# Lecture XVI: Applications of Sylow Theorems II

**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 $G$ $\quad n_p \equiv 1 \mod(p)$ & $n_p \mid |G|$.

## §16.1 Sylow Subgroups of $S_4$:

**Recall:** • $|S_4| = 2^3 \cdot 3 \Rightarrow p = 2$ & $3$

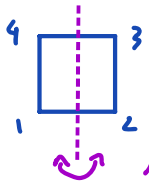
• $Syl_3(S_4) = \{ \langle (123) \rangle, \langle (124) \rangle, \langle (134) \rangle, \langle (234) \rangle \}$.

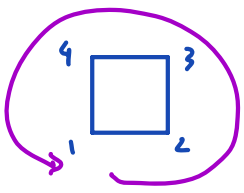
• By Sylow Thm (1) $G$ has a subgroup of order 8.

**Recall:** $D_8 \hookrightarrow S_4$ injective group homomorphism

$s \longmapsto (12)(34)$

$r \longmapsto (1234)$




$r$ = rotation of $\frac{2\pi}{4} = \frac{\pi}{2}$.

So $D_8$ is a Sylow 2-subgroup of $S_4$

$D_8 \simeq P_1 = \{ e, \underset{r}{(1234)}, \boxed{(13)(24)}_{r^2}, \underset{r^3}{(1432)}, \boxed{(12)(34)}_{s}, \underset{sr}{(12)(34)(1234) = (24)}, \underset{sr^2}{(12)(34)(13)(24) = \boxed{(14)(23)}}, \underset{sr^3}{(12)(34)(1432) = (13)} \}$

Any other Sylow 2-subgroup is conjugate to $P_1$. by Sylow Thm (2)

**Note:** $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 3 \Rightarrow n_2 = 1 \text{ or } 3$ by Sylow Thm (3)

$P_\sigma = \sigma P_1 \sigma^{-1}$ for $\sigma \in S_4$.

$P_1 \supseteq$ all (3,2)-cycles of $S_4$, so these elements are permuted when we conjugate by $\sigma$.

(**Reason:** $\sigma((12)(34))\sigma^{-1} = (\sigma_{(1)}\sigma_{(2)})(\sigma_{(3)}, \sigma_{(4)}) \in \{(12)(34), (13)(24), (14)(23)\}$)

• $\sigma(1234)\sigma^{-1} = (\sigma_{(1)}\ \sigma_{(2)}\ \sigma_{(3)}\ \sigma_{(4)})$ has 6 options, but 2 of them are already in $P_1$. (namely $(1234)$ and $(1432)$)

This confirms there are 3 Sylow 2-subgroups of $S_4$:

**Proposition:** Fix a group $G$ and $H = \langle h_i : i \in I \rangle$ a subgroup of $G$. Then, for any $g \in G$ we have $gHg^{-1} = \langle ghg^{-1} : i \in I \rangle$

**Proof:** ($\supseteq$) by definition of subgroup generated by a family of elements.

($\subseteq$) Any $h \in H$ is a word in $h_{i_1} \cdots h_{i_r}$ (only finitely many letters are involved)

Since $gh_i^{-1}g^{-1} = (gh_ig^{-1})^{-1}$ $\forall i \in I$ and $gh_i^n g^{-1} = (gh_ig^{-1})^n$ for all $n \in \mathbb{N}$

we get $h = h_{i_1}^{\ell_1} \cdots h_{i_r}^{\ell_r} \Rightarrow ghg^{-1} = (gh_{i_1}g^{-1})^{\ell_1} \cdots (gh_{i_r}g^{-1})^{\ell_r} \in \langle gh_{i_1}g^{-1}, \ldots, gh_{i_r}g^{-1} \rangle \subseteq \langle ghg^{-1} : i \in I \rangle$

$\Rightarrow ghg^{-1} \in \langle ghg^{-1} : i \in I \rangle$ $\forall h \in H$, as we wanted $\square$

$P_1 = \langle \underset{r}{(1234)}, \underset{s}{(12)(34)} \rangle$

By Proposition, we need to conjugate the generators of $P_1$ to get the other two Sylow 2-subgroups.



