Sylow's theorems and applications

Goal: Find abstract ways to study groups

- similar to $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \rightsquigarrow Z_n = \prod_i Z_{p_i^{\alpha_i}}$, "reducing the study of G to each prime p"
- consider $G \curvearrowright X$ (a way to "represent" a group)

Definition. Fix a prime number p.

(1) A p-group is a finite group whose order is a p-power

(2) If G is a group with $\#G = p^r \cdot m$ with $r, m \in \mathbb{N}$, $p \nmid m$

a subgroup H of G of order p^r is called a Sylow p-subgroup (p-西罗子群)

or p-Sylow subgroup

Write $\mathrm{Syl}_p(G) := \{\text{Sylow } p\text{-subgroups of } G\}$

$n_p := \#\mathrm{Syl}_p(G)$

Theorem (Sylow's theorems) Let G be a finite group with $\#G = p^r \cdot m$ with $r, m \in \mathbb{N}$ & $p \nmid m$.

First Sylow Sylow p-subgroups exist

Second Sylow If P is a Sylow p-subgroup of G, and $Q \leq G$ is a subgroup of p-power order

then $\exists\, g \in G$, $Q \leq gPg^{-1}$ (also a Sylow p-subgroup)

i.e. • all Sylow p-subgroups are conjugate.

• all subgroups of p-power order is contained in a Sylow p-subgroup.

Third Sylow (1) $n_p \equiv 1 \bmod p$

(2) $n_p \mid m$.

Proof of 1st Sylow: (There's a more direct but trickier proof.)

We use induction on $\#G$.

When $p \nmid \#G$, i.e. $r=0 \Rightarrow \{1\} \leq G$ is the Sylow p-subgroup of G. ✓

Now, suppose that 1st Sylow is proved with smaller $\#G = n$.

Case 1: If $p \mid \#Z(G)$, then $Z(G)$ is a finite abelian group.

$$\rightsquigarrow Z(G) = \underbrace{Z_{p^{r_1}} \times \cdots \times Z_{p^{r_s}}}_{p\text{-part } Z(G)_p \neq \{1\}.\ \text{say } \#Z(G)_p = p^{r'}} \times \cdots$$

Consider $\bar{G} := G/Z(G)_p$ has order $n/p^{r'} = p^{r-r'} \cdot m$

$\uparrow \pi$

G

Inductive hypothesis $\Rightarrow \bar{G}$ contains a subgroup $\bar{H}$ of order $p^{r-r'}$

Then $\pi^{-1}(\bar{H})$ is a group of order $\#\bar{H} \cdot \#Z(G)_p = p^{r-r'} \cdot p^{r'} = p^r$

It is a Sylow p-subgroup of G.

Case 2. If $p \nmid \#Z(G)$, recall that we may assume $p \mid \#G$

Class equation $\Rightarrow$ $\underbrace{\#G}_{\text{div. by } p} = \underbrace{\#Z(G)}_{\text{not div. by } p} + \sum_{\text{nontriv orbits}} [G : C_G(g_i)]$

$\Rightarrow \exists\, i$ s.t. $[G : C_G(g_i)]$ is not divisible by p and is not 1

$\Rightarrow C_G(g_i)$ has order $p^r \cdot m'$ for some $m' \mid m$ and $m' \neq m$.

By inductive hypothesis, $\exists\, H \leq C_G(g_i)$ a Sylow p-subgroup of order p^r

$\Rightarrow H$ is a Sylow p-subgroup of G. $\square$

Proof of 2nd Sylow. $P \leq G$ a Sylow p-subgroups and $Q \leq G$ a subgroup of p-power order

When $\#Q = 1$, $Q = \{1\} \leq P$ ✓

Now assume $\#Q = p^{r'}$ with $r' \geq 1$

Consider the left translation action $Q \curvearrowright G/P = \{gP \mid g \in G\}$

Then $\underbrace{\#\, G/P}_{\text{not divisible by } p} = \sum \#\text{orbits} = \sum \#\, Q/\text{Stab}_i$

$\Rightarrow \exists$ an orbit, say the orbit of gP s.t. $\#\, Q/\text{Stab}_{gP}$ is not divisible by p.

