Lecture 7 : Sylow Theorems

Last week: • Defined $G \curvearrowright X$ (gp, set) via $G \longrightarrow \mathrm{Aut}_{set}(X)$ gp hom.
$g \longmapsto (x \longmapsto g \cdot x)$

- $G \cdot x \subseteq X$ orbit $\forall x \in X$ $\quad \mathrm{Stab}_G(x) < G$ stabilizer $\forall x \in X$
- $X^g \subseteq X$ fixed pt set $\forall g \in G$

• **Examples:** ① $S_n \curvearrowright \{1, \dots, n\}$,
② $D_n \subset \mathbb{R}^n, \{(0,0)\}$
③ $G \curvearrowright G$ left mult $x \longmapsto g \cdot x$
right — $x \longmapsto x \cdot g^{-1}$
conjugation $x \longmapsto gxg^{-1}$

• **Counting lemmas:**

(1) $|G| = |\mathrm{Stab}_G(x)| \, |G \cdot x| \quad \forall x \in G$

(2) $|X| = \sum_{\alpha \in G \backslash X} |G \cdot x_\alpha| = \sum_{\alpha \in G \backslash X} \frac{|G|}{|\mathrm{Stab}_G(x_\alpha)|}$

(3) **Burnside** $\left| \frac{X}{G} \right| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$ (G finite)

• **Applications** ① $\binom{p^c m}{p^c} \equiv m \pmod p$

② $|G| = p^k$ (p-group) $\Rightarrow |X| \equiv |X^G| \pmod p$ where $X^G = \bigcap_{g \in G} X^g$

Sylow Theorems

- Fix $p > 0$ prime & write $n = p^r m$ with $(m : p) = 1$. Let 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 (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) $n_p \mid m$

We will prove them using G-actions!

Sylow Thm (A): Sylow p-subgroups exist

Pf/ Let $\xi = \{ Y \subset G \text{ subset} : |Y| = p^r \}$

$G \curvearrowright \xi$ induced by left multiplication action $G \curvearrowright G$, ie:

given $g \in G$ & $Y = \{y_1, \dots y_{p^r}\} \in \xi$ we $\boxed{g \cdot Y} = \{g \cdot y_1, \dots, g \cdot y_{p^r}\} \in \xi$

Claim: There exists $X \in \xi$ with $p \nmid |G \cdot X|$

Pf/ By the Counting Lemma 2: $|\xi| = \sum_{\alpha \in G \backslash \xi} |G \cdot x_\alpha|$

By Application ① $|\xi| = \binom{p^r m}{p^r} \equiv m \pmod p \not\equiv 0 \Rightarrow p \nmid |G \cdot x_\alpha|$ for some α

- Let $\boxed{H_x = \operatorname{Stab}_G(X)} < G$ Then, $|G \cdot X| = \dfrac{|G|}{|H_x|} \not\equiv 0 \pmod p \Rightarrow \boxed{p^r \mid |H_x|}$ (1)

- To finish, choose $x_0 \in X$ and define $\varphi : H_x \longrightarrow X$, $g \longmapsto g \cdot x_0 \in X$ (by definition of Stabilizer)

- φ is injective ($g x_0 = h x_0 \in G$)

$\Rightarrow \boxed{|H_x| \leq |X| = p^r}$ (2)

Combined (1) & (2) gives $|H_x| = p^r$. $\square$

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

Pf/ Let $H<G$ be a p-subgroup of G, so $|H|=p^k$ with $k\leq r$.

- Let Q be any Sylow p-subgroup of G (which exists by Thm (A))
- $H\curvearrowright X:=G/Q$ via $h\cdot gQ=(hg)Q$.
- By Application (2) $|X^H|\equiv |X| \pmod p$

But $|X|=m\not\equiv 0 \pmod p \Rightarrow X^H\neq\emptyset$ $\Leftarrow \exists\ gQ\in X^H$ $(hgQ=gQ\ \ \forall h\in H)$

$\Rightarrow g^{-1}hg\in Q\ \ \forall h\in H$ so $\boxed{H\subseteq gQg^{-1}=:P}$