$\Rightarrow P_2 = (34)P_1(34) = \langle (34)(1234)(34), (34)(12)(34)(34) \rangle$

$= \langle (1243), (12)(34) \rangle \neq P_1$ because $(1243) \notin P_1$.

2-cycles in $P_2$: $(34)(1234)(34) = (1243)$

$(34)(1432)(34) = (1342)$

$P_3 = (24)(34)P_1(34)(24) = (243)P_1(243)$

$= \langle (243)(1234)(243), (243)(12)(34)(243) \rangle$

$\langle (1423), (14)(23) \rangle \neq P_1$ because $(1423) \notin P_1$.

$\neq P_2$ —— $(1423) \notin P_2$

**Conclude:** $Syl_2(S_4) = \{P_1, P_2, P_3\}$

## §16.2 Sylow subgroups of $GL_2(\mathbb{F}_5)$:

**Aside:** For any prime $p \in \mathbb{Z}_{\geq 2}$, $\mathbb{F}_p$ denotes the field with $p$ elements. As a set $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. As an additive group $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. However, $x \cdot y$ = multiplication mod $p$

(Eg: $\mathbb{F}_5 = \{0,1,2,3,4\}$ $2 \cdot 4 = 3 \pmod 5$ $4 \cdot 4 = 1 \pmod 5$ )

$GL_2(\mathbb{F}_5) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{F}_5 \quad ad - bc \neq 0 \pmod 5 \right\}$

Q: What is the size of $G = GL_2(\mathbb{F}_5)$ ?

Idea: Options for 1st column $\begin{bmatrix} a \\ c \end{bmatrix} \in \mathbb{F}_5^2 \setminus \{\begin{bmatrix} 0 \\ 0 \end{bmatrix}\}$ $\Rightarrow$ $25-1 = 24$ options.

Options for 2nd ____ $\begin{bmatrix} b \\ d \end{bmatrix} \in \mathbb{F}_5^2 \setminus \mathbb{F}_5 \langle \begin{bmatrix} a \\ c \end{bmatrix} \rangle$ (columns are l.i.)

$\Rightarrow 25 - 5 = 20$.

$\Rightarrow |G| = 24 \cdot 20 = 480 = 2^5 \cdot 3 \cdot 5$ → same primes as in $\mathbb{F}_5$.

$\Rightarrow$ Only have Sylow 2-, 3- and 5-subgroups.

- $n_2 \equiv 1 \pmod 2$ & $n_2 \mid 15$ $\Rightarrow$ $n_2 = 1, 3, 5, 15$ (all are possible)
- $n_3 \equiv 1 \pmod 3$ & $n_3 \mid 2^5 \cdot 5$ $\Rightarrow$ $n_3 = 1, 2, 4, 8, 16, 32, 10, 20, 40, 80, 160$
  so $n_3 = 1, 4, 10, 16, 160$.
- $n_5 \equiv 1 \pmod 5$ & $n_5 \mid 2^5 3$ $\Rightarrow$ $n_5 = 1, 2, 4, 8, 16, 32, 3, 6, 12, 24, 48, 96$
  so $n_5 = 1, 6, 16$ or $96$

① An example of a Sylow 5-subgroup $= \{\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} : x \in \mathbb{F}_5\} =: P$.

