Group Theory
Week #7, Lecture #25

Theorem (Sylow I) If $p^k \mid |G|$ for some prime p and $k \geq 0$, then there is a subgroup $H \leq G$ of order p^k:

$$\boxed{p^k \mid |G| \implies \exists H \leq G,\ |H| = p^k} \quad (*)$$

Proof WLOG, assume $k>0$. We will use induction on the order $n = |G|$.
Clearly statement $(*)$ holds for $n=1$. So assume theorem is true for all G finite groups of order $|G| < n$.
To show it holds for $|G| = n$, we will rely on the Class Equation (for the conjugation action of G on itself):

$$\boxed{|G| = |Z(G)| + \sum_{|cl(x)|>1} [G : C(x)]} \quad \#$$

Case 1 $\boxed{\forall x \notin Z(G),\quad p \mid [G : C(x)]}$

$|cl(x)| > 1$ — so that the sum in $\#$ is divisible by p

By assumption, $p^k \mid |G|$, so $p \mid G$ (since $k>0$)
So, by $\#$,
$$\boxed{p \mid |Z(G)|}$$

Thus, by Cauchy's Theorem, $\exists a \in Z(G)$ of order p

Note: the subgroup $\langle a \rangle \subset G$ is a normal subgroup, since $g a^r g^{-1} = a^r$, $\forall r$, $\forall g \in G$ [since $a^r \in Z(G)$]

So, we may define the factor group,
$$\boxed{\bar{G} = G/\langle a \rangle},$$ with projection $\pi : G \to \bar{G}$ whose kernel is $\ker(\pi) = \langle a \rangle$.

note: $* \quad |\bar{G}| \underset{\text{Lagrange}}{=} \dfrac{|G|}{|\langle a \rangle|} = \dfrac{n}{p} < n$

$$* \quad |\bar{G}| \stackrel{\downarrow}{=} \frac{|G|}{|\langle a\rangle|} = \frac{p^k \cdot m}{p} = p^{k-1}\cdot m \implies p^{k-1} \mid |\bar{G}|$$

So, by the induction hypothesis, $\bar{G}$ has a subgroup $K \leq \bar{G}$ of order p^{k-1}.

Now let's look at the correspondence between subgroups of $\bar{G}$ and those subgroups of G containing $\ker(\pi) = \langle a \rangle$:

$$\boxed{\begin{array}{ccc} G & \xrightarrow{\pi} & G/\langle a\rangle = \bar{G} \\ \cup & & \cup \\ H = \pi^{-1}(K) & \longleftrightarrow & K = \pi(H) \end{array}}$$

Then

* $H := \pi^{-1}(K)$ is a subgroup of G, and
* $|H| = |\langle a\rangle| \cdot |K| = p \cdot p^{k-1} = p^k$ ✓

$\boxed{\text{Case 2}}$ $\boxed{\exists x \notin Z(G),\ p \nmid [G : C(x)]}$

Then:

* $n = |G| = |C(x)| \cdot \underbrace{[G : C(x)]}_{\text{coprime to } p}$ (Lagrange)
* $p^k \mid n$ (hypothesis of thm)
* $p \nmid [G : C(x)]$ (hypothesis of Case 2)

Hence:

$$\boxed{p^k \mid |C(x)|} \quad (\mathrm{i})$$

On the other hand: $C(x) \neq G$ (since $x \notin Z(G)$, so $\exists y \in G$ s.t. $yx \neq xy$, i.e. $y \notin C(x)$)

so $$\boxed{|C(x)| < n} \quad (\mathrm{ii})$$

By the induction hypothesis, $C(x)$ contains $H \leq C(x)$ of order p^k.

But $H \leq C(x) \implies H \leq G$, so done with Case (2).

Hence, done with induction step. Hence, done w/ proof! $\boxed{\text{QED}}$

Sylow p-subgroups

Let G be a finite group, and p a prime dividing $|G|$

<u>Def</u> A subgroup $P \leq G$ is a called a <u>p-Sylow subgroup</u> if $|P| = p^k$, where $p^k \mid |G|$ but $p^{k+1} \nmid G$.

<u>Eg</u> If $|G| = 40 = 2^3 \cdot 5$, then the 2-Sylow subgroups have order 8, and the 5-Sylow subgroups have order 5.

Notation:

$$\boxed{\begin{array}{l} * \ Syl_p(G) := \{ P \leq G : P \text{ is a } p\text{-Sylow subgroup of } G \} \\ * \ n_p := |Syl_p(G)| \end{array}}$$

In other words, if $|G| = p^k \cdot m$, where $(p,m)=1$, then

$$Syl_p(G) = \{ P \leq G : |P| = p^k \}$$

Anothe interpretation of p-Sylow subgroups: they are the <u>maximal</u> p-subgroups of G.