- Since $|gQg^{-1}|=|Q|=p^r$, P is Sylow p-subgp & $H\subseteq P$ $\square$

Sylow Thm (B2): Any two Sylow p-subgroups are conjugate

Pf/ Pick 2 Sylow p-subgroups Q, P'. Take $H=P'$, Q in proof of Thm (B1). Then $P'\subseteq gQg^{-1}$ & both have the same size, so $P'=gQg^{-1}$ is conjugate! $\square$

Sylow Thm (C1): If $n_p := \#$ Sylow p-subgroups of G, then $n_p \equiv 1 \pmod{p}$

Pf/ Let $\mathcal{S}$ be the set of all Sylow p-subgroups of G. $\Rightarrow n_p = |\mathcal{S}| \geq 1$ by Thm (A)

By Thm (B), we know that $G \curvearrowright \mathcal{S}$ by conjugation is transitive. Fix $\boxed{P \in \mathcal{S}}$

$(x \cdot Q = xQx^{-1})$.

$\Rightarrow P \curvearrowright \mathcal{S}$ by restriction.

Claim: $\mathcal{S}^P = \{P\}$ $\left(\Rightarrow n_p = |\mathcal{S}| \equiv |\mathcal{S}^P| = 1 \pmod{p}\ \checkmark\right)$

↑ by Application (2)

Proof of claim: Fix $Q \in \mathcal{S}^P$ $\left(xQx^{-1} = Q \ \forall x \in P \ \& \ Q \in \mathcal{S}\right)$

Define $\boxed{N_Q} = \{g \in G : gQg^{-1} = Q\} < G$ (normalizer of Q in G)

$= \mathrm{Stab}_G(Q)$ under action by conjugation

Then $Q, P \subset N_Q$ & $|N_Q| \,\big|\, |G| = p^r m$ so P & Q are two Sylow p-subgroups of N_Q

$\Longrightarrow$ (Thm (B2)) P & Q are conjugate in N_Q, so $\exists\, x \in N_Q$ with $P = xQx^{-1} = Q$ (↑ $x \in N_Q$)

$\Rightarrow \boxed{P = Q}$ ∎

Sylow Thm (c2): If $n_p := \#$ Sylow p-subgroups of G, $|G| = p^r m$, then $n_p \mid m$

Pf/ Let $\mathcal{S}$ be the set of all Sylow p-subgroups of G. Fix $\boxed{P \in \mathcal{S}}$

By Thm (B), we know that $G \curvearrowright \mathcal{S}$ by conjugation is transitive
$(x \cdot Q = xQx^{-1})$.

Use Counting Lemma 1:

$$n_p = |\mathcal{S}| = |G \cdot P| = \frac{|G|}{|\mathrm{Stab}_G(P)|} = \frac{|G|}{|N_P|}$$

Since $P < N_P < G \Rightarrow |N_P| = p^r m'$ for some $m' \mid m$.

Then $n_p = \frac{m}{m'}$ & so $\boxed{n_p \mid m}$. □

Obs: Thm (A) is <u>not</u> constructive, but Thm (B1) gives a potential (in practice) algorithm: Start from $H = \langle x \rangle$ where $\mathrm{ord}(x) = p^k$, & add to it elements with order a power of p until we reach a subgroup of the expected order $(= p^r)$

An Example

- Fix $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ $\quad G = GL_2(\mathbb{F}_5) = \{$ invertible 2×2 matrices over $\mathbb{F}_5\}$

Claim 1: $|G| = 480 = 2^5 3 \cdot 5$ $\quad (\Rightarrow$ Thm (A) gives Sylow p-subgroups for $p = 2, 3, 5)$

Pf/ # choices for 1st column $= |\mathbb{F}_5^2 \setminus \{[0]\}| = 25 - 1 = 24$

choices for 2nd column $= |\mathbb{F}_5^2 \setminus \{\lambda \cdot 1^{st}\text{ column} \mid \lambda \in \mathbb{F}_5\}| = 25 - 5 = 20$

$480 = 24 \cdot 20$ ✓

- Two Sylow 5-subgroups: $P = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \; x \in \mathbb{F}_5 \right\}$ & $P' := \left\{ \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix} \; x \in \mathbb{F}_5 \right\}$

$\left(P < G: \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix} \in P, \quad \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} \in P\right)$ $\quad P \neq P'$, so $n_5 \geq 2$

- Sylow 3-subgroups: Need $A^3 = Id$, so $x^3 - 1$ vanishes along A

Write $x^3 - 1 = (x^2 + x + 1)(x - 1)$

If we pick A with characteristic polynomial $x^2 + x + 1$, then by the Cayley–Hamilton Theorem, $A^2 + A + 1 = 0$ so $A^3 = Id$. If $A \neq Id$, this will say A has order 3.