Another example $\{\begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} : y \in \mathbb{F}_5\} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} P \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\Rightarrow n_2 \neq 1$

② An example of a Sylow 2-subgroup

$$H = \{\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}, \begin{bmatrix} 0 & \mu_1 \\ \mu_2 & 0 \end{bmatrix} \quad \lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{F}_5 \setminus \{0\}\}$$

Claim: $H$ is a subgroup of $GL_2(\mathbb{F}_5)$

Proof: $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}\begin{bmatrix} 0 & \mu_1 \\ \mu_2 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \lambda_1\mu_1 \\ \lambda_2\mu_2 & 0 \end{bmatrix}$ & $\begin{bmatrix} 0 & \mu_1 \\ \mu_2 & 0 \end{bmatrix}\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} = \begin{bmatrix} 0 & \mu_1\lambda_2 \\ \mu_2\lambda_1 & 0 \end{bmatrix}$

$\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}^{-1} = \begin{bmatrix} \lambda_1^{-1} & 0 \\ 0 & \lambda_2^{-1} \end{bmatrix}$, $\begin{bmatrix} 0 & \mu_1 \\ \mu_2 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & \mu_1^{-1} \\ \mu_2^{-1} & 0 \end{bmatrix}$ ; $I_2 \in H$ ∎

$|H| = 4^2 + 4^2 = 32$ elements, so it's a Sylow 2-subgroups.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= \frac{1}{ad-bc}\begin{bmatrix} \lambda_1 a & \lambda_2 b \\ \lambda_1 c & \lambda_2 d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= \frac{1}{ad-bc}\begin{bmatrix} \lambda_1 ad - \lambda_2 bc & -(\lambda_1 - \lambda_2)ba \\ (\lambda_1 - \lambda_2)dc & \lambda_2 ad - \lambda_1 bc \end{bmatrix}$$

Typically not in $H$, so $n_5 \neq 1$

(2) An example of a Sylow 3-subgroup $= \langle A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \rangle$ of order 3

$\det^3 = (ad-bc)^3 = 1 \Rightarrow \det = 1$ because $4^3 = 1 \pmod 5$, $(\pm 2)^3 = \mp 2 \pmod 5$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^3 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a^2+bc & ab+bd \\ ac+dc & bc+d^2 \end{bmatrix}$$

$$= \begin{bmatrix} a^3+abc+abc+bcd & a^2b+abd+b^2c+bd^2 \\ ca^2+bc^2+acd+d^2c & abc+bcd+bcd+d^3 \end{bmatrix}$$

$$= \begin{bmatrix} a^3+bc(2a+d) & ab(a+d)+bc(b+d) \\ c(a^2+bc+ad+d^2) & bc(a+2d)+d^3 \end{bmatrix}$$

Replace $bc = ad-1 \Rightarrow$ $I_2 = \begin{bmatrix} a^3+(ad-1)(2a+d) & ab(a+d)+(ad-1)(b+d) \\ c(a^2+ad-1+ad+d^2) & (ad-1)(a+2d)+d^3 \end{bmatrix}$

$$\begin{cases} 1 = a^3+2a^2d+ad^2-2a-d & [Eq1] \\ 1 = a^2d+2ad^2-a-2d+d^3 & [Eq2] \\ 0 = c(a^2+2ad+d^2-1) = c\left((a+d)^2-1\right) = c(a+d+1)(a+d-1) & [Eq3] \\ 0 = a^2b+abd+abd+ad^2-b-d = a^2b+2abd+ad^2-b-d & [Eq4] \end{cases}$$

3 cases from [Eq3]: $c=0$ (1) or $d=-1-a$ (2) or $d=1-a$ (3)

(1) $\boxed{c=0} \Rightarrow A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = a\begin{bmatrix} 1 & b/a \\ 0 & d/a \end{bmatrix}$ $ad=1$

$\Rightarrow a[Eq1]$ $a = a^4+2a^3d+a^2d^2-2a^2-ad = a^4+2a^2+1-2a^2-1 = a^4 \pmod 5$

This is true for all $a$.

$\Rightarrow a[Eq2]$ $a = a^3d+2a^2d^2-a^2-2ad+ad^3 = a^2+2-a^2-2+d^2 = d^2$

$(a,d) = (1,1), (4,2), (4,3), (1,4)$

$\Rightarrow a[Eq4]$ $0 = a^3b+2a^2bd+a^2d^2-ab-ad = a^3b+2ab+1-ab-1$
$= a^3b+ab = ab(a^2+1)$

This can't happen since $a = \pm 1 \bmod 5$.

