# Lecture 16

(16.0) Recall that we have been studying the applications of Sylow theorems. In this lecture we will solve some problems of the following 2 general types.

(I) Given a finite group $G$ and a prime ~~dividing~~ $p$ dividing $|G|$, find one (or all) $Syl_p(G)$.

(II) Can we exhibit <u>one</u> non-trivial $(\neq \{e\})$, proper $(\neq G)$ <u>normal</u> subgroup of $G$?

Definition. – If $G$ is a group such that there are <u>no</u> <u>non-trivial</u>, <u>proper</u>, <u>normal</u> subgroups in $G$, then we say that $G$ is <u>simple</u>.

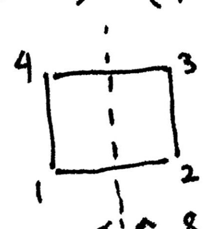
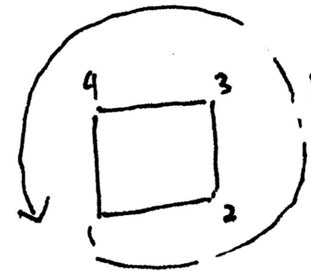
(16.1) Example 1. $G = S_4$. $|G| = 24 = 2^3 \cdot 3$.

By Sylow Thm. (part 1), $G$ has a subgroup of size 8.

e.g. $D_8 \longrightarrow S_4$ injective group hom.

$s \longmapsto (12)(34)$

$r \longmapsto (1234)$

( geometrically  $s$ = reflection  $r$ = rotation )

# Example of a Sylow 2-subgroup of $S_4$

$$P_1 = \left\{ e, \ \underset{}{\overset{(s)}{\boxed{(12)\cdot(34)}}}, \ \overset{(sr)}{(24)}, \ \overset{(sr^2)}{\boxed{(14)(23)}}, \ \overset{(sr^3)}{(13)}, \ \underset{(r)}{(1234)}, \ \underset{(r^2)}{\boxed{(13)(24)}}, \ \underset{(r^3 = r^{-1})}{(1432)} \right\}$$

Any other Sylow 2-subgroup $= \sigma P_1 \sigma^{-1}$ $(\sigma \in S_4)$ by Sylow Thm (part 2).

Three "boxed" elements of $P_1$ only get flipped around by $\mathrm{Conj}(\sigma)$: e.g. $\sigma\big((12)(34)\big)\sigma^{-1} = \big(\sigma(1)\ \sigma(2)\big)\big(\sigma(3)\ \sigma(4)\big)$

$\in \{(12)\cdot(34), (13)\cdot(24), (14)\cdot(23)\}$

↑ <u>All</u> permutations of cycle type $(2,2)$.

$$(1234) \overset{\mathrm{Conj}(\sigma)}{\longmapsto} \begin{cases} \text{six}^* \text{ options} \\ (1\ x\ y\ z) \\ (^* \ \cancel{\text{one}}\ 2 \text{ of them are in } P_1) \end{cases}$$

$\Rightarrow$ There are 3 Sylow 2-subgroups of $S_4$:

$$P_1 = \left\langle \begin{matrix} (12)\cdot(24) \\ (1234) \end{matrix} \right\rangle \xrightarrow[\mathrm{Conj}((34))]{} P_2 = \left\langle \begin{matrix} (12)\cdot(34) \\ (1243) \end{matrix} \right\rangle = (34)\cdot P_1 \cdot (34)^{-1}$$

$\Big\downarrow$ $\mathrm{Conj}((24))$

$$P_3 = \left\langle \begin{matrix} (12)\cdot(34) \\ (1423) \end{matrix} \right\rangle = (24)\cdot P_2 \cdot (24)^{-1}$$

Note : by Sylow Thm (part 3), $|G| = 24$ implies

$$\left.\begin{array}{l} n_2 \equiv 1 \pmod 2 \\ n_2 \text{ divides } 3 \end{array}\right\} \Rightarrow n_2 = 1 \text{ or } 3.$$

(16.2) $G = GL_2(\mathbb{F}_5)$.

Aside. – for any prime $p \in \mathbb{Z}_{\geq 2}$, $\mathbb{F}_p$ denotes the field with $p$ elements. As a set $\mathbb{F}_p = \{0, 1, \dots, p-1\}$

As an additive group $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Moreover,

$x \cdot y$ = multiplication mod $p$.

$$\left( \text{e.g. } \mathbb{F}_5 = \{0, 1, 2, 3, 4\} \qquad \begin{array}{l} 2 \cdot 4 = 3 \pmod 5 \\ 4 \cdot 4 = 1 \pmod 5 . \end{array} \right)$$

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

$|G| = ?$ <u>Idea</u> : Options for $1^{st}$ column $\begin{bmatrix} a \\ c \end{bmatrix} \in \mathbb{F}_5 \times \mathbb{F}_5$ except $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$