A: Companion Matrices!

Prop: Given $P(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0$ (monic), the $n \times n$ matrix

$$A = \begin{bmatrix} 0 & & & -c_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -c_{n-2} \\ & & 1 & -c_{n-1} \end{bmatrix}$$

has char. poly $P(t)$.

Use <u>companion matrix</u> for any monic $P(t)$.

In our case: $A = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$ gives $P(t) = X^2 + X + 1$ ✓ $\left(A^2 = A^{-1} = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}\right)$

<u>Conclude</u> $P = \left\langle \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \right\rangle$ is a Sylow 3-subgroup.

Another one: $P' = \left\langle \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \right\rangle$ (transpose!)

} so $\boxed{n_3 > 1.}$

$n_3 \equiv 1 \pmod 3$ & $n_3 \mid 160$.

- <u>A Sylow 2-subgroup</u> $P = \left\{ \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}, \begin{bmatrix} 0 & \mu_1 \\ \mu_2 & 0 \end{bmatrix} \;\; \lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{F}_5^* \right\}$

$P < G$

$\cdot \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} 0 & \mu_1 \\ \mu_2 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \lambda_1\mu_1 \\ \lambda_2\mu_2 & 0 \end{bmatrix} \in P$ ✓ $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{\lambda_1} & 0 \\ 0 & \frac{1}{\lambda_2} \end{bmatrix}$ ✓

$\cdot \begin{bmatrix} 0 & \mu_1 \\ \mu_2 & 0 \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} = \begin{bmatrix} \lambda_1\mu_1 & 0 \\ 0 & \lambda_2\mu_2 \end{bmatrix} \in P$ ✓ $\begin{bmatrix} 0 & \mu_1 \\ \mu_2 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & \frac{1}{\mu_2} \\ \frac{1}{\mu_1} & 0 \end{bmatrix}$ ✓

$n_2 \equiv 1 \pmod 2$ & $n_2 \mid 15$ $\Rightarrow$ $n_2 = 1, 3, 5, 15$

Prop: $n_5 = 6$ $\left(P = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} : x \in \mathbb{F}_5 \right\}, \quad P' = \left\{ \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix} : x \in \mathbb{F}_5 \right\} \right)$
$= \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$

Pf/ Thm (c) gives $n_5 \equiv 1 \pmod 5$ & $n_5 \mid 2^5 3$

$n_5 \equiv 2^k 3^j \equiv 2^k (-2)^j \equiv (-1)^j 2^{k+j} \equiv 1 \pmod 5$ for $j = 0, 1$, $k = 0, \dots, 5$

- If $j = 0$, then $k = 0, 4$ so $n_5 = 1$ or 16
- If $j = 1$, then $k = 1, 5$ so $n_5 = 6$ or 96.

$\Big\} \Rightarrow n_5 = 6, 16$ or 96. ($P \neq P'$)

To find them all, use (B2): Build conjugates to P. Enough to use gen!

$$\frac{1}{ad-bc}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} ad-bc-ac & a^2 \\ -c^2 & ad-bc+ac \end{bmatrix} = B$$

Since $-1 \equiv 2^2 (5)$, can assume $ad - bc = 1$ or 2

$\left(\lambda A \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} (\lambda A)^{-1} = A \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} A^{-1} \text{ & } \det \lambda A = \lambda^2 \det A \right)$

- If $ad - bc \equiv 1 \mod 5 \Rightarrow B = \begin{bmatrix} 1 - ac & a^2 \\ -c^2 & 1 + ac \end{bmatrix}$ ≤ 24 options
- If $ad - bc \equiv 2 \mod 5 \Rightarrow B = \begin{bmatrix} 1 - 3ac & 3a^2 \\ -3c^2 & 1 + 3ac \end{bmatrix}$ ≤ 24 options

($2^{-1} \equiv 3 \mod(5)$)

Conclude ≤ 48 options for B, so $n_5 = 6$ or 16.