Conclude: $c \neq 0$.

Symmetry: $\operatorname{ord}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 3 \Rightarrow \operatorname{ord}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}^T\right) = 3$, so $b \neq 0$ as well.

(2) $\boxed{d = -(1+a)}$ Substitute in 3 equations

[Eq1] $1 = a^3 - 2a^2(a+1) + a(1+a)^2 - 2a + (1+a) = a^3 - 2a^3 - 2a^2 + a + a^3 + 2a^2 - 2a + 1 + a$

$= 1$ True for all $a$

[Eq2] $1 = -a^2(1+a) + 2a(1+a)^2 - a + 2(a+1) - (a+1)^3$

$= -a^2 - a^3 + 2a + 2a^3 + 4a^2 - a + 2a + 2 - a^3 - 3a^2 - 3a - 1 = 1$ True for all $a$.

[Eq4] $0 = a^2 b - 2ab(1+a) + a(1+d)^2 - b - d$

$= a^2 b - 2a^2 b - 2ab + a + ad^2 + 2ad - b - d = -a^2 b - 2ab + a + ad^2 + 2ad - b - d$

$= a(-ab - 2b + 1 + d^2 + 2a) - b - d$

Check options for $(a,d) = (0,-1), (1,-2), (2,2), (3,1), (4,0)$

$(a,d) = (0,-1) \rightsquigarrow 0 = -b + 1 \Rightarrow b = 1$ $\qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$c = 1$

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ order 2 ✗

$(a,d) = (1,-2) \rightsquigarrow 0 = -b - 2b + 1 + 4 - 4 - b + 2 = -4b + 3 \Rightarrow b = -3$

$1 = ad - bc = -2 + 3c \Rightarrow c = 1$ $\qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix}$

$\begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix}^2 = \begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 1-3 & -3+6 \\ 1-2 & -3+4 \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ -1 & 1 \end{pmatrix} \neq I_2$

$\begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} -2 & 3 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -2+3 & 3-3 \\ -2+2 & 3-2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ✓

**Conclusion** $H := \left\langle \begin{bmatrix} 1 & -3 \\ 1 & -2 \end{bmatrix} \right\rangle = \left\langle \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \right\rangle$ is Sylow 3-subgroup.

$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \notin H$, so $n_3 \neq 1$.

## §16.3 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.

**Proof:** By Theorem §14.2, $p$-groups have non-trivial centers. We treat 2 cases:

- If the group is not-abelian, then $\{e\} \subsetneq Z(G) \subsetneq G$. Since $Z(G) \trianglelefteq G$, we conclude that $G$ is **not** simple.

- If the group is abelian, any element $h$ of order $p$ will give $H = \langle h \rangle \trianglelefteq G$ with $H \neq \{e\}$ and $H \trianglelefteq G$. Again, we conclude that $G$ is not simple.

Such element $h$ exists. Indeed, if $g \in G \setminus \{e\}$, $\text{ord}(g) = p^l$ for $l \geq 1$. If $l = 1$, we take $h = g$. If $l > 1$, we take $h = g^{p^{l-1}}$ ( $h \neq e$ & $h^p = g^{p^l} = e$ so $\text{ord}(h) = p$ ) □

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: Prove that there are no simple groups of order 28.

Solution: Write $|G| = 28 = 2^2 7$ $\Rightarrow$ only Sylow 2- and 7-subgroups.

- $n_2 \equiv 1 \pmod 2$ & $n_2 | 7$ $\Rightarrow$ $n_2 = 1$ or $7$
- $n_7 \equiv 1 \pmod 7$ & $n_7 | 4$ $\Rightarrow$ $n_7 = 1$

Conclude: The 1 Sylow 7-subgroup is normal. It's size is $7 \neq 1, 28$, so $G$ is NOT simple.

We'll see 2 more tricks in Lecture 17.