<u>Theorem</u> (Corollary to Sylow I) For every prime $p \mid |G|$, there is a p-Sylow subgroup, i.e.,

$$\boxed{Syl_p(G) \neq \emptyset}$$

<u>Proof</u> Let $p^k \mid |G|$ and $p^{k+1} \nmid |G|$, i.e. $|G| = p^k m$, $(m,p)=1$. Then, by Sylow I: $\exists\, P \leq G$, $|P| = p^k$, and so P is a p-Sylow subgroup of G. ∎

Some examples

① If G is a p-group, then $Syl_p(G) = \{G\}$

② $|G| = 6 = 2 \cdot 3$, then:

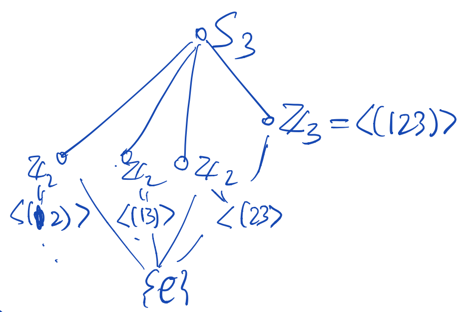
$n_2 = n_3 = 1$

- $G = \mathbb{Z}_6 \longrightarrow Syl_2(\mathbb{Z}_6) = \{\mathbb{Z}_2\}$ $\quad Syl_3(\mathbb{Z}_6) = \{\mathbb{Z}_3\}$
- $G = S_3 \longrightarrow Syl_2(S_3) = \{\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2\}$ $\quad Syl_3(S_3) = \{\mathbb{Z}_3\}$

generated by the 3 transpositions

generated by a 3-cycle

$n_2 = 3$, $n_3 = 1$



③ $G = S_3 \times \mathbb{Z}_2$ $\quad |G| = 12 = 2^2 \cdot 3$

$Syl_2(G) = \{\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2\}$, $\quad Syl_3(G) = \{\mathbb{Z}_3\}$

Theorem (Sylow II) All p-Sylow subgroups of G are conjugate:

$p \mid G$ and $P, Q \in Syl_p(G)$, then $\exists g \in G$ s.t. $Q = gPg^{-1}$

Corollary All p-Sylow subgroups of G are isomorphic.
(since conjugation is an isomorphism)

Example $G = S_4$, $|G| = 24 = 8 \cdot 3$

What are the 2-Sylow subgroups of S_4?

We know that $D_4 \leq S_4$, since $D_4 = \{$symmetries of $\square\}$ (vertices labelled 1, 2, 3, 4)

(more generally, $D_n \leq S_n$)

But $|D_4| = 8$, so $D_4 \in Syl_2(S_4)$.

Hence, by Sylow II: All 2-Sylow subgroups of S_4 are conjugate to D_4
(hence iso to D_4)

In particular, $Q_8 \nleq S_4$ (also, $\mathbb{Z}_8, \mathbb{Z}_4\times\mathbb{Z}_2, \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2 \nleq S_4$)

Theorem (Sylow III) If $|G| = p^k \cdot m$, $(p,m)=1$, then:

- $n_p \equiv 1 \pmod p$
- $n_p \mid m$ (m = index of p-Sylow)

Particular case: If $n_p = 1$, then there is a unique p-Sylow subgroup, which by Sylow II must be normal:

$$\mathrm{Syl}_p(G) = \{P\} \underset{g\in G}{\Longrightarrow} gPg^{-1} = \underset{\substack{\uparrow \\ \text{also Sylow} \\ \text{(since } |Q|=|P|)}}{Q} = P \quad \text{since } n_p = 1$$

$\therefore P \trianglelefteq G$

Corollary $n_p(G) = 1 \iff \exists!\, P$ p-Sylow subgroup of G and P is normal subgroup

In particular: $n_p(G) \Longrightarrow \exists\, P \trianglelefteq G$

so, if G is not a p-group & $n_p(G)=1$, then G is not simple.

Examples

① $|G| = 100 = 2^2 \cdot 5^2$. Then, by SIII:

$$n_5 \equiv 1 \pmod 5 \quad \& \quad n_5 \mid 4 \quad \Longrightarrow n_5 = 1$$
$$n_5 = 1, 2, \text{ or } 4$$

$\therefore \exists\, P \trianglelefteq G$ (of order 25)

$\therefore G$ is not simple

② $G = S_4$ $\quad |G| = 24 = 8\cdot 3$

$$n_2 \equiv 1 \pmod 2 \quad \& \quad n_2 \mid 3 \quad \Longrightarrow n_2 = 1 \text{ or } 3$$
$$n_3 \equiv 1 \pmod 3 \quad \& \quad n_3 \mid 8 \quad \Longrightarrow n_3 = 1 \text{ or } 4$$

we know $D_4 \in Syl_2(S_4)$. in fact, $n_2 = 3$, and

$$Syl_2(S_4) = \{3 \text{ conjugated copies of } D_4\}$$

$$= \{ \langle (1234), (12)(34) \rangle, \langle (1234), (13)(24) \rangle, \langle (1234), (14)(23) \rangle \}$$

Also, $n_3 = 4$ and

$$Syl_3(S_4) = \{4 \text{ conjugated copies of } \mathbb{Z}_3\}$$

$$= \{ \langle (123) \rangle, \langle (124) \rangle, \langle (134) \rangle, \langle (234) \rangle \}$$