CASE 1 $B = \begin{bmatrix} 1-ac & a^2 \\ -c^2 & 1+ac \end{bmatrix}$ & $ad-bc \equiv 1 \pmod 5$

- $c=0$ & any $a \neq 0$ gives $P = \langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rangle$
- $a=0$ & any $c \neq 0$ gives $P' = \langle \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \rangle$

} $\rightsquigarrow 2$

Next we compute the remaining combinations & $\{B^2, B^3, B^4\}$.

a \ c	1	2	3	4
1	$\begin{bmatrix} 0 & 1 \\ 4 & 2 \end{bmatrix}$	$\begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 \\ 1 & 4 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 \\ 4 & 0 \end{bmatrix}$
2	$\begin{bmatrix} 4 & 4 \\ 4 & 3 \end{bmatrix}$	$\begin{bmatrix} 2 & 4 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 4 \\ 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}$
3	$\begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}$	$\begin{bmatrix} 0 & 4 \\ 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 4 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 4 & 4 \\ 4 & 3 \end{bmatrix}$
4	$\begin{bmatrix} 2 & 1 \\ 4 & 0 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 \\ 1 & 4 \end{bmatrix}$	$\begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 4 & 2 \end{bmatrix}$

$\rightsquigarrow 3$ $\rightsquigarrow 1$

$\begin{bmatrix} 0 & 1 \\ 4 & 2 \end{bmatrix}^4 = \begin{bmatrix} 2 & 4 \\ 1 & 0 \end{bmatrix}$

$\begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}^4 = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}$

$\begin{bmatrix} 3 & 1 \\ 1 & 4 \end{bmatrix}^4 = \begin{bmatrix} 4 & 4 \\ 4 & 3 \end{bmatrix}$

$\begin{bmatrix} 2 & 1 \\ 4 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & 4 \\ 1 & 2 \end{bmatrix}^2$

$\begin{bmatrix} 2 & 4 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 1 \\ 4 & 2 \end{bmatrix}^3$

= repeated generators. $\rightsquigarrow$ = repeated subgp.

TOTAL = 6 $\langle B \rangle$

CASE 2: $B = \begin{bmatrix} 1-3ac & 3a^2 \\ -3c^2 & 1+3ac \end{bmatrix}$ & $ad-bc \equiv 2 \pmod 5$

- $c=0$ & any $a \neq 0$ gives $P = \langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rangle$
- $a=0$ & any $c \neq 0$ gives $P' = \langle \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \rangle$

} already counted!

Next we compute the remaining combinations & $\{B^2, B^3, B^4\}$.

a \ c	1	2	3	4
1	$\begin{bmatrix} 3 & 3 \\ 2 & 4 \end{bmatrix}$	$\begin{bmatrix} 0 & 3 \\ 3 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 3 \\ 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 4 & 3 \\ 2 & 3 \end{bmatrix}$
2	$\begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 4 & 2 \\ 3 & 3 \end{bmatrix}$	$\begin{bmatrix} 3 & 2 \\ 3 & 4 \end{bmatrix}$	$\begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix}$
3	$\begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 3 & 2 \\ 3 & 4 \end{bmatrix}$	$\begin{bmatrix} 4 & 2 \\ 3 & 3 \end{bmatrix}$	$\begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix}$
4	$\begin{bmatrix} 4 & 3 \\ 2 & 3 \end{bmatrix}$	$\begin{bmatrix} 2 & 3 \\ 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 3 \\ 3 & 2 \end{bmatrix}$	$\begin{bmatrix} 3 & 3 \\ 2 & 4 \end{bmatrix}$

} Same subgroups from previous Table

= repeated generators. ~~~ = repeated subgp.

Alternative proof

Count $\leq 6 + 8 = 14 < 16$

(6: TABLE 1, 8: TABLE 2)

$\Rightarrow \boxed{n_5 = 6}$