Lecture 7: Sylow Theorems

Last week: • Defined $\underset{\text{gp}}{G} \circlearrowright \underset{\text{set}}{X}$ via $G \longrightarrow \mathrm{Aut}_{\text{set}}(X)$ 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 $S_n \circlearrowright \{1,\ldots,n\}$, ② $D_n \circlearrowright \mathbb{R}^n \setminus \{(0,0)\}$
  ③ $G \circlearrowright G$ left mult $x \mapsto g\cdot x$; right — $x \mapsto x\cdot g^{-1}$; conjugation $x \mapsto gxg^{-1}$
- Counting lemmas:

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

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

(3) Burnside $\left|{}_G\backslash X\right| = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} |X^g|.$ $\quad$ (G finite)

- **Applications** ① $\dbinom{p^r m}{p^r} \equiv m \pmod p$

② $|G| = p^k \Rightarrow |X| \equiv |X^G| \pmod p$ where $X^G = \displaystyle\bigcap_{g \in G} X^g$

(p-group)

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) $n_p\equiv 1 \mod (p)$
(ii) $n_p \mid m$

We will prove them using G-actions!

Sylow Thm (A): Sylow p-subgroups exist

Pf/

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

Pf/

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

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

Pf/

$\boxed{\text{Sylow Thm (C2): If } n_p := \#\text{ Sylow } p\text{-subgroups of } G,\ |G| = p^r m, \text{ then } n_p \mid m}$

Pf/

Obs: Thm (A) is not constructive in practice, but Thm (B1) gives a potential 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 $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ $G = GL_2(\mathbb{F}_5) = \{$ invertible 2×2 matrices over $\mathbb{F}_5\}$

<u>Claim 1</u>: $|G| = 480 = 2^5 3.5$ ($\Rightarrow$ Thm (A) gives Sylow p-subgroups for $p = 2,3,5$)

Pf/

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

- <u>Sylow 3-subgroups</u>: Need $A^3 = Id$, so $X^3 - 1$ vanishes along A

A: Companion Matrices!

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

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

has char. poly $P(t)$

Use companion matrix for any monic $P(t)$.

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

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

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

so $\boxed{n_3 > 1.}$

- A Sylow 2-subgroup

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

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

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

$n_5 \equiv 2^k 3^j \equiv 2^k (-2)^j \equiv (-1)^j 2^{k+j} \equiv 1 \mod(5)$ 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.

$\Big\} \underset{P \neq P'}{\Longrightarrow} n_5 = 6, 16$ or 96.

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 $ad-bc \equiv 1 \mod 5 \Longrightarrow B = \begin{bmatrix} 1-ac & a^2 \\ -c^2 & 1+ac \end{bmatrix}$ $\quad \leq 24$ options
- If $ad-bc \equiv 2 \mod 5 \underset{2^{-1} \equiv 3 \mod(5)}{\Longrightarrow} B = \begin{bmatrix} 1-3ac & 3a^2 \\ -3c^2 & 1+3ac \end{bmatrix}$ $\quad \leq 24$ options

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

CASE 1

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

$$\left.\begin{array}{l} \bullet\ c=0 \ \& \text{ any } a\neq 0 \text{ gives } P = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle \\ \bullet\ a=0 \ \& \text{ any } c\neq 0 \text{ gives } P' = \left\langle \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\rangle \end{array}\right\} \rightsquigarrow 2$$

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

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

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

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

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

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

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

$$\boxed{\underline{\text{TOTAL}} = 6 \ \langle B \rangle}$$

CASE 2:

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

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

$\Big\}$ already counted!

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

$a \backslash c$	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

Alternative proof

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

$$\Longrightarrow \boxed{n_5 = 6}$$