$\rightsquigarrow 25 - 1 = 24.$

Options for $2^{nd}$ column $\begin{bmatrix} b \\ d \end{bmatrix}$ : any vector except <u>scalar</u> multiples of $\begin{bmatrix} a \\ c \end{bmatrix}$ ← already picked

there are 5 scalars. $\longrightarrow$

$\rightsquigarrow 25 - 5 = 20$

$$\Rightarrow \quad |G| = 24 \cdot 20 = 480$$
$$= 2^5 \cdot 3 \cdot 5 \longleftarrow \text{same prime as in } \mathbb{F}_5.$$

Examples of Sylow 5-subgroup : $\left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} : x \in \mathbb{F}_5 \right\} =: P$

$$\left( \left\{ \begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} : y \in \mathbb{F}_5 \right\} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} P \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1}. \right)$$

An example of a Sylow 2-subgroup

$$\left\{ \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \right\} \cup \left\{ \begin{bmatrix} 0 & \mu_1 \\ \mu_2 & 0 \end{bmatrix} \right\} \qquad \text{total } 32 \checkmark.$$

(16 elts) (16 elts)

$\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{F}_5 \setminus \{0\}$

Ex. Give an example of a Sylow 3-subgroup (i.e. find $X \in GL_2(\mathbb{F}_5)$ of order 3.)

(16.3) Prove that there are no simple groups of order 28.

$|G| = 28 = 2^2 \cdot 7$.

$n_2 \equiv 1 \pmod 2$
$n_2 \mid 7$

$$\boxed{\begin{matrix} n_7 \equiv 1 \pmod 7 \\ n_7 \mid 4 \end{matrix}}$$
$$\Downarrow$$
$$n_7 = 1$$

so $G$ has a normal subgroup of size 7. Hence $G$ is not simple.

(16.4) Prove that there are no simple groups of size 224.

$|G| = 224 = 2^5 \cdot 7$.

Again, $n_2 \equiv 1 \mod 2$, $n_2 \mid 7$ $\Rightarrow n_2 = 1$ or $7$

$n_7 \equiv 1 \mod 7$, $n_7$ divides 32 $\Rightarrow n_7 = 1$ or $8$

If $n_2 = 1$ we are done. So let us assume $n_2 = 7$.
(i.e. G has a normal subgp of size 32.)

Now $G \circlearrowright Syl_2(G)$ ← has 7 elements $\Rightarrow$ we have a group hom

$g \in G$, $P \in Syl_2(G)$

$[\, g \cdot P = g P g^{-1} \,]$

$\varphi : G \longrightarrow S_7$

$G$: 224 elements

$S_7$: ~~5040~~ 5040 elements

If $\varphi$ were injective, 224 would divide $7!$ but $7!$ is not divisible by 32. ($7! = 1 \cdot \underset{\text{one } 2}{2} \cdot 3 \cdot \underset{\text{two } 2\text{'s}}{4} \cdot 5 \cdot \underset{\text{one } 2}{6} \cdot 7$
$\Downarrow$
16 divides $7!$ but not 32.)

Since $\varphi$ is not injective

$\{e\} \neq \mathrm{Ker}(\varphi) \lhd G$.

<u>Note</u>: $\mathrm{Ker}(\varphi) = G$ means $G \circlearrowright Syl_2(G)$ is trivial action which contradicts transitivity as $n_2 \neq 1$.

Hence $\text{Ker}(\varphi)$ is a proper, non-trivial, normal subgroups of $G$, implying that $G$ cannot be simple.

(16.5) Another trick - overcounting.

Let $|G| = 56 = 2^3 \cdot 7$. Again

$n_2 \equiv 1 \mod 2$
$n_2 \mid 7$
$\Rightarrow n_2 = 1$ or $7$

$n_7 \equiv 1 \mod 7$
$n_7 \mid 8$
$\Rightarrow n_7 = 1$ or $8$

If $n_7 = 1$ we are done (i.e. $G$ cannot be simple.)

If $n_7 = 8$; say $\text{Syl}_7(G) = \{P_1, \ldots, P_8\}$

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

Hence, we get $(7 - \underset{\substack{\uparrow \\ \text{identity } e \in P_i}}{1}) \cdot 8 = 48$ elements of order 7.

We are left with $\underset{e \in G}{1} + \underset{\text{left over - none of order 7.}}{7}$ elements in $G$.

As any $Q \in Syl_2(G)$ has ~~order~~ size 8, we are forced to have $n_2 = 1$. Meaning $G$ has a normal subgp. of order 8. Hence $G$ cannot be simple.

(16.6) A non-trivial example featuring all the tricks.

Assume $G$ is simple and $|G| = 60 = 2^2 \cdot 3 \cdot 5$.

Prove that $n_5 = 6$, $n_3 = 10$, $n_2 = 5$.

[ Think about this problem! ]