26 October 2010  Algebra

In the midst of Sylow's theorem §4.5 continued
G group, \( |G| = p^m \), \( p^m \), \( p \) prime \( \neq 1 \)

**Sylow's Theorem**

1) \( n_p = n_p(G) \geq 1 \)

2) The \( p \)-Sylow subgroups of \( G \) are all conjugate.
   i.e. \( Syl_p(G) = \{S_P \} \) for some \( p \)-Sylow subgroup
   If \( H \) is any \( p \)-subgroup of \( G \), it is contained in
   a Sylow \( p \)-subgroup.

3) \( n_p \equiv 1 \pmod{p} \) and \( n_p \mid m \)

Also recall
The Cauchy Lemma of \( G \) order \( p \)
\[ P \in Syl_p(G), \ Q \text{ a } p \text{-subgroup}, \]
\[ \Rightarrow Q \cap N_G(P) = Q \cap P \]

**Proof of Sylow's theorem continued**

Let \( P \) be last time
for (2) and (3)
Set \( P \) be a Sylow \( p \)-subgroup of \( G \), using (1)
Let \( S = \{P_1, P_2, \ldots, P_r\} \) set of (distinct) conjugations of \( P \)
Let $Q$ be a $p$-subgroup of $G$.

Then $Q$ acts on $S$ by conjugation.

Let $\Theta_1, \ldots, \Theta_s$ be the orbits in $S$ under $Q$-action.

Then
\[ r = |S| = |\Theta_1| + \cdots + |\Theta_s| \]

Re-numbering if needed, can assume
\[ P_i \in \Theta_i \text{ for } 1 \leq i \leq s \]

By orbit-stabilizer formula, for each $1 \leq i \leq s$
\[ |Q| = |N_Q(P_i)| |\Theta_i| \]

Hence
\[ |\Theta_i| = \frac{|Q|}{|N_Q(P_i)|} \]

By lemma $N_Q(P_i) = P_i \cap Q$ and so
\[ |\Theta_i| = |Q : P_i \cap Q| \]

\textbf{Claim} $r \equiv 1 \pmod{p}$

\textbf{Proof}

Assume $Q = P_1$ temporarily.

\[ \therefore \Theta_1 = \{P_i\} \text{ hence } |\Theta_1| = 1 \]

\textbf{NB} $i \neq 1$, $P_i \cap P_1 \neq P_i$.

By above, $|\Theta_i| = |P_1 : P_i \cap P_1| > 1$ for $2 \leq i \leq s$

Since $P_i$ all $p$-groups, and since $|P_i| = |P_1 : P_i \cap P_1| \cdot |P_1 \cap P_i|$

we see $|P_1 : P_i \cap P_1|$ is a power of $p$.

Thus $p | \Theta_i|$

\[ r = |\Theta_1| + |\Theta_2| + \cdots + |\Theta_s| \]

\[ = 1 \text{ therefore } r \equiv 1 \pmod{p} \]
Proof of (a) Now let \( Q \) be again be an arbitrary \( p \)-subgroup of \( G \), and let \( P_1 \ldots P_r \) be as before.

Assume \( Q \leq P_1 \ldots P_r \)
\[ \therefore Q \cap P_i = Q \text{ for } \forall i \]
\[ \therefore |Q_i| = |Q : Q \cap P_i| \geq 1 \text{ for } 1 \leq i \leq r \]
\[ \therefore p \mid |Q_i| \text{ for all } 1 \leq i \leq r \]

Since
\[ r = |Q_i| + \ldots + |Q_r| \]
\[ p \mid r \quad \text{But } r \equiv 1 \pmod{p}, \text{ contradiction} \]

Thus \( Q \) is contained in at least one of \( P_1 \ldots P_r \).

In particular, if \( Q \) is a \( p \)-Sylow subgroup, then
\[ |Q| = |P_1| = \ldots = |P_r| \]

and so \( Q \in \{ P_1, \ldots, P_r \} \).

Therefore \( \text{Syl}_p(G) \) is a single conjugacy class.

Part (2) follows.
Keeping $r$ as above, follows from (2)

\[ n_p = r \equiv 1 \pmod{p} \]

By orbit-stabilizer theorem

\[ |G| = n_p \cdot |N_G(P)| \]

when $P$ is any Sylow $p$-subgroup

\[ n_p \mid p^a m \] since $|G| = p^a m$.

