Section 4.5 Sylow's Theorem

Theorem 7 (Ch. 2) Suppose G is finite and cyclic. Then:

$$(k \text{ divides } |G|) \iff (\exists\, H \le G,\ |H| = k)$$

Lagranges Theorem (Theo. 8, Ch 3) Suppose G finite. Then:

$$(k \text{ divides } |G|) \Leftarrow (\exists\, H \le G,\ |H| = k)$$

Lagrange's Theorem is not an if and only if theorem.

Example: 30 divides $|A_5| = 60$. But A_5 has no subgroup H of order 30. (If so, $|G:H| = 2$, so $H \trianglelefteq G$, but A_5 is simple.)

TODAYS GOAL ~~Answ.~~

Find out for what #'s k dividing $|G|$ there is an $H \le G$, $|H| = k$.

Cauchys Theorem (Theo. 11, Ch. 3)

$$\left(\begin{matrix} p \text{ divides } |G|, \\ p \text{ is prime} \end{matrix}\right) \Rightarrow (\exists\, H \le G,\ |H| = p)$$

Proof: Let $A = \{(g_1, g_2, \dots g_p) \mid g_i \in G,\ g_1 g_2 g_3 \cdots g_p = 1\} \subseteq \underbrace{G \times G \times G \times \cdots \times G}_{p}$

Then $|A| = |G|^{p-1}$ $\quad \{g_p = (g_1 g_2 \cdots g_{p-1})^{-1}\}$

Let $K = \langle (1\,2\,3\,4 \dots p) \rangle \le S_p$ so $K \cong \mathbb{Z}_p$.

Note K acts on A as $\pi.(g_1 g_2 \cdots g_p) = (g_{\pi(1)} g_{\pi(2)} \cdots g_{\pi(p)})$

Note $\pi.(\underbrace{g_1 g_2 \cdots g_\ell}_{g} \mid \underbrace{g_{\ell+1} \cdots g_p}_{g^{-1}}) = \underbrace{(\underbrace{g_{\ell+1} \cdots g_p}_{g^{-1}} \mid \underbrace{g_1 g_2 \cdots g_\ell}_{g})}_{\text{product } 1}$

Orbit of $(g_1 g_2 \cdots g_p)$ has $|G : K_{(g_1 \cdots g_p)}|$ elements.

" " " " " 1 or p " " ".

$|G|^{p-1} = |A| = \underset{\substack{\uparrow \\ \text{\# of orbits} \\ \text{with 1 element}}}{k} + m\underset{\substack{\uparrow \\ \text{\# of orbits} \\ \text{with } p \text{ elements}}}{p} \quad \longrightarrow \quad k = |G|^{p-1} + mp \Rightarrow k | p$

$\Rightarrow k$ multiple of $p \Rightarrow k > 1$.

Orbits with 1 element: $(1,1,1,1,\dots 1)$, $(a,a,a,\dots a)$ etc.

Then $a^p = 1$, so $\langle a \rangle \le G$ has order p ■

Sylow's theorems offer more information along these lines

Definitions Let G be a group, p a prime.

1. A group of order p^α is called a p-group. Subgroups of order p^α are called p-subgroups
2. If $|G|$ has prime factorization $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ then $H \le G$ with $|H| = p_i^{\alpha_i}$ is called a Sylow p_i-group
   i.e. if $H \le G$ and $|H| = p^\alpha$ where $|G| = p^\alpha m$ and $p \nmid m$.
3. Set of sylow p-subgroups is denoted $Syl_p(G)$. Number of Sylow p-subgroups of G is $n_p(G)$ or n_p.