But $\#Q$ is p-power $\Rightarrow Q = \text{Stab}_{gP}$

i.e. $\forall\, q \in Q,\ qgP = gP \Rightarrow qg \in gP \Rightarrow q \in gPg^{-1}$

So $Q \leq gPg^{-1}$ □

Cor 1. All Sylow p-subgroups are conjugate.

Cor 2. There is only one Sylow p-subgroup $\Leftrightarrow$ A Sylow p-subgroup $P \leq G$ is normal.

Proof: "$\Rightarrow$" $\forall\, g \in G$, gPg^{-1} is a Sylow p-subgroup

So $gPg^{-1} = P$ (as there's only one)

$\Rightarrow P$ is normal. (In fact, P is characteristic in G

"$\Leftarrow$" As all Sylow p-subgroups are conjugate,

any "other" Sylow p-subgroup is $gPg^{-1} \overset{\text{normality}}{=} P$ $\Rightarrow$ Only one Sylow p-subgroup

Cor 3. If P is a Sylow p-subgroup, $N_G(N_G(P)) = N_G(P)$

and $N_G(P)$ contains a unique Sylow p-subgroup.

Proof: Note: $P \trianglelefteq N_G(P)$ by tautology, so P is a normal Sylow p-subgroup of $N_G(P)$

$\Rightarrow P$ is the unique Sylow p-subgroup of $N_G(P)$

If $n \in N_G(N_G(P)) \Rightarrow n N_G(P) n^{-1} = N_G(P)$

$$\begin{matrix} n N_G(P) n^{-1} & = & N_G(P) \\ \rotatebox{90}{$\leq$} & & \rotatebox{90}{$\leq$} \\ nPn^{-1} & & P \end{matrix}$$

But $N_G(P)$ has a unique Sylow p-subgroup $\Rightarrow nPn^{-1} = P$

So $n \in N_G(P)$. □

<u>Proof of 3rd Sylow</u>: $n_p :=$ # of Sylow p-subgroup

① Since all Sylow p-subgroups are conjugate,

$G \circlearrowright \{\text{Sylow } p\text{-subgroups}\}$ action by conjugation, is transitive.

$$\Rightarrow n_p = \#\{\text{Sylow } p\text{-subgroup}\} = \#\left(G/N_G(P)\right) = \frac{p^r \cdot m}{p^r \cdot ?} \leftarrow [N_G(P):P]$$

So $n_p \mid m$

② Consider $P \circlearrowright \{\text{Sylow } p\text{-subgroups}\}$ action by conjugation

$$\Rightarrow n_p = \#\{\text{Sylow } p\text{-subgroups}\} = \sum_i \# P/\text{Stab}_i$$

- If $\text{Stab}_i \neq P$, $\# P/\text{Stab}_i$ is a p-power.
- If $\text{Stab}_i = P$, say Stab_i is the stabilizer of a Sylow p-subgroup P_i

$$\Rightarrow P \subseteq N_G(P_i)$$

But <u>Cor 3</u> $\Rightarrow N_G(P_i)$ has the unique Sylow p-subgroup P_i

$\Rightarrow P = P_i$; there's a unique such orbit.

$$\Rightarrow n_p \equiv 1 \pmod{p}$$

<u>Application of Sylow's Theorem</u>

(1) Group G of order pq, p, q prime $p<q$

- $Q :=$ a Sylow q-subgroup

  Note: $n_q \mid p$, $n_q \equiv 1 \bmod q \Rightarrow n_q = 1$

  So Q is a normal subgroup.

