Lecture 8: Sylow Theorems II

Last time: Fix $p>0$ prime & set $\boxed{n = p^r m}$ with $(m:p)=1$. Fix G gp, $|G|=n$

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 (i.e. $\exists\, g\in G$ with $Q = gPg^{-1}$)

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

TODAY: . Applications of Sylow Thms: { ① Detect Simple groups ② Classification of some groups.

. Classify groups of order p^2.

Some Observations (see HW3)

(*) HARD. $G \lhd H$, $p \mid |G|$ & H has a Sylow p-subgp, then G has one too!

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

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

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

Step ① $G \hookrightarrow \underset{\text{Aut}_{\text{set}}(G)}{S_n} \xrightarrow{\Phi} GL_n(\mathbb{F}_p)$ (permutation matrix.)

$g \longmapsto L_g$

$$\Phi(\sigma) = (P_\sigma)_{ij} = \begin{cases} 1 & \text{if } \sigma_{(i)} = j \\ 0 & \text{else} \end{cases}$$

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

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

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

(*)

Obs 3: Can count n_p for $GL_n(\mathbb{F}_q)$ for any finite field $\mathbb{F}_q$ of char p ($q = p^k$)

$$n_p = \prod_{k=1}^{n} \underbrace{(q^{k-1} + q^{k-2} + \dots + 1)}_{=: [K]_q \ (q\text{-number})} =: [n!]_q \quad (q\text{-factorial number!})$$

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

Application 1: Simple groups

Aim: Classification of groups.

Obs: If $H \neq e, G$, $H \trianglelefteq G$, then G/H is group of smaller order $\Rightarrow$ induction!

Def A group G is **simple** if it has **no** nontrivial, proper, normal subgroups

- **3 main Tricks** involving Sylow Thms:

Lemma: Assume G has a unique Sylow p-subgroup P. Then, $P \trianglelefteq G$.
($p \mid |G|$ & G not a p-gp)

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

Proposition 1: There are no simple groups of order 28

Pf/ $|G| = 2^8 = 2^2 7 \xrightarrow[\text{Thm(C)}]{} \left.\begin{array}{l} n_7 \equiv 1 \mod 7 \\ n_7 \mid 4 \end{array}\right\} \Rightarrow \boxed{n_7 = 1}$

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/ $|G| = 224 = 2^5 \cdot 7$ $\xrightarrow[\text{Thm(C)}]{}$ $\cdot\ n_2 \equiv 1 \mod 2$, $\cdot\ n_2 \mid 7$ $\Rightarrow$ $\boxed{n_2 = 1 \text{ or } 7}$

CASE 1: $n_2 = 1 \Rightarrow \mathrm{Syl}_2(G) = \{P\}$, $P \neq e, G$, $P \trianglelefteq G$, G not simple

CASE 2: $n_2 = 7$ so $|\mathrm{Syl}_2(G)| = 7$. By Thm (B2), $G \curvearrowright^{\text{conj}} \mathrm{Syl}_2(G)$

$\rightsquigarrow$ Group homomorphism $\varphi: G \longrightarrow \mathrm{Aut}_{\text{set}}\, \mathrm{Syl}_2(G) = S_7$

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

Claim 1: φ is not injective (If so, $G \simeq \mathrm{Im}\,\varphi < S_7$ so $224 \mid 7!$ Contr!)

Claim 2: φ is not trivial

Pf/ $\ker \varphi = G$ means $G \curvearrowright \mathrm{Syl}_2(G)$ is a trivial action transitive with $|\mathrm{Syl}_2 G| \neq 1$ Contr!

Conclusion $\ker(\varphi) \trianglelefteq G$, $\ker(\varphi) \neq e, G$, so G is not simple. $\square$

Proposition 3: There are no simple groups of order 56. (overcount trick!)