However, since $(n_p, p^a) = 1$, we see $n_p \mid m$.

Pt (d) follows.

\[ \square \]

Cor. \hspace{10pt} P is a Sylow $p$-subgroup of $G$, finite group

These are equivalent

1. $P$ is the unique $p$-Sylow subgroup of $G$.

2. $P \subseteq G$

3. $P$ is characteristic in $G$, that is, every automorphism of $G$ maps $P$ to itself.

4. Let $H = \langle h, \ldots, h_k \rangle$ for all $h, \ldots, h_k \in G$ s.t.

Suppose $h, \ldots, h_k$ all have $p$-power orders.

Then $H$ is a $p$-subgroup.
(1) $\Rightarrow$ (2) Because the $p$-Sylow subgroups form a single conjugacy class,

(1) $\Rightarrow$ (3) Let $\sigma : G \to G$ automorphism. Then $\sigma(P)$ is a Sylow $p$-subgroup [mb. order preserved] Thus $\sigma(P) = P$

(3) $\Rightarrow$ (2) Let $g \in G$. Then

$G \rightarrow G$

$a \rightarrow g a g^{-1}$

is automorphism of $G$

$\therefore \sigma(P) = P$

$\therefore g P g^{-1} = P$

$\therefore P \leq G$

(1) $\Rightarrow$ (4)

Let $g$ be of order power of $p$

Then $\langle g \rangle$ is a $p$-subgroup

$\therefore \langle g \rangle \leq P$ by Sylow, since $P$ is unique $p$-Sylow subgroup

Now

$H = \langle h_1, \ldots, h_k \rangle$ as assumed. Then $H \leq P$, so $|H||P|

so $H$ is a $p$-subgroup

(4) $\Rightarrow$ (1)

Suppose $P, P'$ distinct Sylow $p$-subgroups. Then

$P \not\subseteq \langle P, P' \rangle$

But $\langle P, P' \rangle$ is generated by finitely many elements of order a power of $p$

$\therefore \langle P, P' \rangle$ is a $p$-subgroup, contradiction, since Sylow $p$-subgroups are maximal $p$-subgroups.
Application

Ex. 1. Prove that there are no simple groups of order 20.

Assume \(|G| = 20 = 2^2 \cdot 5\).

Then \(n_5 = 1 \pmod{5}\) and \(n_5 \mid 2^2\).

Conclude \(n_5 = 1\) so \(G\) has a unique 5-Sylow subgroup normal in \(G\), hence \(G\) is not simple.

Example

No group order 24 simple.

\(|G| = 24 = 2^3 \cdot 3\).

Then \(n_3 = 1 \pmod{3}\)

and \(n_3 \mid 2^3\)

so \(n_3 = 1\) or \(4\).

If \(n_3 = 1\) then 3-Sylow subgroup is normal in \(G\), so \(G\) not simple.

If \(n_3 \neq 1\) then \(n_3 = 4\).

Now \(G\) acts on \(\text{Syl}_3(G)\) by conjugation.

Also \(|\text{Syl}_3(G)| = 4\).

\(\exists\) group hom. \(\psi: G \longrightarrow S_4\) via permutation rep.

Since \(|G| = 24\), \(|S_4| = 12\), so \(\psi\) not injective, hence \(\ker \psi \neq 1\), \(\psi\) not injective, hence \(\ker \psi \neq 1\), \(\psi\) not injective, hence \(\exists\) nontrivial normal subgroup of \(G\) - not simple.

\(\S\) 4.6. \(A_5\) is simple.

Read This: in fact, \(A_n\) simple if \(n \geq 5\).
Misc from Ch 5

homework due between thurs & monday

§ 5.1 DIRECT PRODUCTS

Let $G_1 \ldots G_n$ be (multiplicative) groups

Then the DIRECT PRODUCT

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n$$

$$= \{(g_1, g_2, \ldots, g_n) | g_i \in G_i\}$$

with the (product) group operation

$$(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

with identity $(1, 1, \ldots, 1)$

Prop: $G_1 \times \ldots \times G_n$ with above operation is a group.

Ref: Exercise □