- $P :=$ a Sylow p-subgroup

  Note: $n_p \mid q$, $n_p \equiv 1 \bmod p$.

  Case 1: $n_p = 1$. Thus P is normal

  $\Rightarrow G = P \times Q$

  Case 2: $n_p = q \equiv 1 \bmod p$

  $\rightsquigarrow G = Q \rtimes P$

  coming from a homomorphism $P \simeq Z_p \hookrightarrow Z_{q-1} \simeq \mathrm{Aut}(Q) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$

(2) A group of order 132 cannot be a simple group

Proof: $132 = 11 \times 3 \times 4$

Suppose G is simple $\Rightarrow$ no nontriv normal subgroup

- $n_{11} \equiv 1 \pmod{11}$ $n_{11} \mid 12 \Rightarrow n_{11} = 12$ $\Rightarrow$ at least 12×10 ($= 120$) elements have order 11.
- $n_3 \equiv 1 \pmod 3$ $n_3 \mid 44 \Rightarrow n_3 = 4$ or 44 $\Rightarrow$ at least 4×2 ($= 8$) elements have order 3.
- $n_2 \neq 1 \Rightarrow \exists$ at least two Sylow 2-subgroups P_1, P_2

  $\Rightarrow$ at least $4 + 4 - 2 = 6$ elements whose order $\mid 4$.

too many elements.

(2) Let G be a finite group and N a normal subgroup, $\pi : G \twoheadrightarrow G/N$

$|G| = p^r \cdot m$, $|N| = p^{r'} \cdot m'$, $(r' \leq r, m' \mid m) \Rightarrow |G/N| = p^{r-r'} \cdot \frac{m}{m'}$

Let H be a Sylow p-subgroup, $|H| = p^r$

Claim (a) $\pi(H)$ is a Sylow p-subgroup of G/N

(b) $\ker\left(\pi|_H : H \to G/N\right) = H \cap N$ is a Sylow p-subgroup of N

Proof: $\pi|_H : H \twoheadrightarrow \pi(H)$ has kernel $H \cap N$

1^{st} Isom Thm $\Rightarrow H/_{H\cap N} = \pi(H)$

So $|H| = p^r = |H \cap N| \cdot |\pi(H)|$ $\begin{cases} |H\cap N| \text{ divides } |N| = p^{r'} \cdot m' \\ |\pi(H)| \text{ divides } |G/N| = p^{r-r'} \cdot \frac{m}{m'} \end{cases}$

This forces $|H \cap N| = p^{r'}$ and $|\pi(N)| = p^{r-r'}$.

(3) If $\#G = 105$ contains a normal Sylow 3-subgroup P_3, then $G \simeq Z_{105}$.

Proof: $n_5 \mid 3\times 7$, $n_5 \equiv 1 \pmod 5 \Rightarrow n_5 = 1$ or 21

$n_7 \mid 3\times 5$ $n_7 \equiv 1 \pmod 7 \Rightarrow n_7 = 1$ or 15

Now, we need to use the normal Sylow 3-subgroup P_3

- Consider $G \overset{Ad}{\curvearrowright} P_3$ ← since P_3 is normal

  induces: $Ad : G \to Aut(P_3) \simeq Aut(Z_3) = \{\pm 1\}$.

  But $|G| = 105$ is odd $\Rightarrow Im(Ad) =$ trivial.

  This says every element of P_3 commutes with every element of G

  $\Rightarrow P_3 \subset Z(G)$.

Now, returns to the proof of 3^{rd} Sylow

$G \overset{conj}{\curvearrowright} \{\text{Sylow 5-subgroup}\} \Rightarrow n_5 \mid \#G/\#N_G(P_5) \Rightarrow n_5 \neq 21$

↑ contains P_5 and P_3

Similar argument $\Rightarrow n_7 = 1$

$\Rightarrow$ All P_3, P_5, P_7 are normal $\Rightarrow G = P_3 \times P_5 \times P_7$