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

- **CASE 1:** $n_7 = 1 \Rightarrow$ G is not simple ($P \in \mathrm{Syl}_7(G)$ works)
- **CASE 2:** $n_7 = 8$ Write $\mathrm{Syl}_7(G) = \{P_1, \dots, P_8\}$.
  - Each P_i has 7 elements. & $P_i \cap P_j = \{e\}$ for $i \neq j$

  $\Rightarrow \bigcup_{i=1}^{8} P_i$ 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.
  - **Claim:** H is a Sylow 2-subgroup of G, so $n_2 = 1$ & G is not simple

    If $Q \in \mathrm{Syl}_2(G)$, then $Q \cap P_i = \{e\}$ (orders are coprime)

    So $Q \subseteq H$ but $|Q| = |H| = 8$ so $Q = H$ □

All 3 tricks: G simple (eg: $G = A_6$) $|G| = 60 = 2^2 3 \cdot 5 \Rightarrow n_2 = 5,\ n_3 = 10$ & $n_5 = 6$ (HW3)

Classification of groups of order p^2

(*) can be weakened (semidirect products!)

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

Pf/ Consider $G \curvearrowright G$ by conjugation, then $|G^G| \equiv |G| \equiv 0 \pmod p$

$G^G = \{x \in G : gxg^{-1} = x \ \forall g \in G\} = Z(G) \Rightarrow p \mid |Z(G)|$ □

Obs: $Z(G) \triangleleft G$ is a normal abelian subgroup $\Rightarrow$ { If G not abelian $\Rightarrow$ not simple; G abelian, $\langle g \rangle \neq G \Rightarrow \langle g \rangle \triangleleft G$

Proposition: If $|G| = p^2$, then G is abelian and $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (coordwise product)

(Fails for p^3, Eg $G = D_4$ or Q_8)

Pf/ • $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2 \Rightarrow G$ abelian

If $|Z(G)| = p \Rightarrow |G/Z(G)| = p$ so $G/Z(G)$ cyclic $\underset{\text{HW1}}{\Rightarrow} G$ abelian Contr!

• Classification? If $\exists g \in G$ of order $p^2 \Rightarrow G = \langle g \rangle \simeq \mathbb{Z}/p^2\mathbb{Z}$

Otherwise, pick $\sigma \in G \setminus \{e\}$, $\tau \in G \setminus \langle \sigma \rangle \Rightarrow \langle \sigma \rangle \simeq \mathbb{Z}/p\mathbb{Z} \simeq \langle \tau \rangle$

Check: ① $\langle \sigma, \tau \rangle = G$ ($p < \langle \sigma, G \rangle \mid p^2$) (G abelian)

(*) ② $\langle \sigma \rangle, \langle \tau \rangle \triangleleft G$

③ $\langle \sigma \rangle \cap \langle \tau \rangle = \{e\}$

} $\Rightarrow \varphi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G$, $(k, \ell) \mapsto \sigma^k \tau^\ell$ is group iso. □

Application: Classify groups of order 45

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

Then: $n_3 \equiv 1 \ (3)$ & $n_3 \mid 5 \Rightarrow \boxed{n_3 = 1}$; $n_5 \equiv 1 \ (5)$ & $n_5 \mid 9 \Rightarrow \boxed{n_5 = 1}$

Conclusion If $Syl_3(G) = \{P\}$, $Syl_5(G) = \{Q\}$, then $P \trianglelefteq G$, $Q \trianglelefteq G$.

Observe ① If $H = \langle P, Q \rangle \leq G$, then $9 = |P| \, |H|$, $5 = |Q| \, |H| \Rightarrow |H| = 45$.

Thus, $\boxed{H = G}$.

② If $g \in P \cap Q \Rightarrow \begin{cases} \text{ord}(g) \mid |P| = 9 \\ \text{ord}(g) \mid |Q| = 5 \end{cases} \Rightarrow \text{ord}(g) = 1$ so $g = e$

Thus, $\boxed{P \cap Q = \{e\}}$

$\Longrightarrow$ (HW 1) P commutes with Q ($[a, b] \in P \cap Q = \{e\}$ for $a \in P$, $b \in Q$)

$\rightsquigarrow$ $\varphi : P \times Q \xrightarrow{\sim} G$, $(p, q) \longmapsto pq$ is group homomorphism But $|P \cdot Q| = |G|$ so iso!

(coordinwise prod)

Note: $P \simeq \mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$; $Q \simeq \mathbb{Z}/5\mathbb{Z}$