Example $G = A_4$ $\quad |G| = 12 = 2^2 \cdot 3^1$

Sylow 2-subgroup: $H = \{1, (12)(34), (13)(24), (14)(32)\} \cong V_4$

Sylow 3-subgroups: $\langle(123)\rangle$ $\langle(124)\rangle$ $\langle(134)\rangle$ $\langle(234)\rangle$

Theorem 18 (Sylow's Theorem)

Suppose $|G| = p^\alpha m$, p prime, $p \nmid m$. Then:

1. There is at least one Sylow p-subgroup, i.e. $Syl_p(G) \ne \emptyset$.
2. Any two Sylow p-subgroups are conjugate.
   i.e. $P, Q \in Syl_p(G) \implies Q = gPg^{-1}$ for some $g \in G$.
   Also $P \in Syl_p(G)$ and Q a p-subgroup $\implies Q \le gPg^{-1}$
3. ~~$n_p(G) = 1G$~~ If $P \in Syl_p(G)$, Then
   $n_p(G) = |G : N(P)| = 1 + kp$ for some k. Hence $n_p(G) \mid m$

Lemma Suppose $|G| = p^\alpha m$, p prime, $p \nmid m$. If $H \le G$, $|H| = p^\beta$

then $|G : H| \equiv |N_G(H) : H| \pmod p$

Proof $A = \{gH \mid g \in G\}$. H acts on A as $h.gH = hgH$.

Which cosets are fixed by this action?

$h.gH = gH \;\forall h \in H \iff hgH = gH \;\forall h \in G \iff g^{-1}hgH = H \;\forall h \in H \iff$

$g^{-1}hg \in H \;\forall h \in G \iff g \in N_G(H)$

$\boxed{\text{Therefore orbit of } gH \text{ has only one element} \iff g \in N_G(H)}$

$|A| = \left|\{gH \mid g \in N_G(H)\}\right| + \sum_{g_iH \in} |\text{orbit of } g_iH|$

(Let $\{g_1H, g_2H, \ldots g_kH\}$ be representatives of orbits with more Then 1 element)

$$|A| = \begin{pmatrix}\#\text{ of } H \text{ cosets} \\ \text{in } N_G(H)\end{pmatrix} + \sum_{i=1}^{k} |\text{orbit of } g_iH|$$

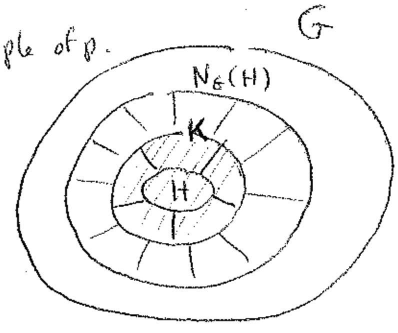
$$|G : H| = |N_G(H) : H| + \underbrace{\sum_{i=1}^{k} |H : H_{g_iH}|}_{\text{multiple of } p}$$

Then $|G : H| - |N_G(H) : H| = (\text{multiple of } p)$ ▨

Proof of ①

By Cauchy's Theorem, G has subgroup, order p. Will show:

$$\begin{pmatrix} G \text{ has subgroup} \\ \text{order } p^{\beta} \end{pmatrix} \Rightarrow \begin{pmatrix} G \text{ has subgroup} \\ \text{order } p^{\beta+1} \end{pmatrix} \quad \text{for } \beta < \alpha.$$



Suppose $H \le G$, $|H| = p^{\beta}$. Then $|G:H|$ is multiple of p.

By lemma, p divides $|N_G(H):H| = |N_G(H)/H|$

By Cauchy's Theorem $N_G(H)/H$ has a subgroup ~~$\overline{K}$ of order p~~ $\overline{K}$ of order p.

By 4th isomorphism theorem, $\overline{K} = K/H$ for some $H \le K \le N_G(H) \le G$

Then $|K| = p|H| = p \cdot p^{\beta} = p^{\beta+1}$.

Conclusion: G has sylow p-group P, $|P| = p^{\alpha}$.

Proof of ② ③, read text. ▨

<u>Corollary 20</u> Suppose $P \in Syl_p(G)$. The following are equivalent.

① P is unique Sylow p-subgroup of G, i.e. $n_p(G) = 1$.

② $P \trianglelefteq G$.

③ P char G

④ All subgroups generated by elements of orders p^i are p-subgroups.

In summary, we've achieved our goal in the following sense:

If $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ (prime factorization)
then for each $1 \le i \le n$ G has subgroups of order
$p_i \;\; p_i^2 \;\; p_i^3 \;\ldots\; p_i^{\alpha_i}$.