 2: Every non-identity element has order p. We claim

$$\boxed{G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}} \quad \text{(coordinatewise multiplication)}$$

Pick any $\sigma \in G \setminus \{e\}$ & any $\tau \in G \setminus \langle\sigma\rangle$. Then:

$$\langle\sigma\rangle \simeq \mathbb{Z}/p\mathbb{Z} \quad \& \quad \langle\tau\rangle \simeq \mathbb{Z}/p\mathbb{Z}.$$

Check: ① $\langle\sigma,\tau\rangle = G$ because $p < |\langle\sigma,\tau\rangle| \mid |G| = p^2$

② $\langle\sigma\rangle, \langle\tau\rangle \lhd G$ because G is abelian

③ $\langle\sigma\rangle \cap \langle\tau\rangle = \{e\}$ (Otherwise, $\exists\, k \in \{1, \ldots, p-1\}$ with $\tau^k \in \langle\sigma\rangle$ But $o(\tau^k) = p$ because $(k:p) = 1$, so $\langle\tau^k\rangle = \langle\tau\rangle \subseteq \langle\sigma\rangle$. Contradiction!)

Conclude: $G \overset{(**)}{\simeq} \langle\sigma\rangle \times \langle\tau\rangle \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

$\sigma^k \tau^\ell \longleftarrow (\sigma^k, \tau^\ell)$

this is gp homomorphism & surjective by ① $\square$

Obs 1: Proposition fails for $|G| = p^3$ (eg $G = Q_8$ or D_4)

Obs 2: $(*)$ uses that G is abelian! But we can get by with less!

(1) We only need $\langle\sigma\rangle$ & $\langle\tau\rangle$ to mutually commute.

(2) We need only one of them to be normal

These two conditions will lead to semidirect products (next time!)

§3. Application: Classify groups of order 45

Fix G a finite group with $|G| = 45 = 3^2 \cdot 5$

Then $n_3 = \#\{P \leq G : |P| = 9\}$ $\quad n_3 \equiv 1 \ (3), \ n_3 \mid 5 \Rightarrow \boxed{n_3 = 1}$

$n_5 = \#\{Q \leq G : |Q| = 5\}$ $\quad n_5 \equiv 1 \ (5), \ n_5 \mid 9 \Rightarrow \boxed{n_5 = 1}$

Conclusion: In a group with 45 elements there is:

- a unique subgroup P of size 9 $\Rightarrow P \lhd G$
- ———————— Q of size 5 $\overset{(B2)}{\Rightarrow} Q \lhd G$

Observe ① If $H = \langle P, Q\rangle \leq G$, then $\begin{matrix} 9 = |P| \mid |H| \\ 5 = |Q| \mid |H| \end{matrix} \Rightarrow |H| = 45.$ so $H = G$.

② If $g \in P \cap Q \Rightarrow \left.\begin{matrix} \mathrm{ord}(g) \mid |P| = 9 \\ \mathrm{ord}(g) \mid |Q| = 5 \end{matrix}\right\} \Rightarrow \mathrm{ord}(g) = 1$ so $g = e$

Conclusion: $G = \langle P, Q\rangle$, $\quad P, Q \lhd G$, $\quad P \cap Q = \{e\}$.

By HW1 Problem 16: P commutes with Q, ie $ab = ba \ \forall a \in P, b \in Q$.

(Pf/ $[a,b] \in P \cap Q = \{e\}$ so a & b commute)

Conclusion: $G = \{ pq : p \in P, q \in Q \}$ with group operation

$pq \cdot p'q' = \underbrace{pp'}_{\in P} \underbrace{qq'}_{\in Q}$ ($qp' = p'q$ because P, Q are mutually commuting subgps)

Note: $P \times Q \longrightarrow G$ is group homomorphism

$(p, q) \longmapsto pq$ $|P \times Q| = |G|$ so iso!

By Proposition $P \simeq \mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ & $Q \simeq \mathbb{Z}/5\mathbb{Z}$,

so we understand G completely: $G \simeq P \times Q$.