Sylow's theorem & unsolvability of the quintic

Bharathi Ramana Joshi

August 29, 2020

Motivation

Lagrange's theorem : $H \leq G \implies |H| \mid |G|$
(Nice visual proof : https://youtu.be/TCcSZEL_3CQ)
Example: $Z_2 \leq Z_4$ and $|Z_2| \mid |Z_4|$

Converse: $k \mid |G| \implies \exists H \leq G$ with $|H| = k$
Counterexample: A_4 order 12, but no subgroup of order 6

Converse special case: Cauchy's theorem

Another Proof of Cauchy's group theorem, James H. McKay

What if prime $p \mid |G|$? Consider set of tuples

$$T = \{(g_1, \ldots, g_p) : g_1 \ldots g_p = e\}$$

1. T partitioned into equivalence classes under cyclic permutations
2. Each class has either 1 or p elements $\implies |G|^{p-1} = k + pd$ (k = # size-1 classes, d = # size-p classes)
3. $p|k \implies \exists x \in G$ such that $x^p = e$

Definitions

G group, p prime

1. p-subgroup: order p^α
2. Sylow p-subgroup: subgroup order p^α, where group order $p^\alpha m (p \nmid m)$
3. $Syl_p(G)$ set of Sylow p-subgroups
4. $n_p(G) = |Syl_p(G)|$

Sylow's Theorems : Statement

1. $n_p(G) \neq 0$
2. P Sylow p-subgroup and Q any p-subgroup $\implies \exists g \in G$ such that $Q \leq gPg^{-1}$
3. $n_p(G) \equiv 1 (mod\ p)$

$|A_5| = 60 = 2^2 \times 3 \times 5, n_5 \in \{1, 6\}, n_3 \in \{1, 4, 10\}$
Aiming for contradiction, $N \trianglelefteq A_5$. Cases;

- $5 \mid |N|$ or $3 \mid |N|$
- $|N| = 4 \implies n_4 = 1, \text{ but } n_4 > 1$
- $|N| = 2 \implies N = \langle (a_1\ a_2) \rangle$.
  But $(a_1\ a_2\ a_3)(a_1\ a_2)(a_1\ a_2\ a_3)^{-1} = (a_2\ a_3) \notin \langle (a_1\ a_2) \rangle$

Sylow's Theorems : Proof outline

1. Induction to prove existence
2. Use count conjugates for 2& 3

Sylow's Theorems : Existence proof

Cases

1. $p \mid |Z(G)|$
2. $p \nmid |Z(G)|$

Existence proof : $p \mid |Z(G)|$

$$\begin{aligned}
&\iff \exists\ P \leq Z \ni |P| = p \\
&\iff |G/P| = p^{\alpha-1}m \\
&\iff \exists |P'/P| = p^{\alpha-1} \\
&\iff |P'| = p^{\alpha}
\end{aligned}$$

Existence proof : $p \nmid |Z(G)|$

$$|G| = |Z| + \sum \frac{|G|}{|C_G(g_i)|}$$

$$\iff \exists C_G(g_i) \ni |C_G(n_i)| = p^\alpha k$$

Lemma : Conjugate counting

P Sylow p-subgroup and Q any p-subgroup

$$S = \{gPg^{-1} | g \in G\} = \{P_1, \ldots, P_r\}$$

Q acts on S by conjugation

$$S = O_1 \cup \cdots \cup O_s$$

Then

$$|O_i| = |Q : N_Q(P_i)| = |Q : Q \cap N_G(P_i)| = |Q : Q \cap P_i|$$

Lemma : Conjugate counting

$$|Q \cap N_G(P_i)| = |Q \cap P_i|$$
$$\iff |P_i(Q \cap N_G(P_i))| = \frac{|P_i||Q \cap N_G(P_i)|}{|P_i \cap (Q \cap N_G(P_i))|}$$

For the particular case $Q = P (= P_1)$

$$|O_1| = 1, |O_i| = |P_1 : P_1 \cap P_i| > 1$$

Thus #conjugates

$$|S| = |O_1| + (|O_2| \ldots |O_s|) \equiv 1 (mod\ p)$$

Sylow's Theorems : Containment & Congruence to 1

Aiming for contradiction, let Q not be contained in any conjugate. Then

$$|O_i| = |Q : Q \cap P_i|$$

Thus p divides #orbits $\implies$ contradiction!

Since all Sylow p-subgroups are conjugates, $S = Syl_p(G)$

Exercises

1. Write a program that given n, finds all permissible values of n_p for all groups G of odd size $< n$ with $|Syl_p(G)| \neq 1$ for each prime divisor p of group size.
2. P normal and $P \in Syl_p(G) \implies$
   2.1 $|Syl_p(G)| = 1$
   2.2 P characteristic in G
3. G simple and $|G| = 60 \implies G \cong A5$