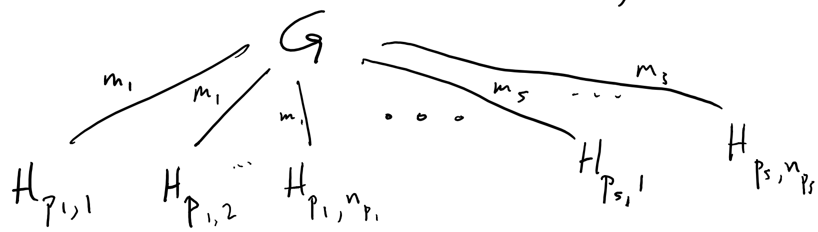
Lecture 17

Monday, February 23, 2015 9:57 AM

$$|G| = \prod_{i=1}^{s} p_i^{\alpha_i} \qquad m_j = \prod_{i \neq j} p_i^{\alpha_i}$$



Sylow Theorems

Defn G a gp, p prime

① A group of order p^α for some $\alpha \geq 0$ is a <u>p-group</u>. A subgp of G which is a p-group is called <u>p-subgroup</u>.

② If $|G| = p^\alpha m$, $p \nmid m$, then a subgp of order p^α is called a <u>Sylow p-subgroup</u>.

③ $\mathrm{Syl}_p(G) = \{ H \leq G \mid |H| = p^\alpha \}$.

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

Sylow's theorem G a gp of order $p^\alpha m$, $p \nmid m$.

① $\mathrm{Syl}_p(G) \neq \emptyset$

② $P \in \mathrm{Syl}_p(G)$, Q a p-subgp of G, then $\exists g \in G$ s.t. $Q \leq gPg^{-1}$. Moreover if $P, Q \in \mathrm{Syl}_p(G)$, then $\exists g \in G$ s.t. $Q = gPg^{-1}$.

③ $n_p \equiv 1 \pmod p$ & $n_p = [G : N_G(P)]$

(thus $n_p \mid m$)

$|G| = p^\alpha m$, $n_p = \dfrac{|G|}{|N_G(P)|}$ so $n_p \mid |G|$

since $n_p \equiv 1 \pmod p$ know $n_p \mid p^\alpha m \Rightarrow n_p \mid m$.

<u>Notation</u> If H is a p-subgp of G, write $H \leq_p G$.

<u>Lemma</u> $P \in Syl_p(G)$, $Q \leq_p G \Longrightarrow Q \cap N_G(P) = Q \cap P$.

<u>Pf</u> Set $H = N_G(P) \cap Q \geq P \cap Q$.

Thus suffices to show $H \leq P \cap Q$. $H \leq Q$ so in fact suffices to show $H \leq P$.

Strategy: Show $PH \leq_p G$. $PH \geq P$ and P is max'l among p-subgps so $PH = P \Longrightarrow H \leq PH = P$.

$H \leq N_G(P) \Longrightarrow PH \leq G$, $|PH| = \dfrac{|P||H|}{|P \cap H|} = p^\beta$

so $PH \leq_p G$. $\square$

Pf of Sylow ① by induction $|G|$. If $|G| = 1$, nothing to prove. Assume for induction that if $|H| < |G|$, then $Syl_p(H) \neq \emptyset$.

Case 1 $p \mid |Z(G)|$. Cauchy's theorem for abelian groups implies that $Z(G)$ has a subgp N of order p. $N \leq Z(G)$ so $N \trianglelefteq G$ and $|G/N| = p^{\alpha-1}m$. $< |G|$ so the induction hypothesis $\Rightarrow \exists \bar{P} \leq G/N$ w/ $|\bar{P}| = p^{\alpha-1}$. By the 4th iso thm, $\exists P \leq G$ w/ $P/N = \bar{P}$. Then

$$|P| = |N| \cdot |\bar{P}| = p \cdot p^{\alpha-1} = p^{\alpha} \text{ so}$$

$P \in Syl_p(G)$.

Case 2 $p \nmid |Z(G)|$. Take $g_1, \ldots, g_r$ reps of distinct non-central conj classes of G so that

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)].$$

Claim $\exists i$ s.t. $p \nmid [G : C_G(g_i)]$. ✓

Set $H = C_G(g_i)$ for some i s.t. $p \nmid [G : C_G(g_i)]$.

$[G:H] = \dfrac{|G|}{|H|}$ so $|H| = p^\alpha \cdot k$, $p \nmid k$.

Since $g_i \notin Z(G)$, know $H \lneq G$ so $|H| < |G|$.

By ind hyp, $\exists P \leq H$, $|P| = p^\alpha$.

Thus $P \in Syl_p(G)$. $\square$

What can we say about $P \in Syl_p(G)$?

$$\mathcal{S} = \{ gPg^{-1} \mid g \in G \} = \{P_1, P_2, \dots, P_r\}.$$

Take $Q \leq_p G$. $Q \underset{conj}{\circlearrowright} \mathcal{S} \rightsquigarrow \mathcal{S} = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \cdots \sqcup \mathcal{O}_s$.

where $\mathcal{O}_j$ are the orbits of $Q \circlearrowright \mathcal{S}$.

$$r = |\mathcal{S}| = |\mathcal{O}_1| + \cdots + |\mathcal{O}_s|.$$

Let's reorder P_i so that $P_i \in \mathcal{O}_i$ for $1 \leq i \leq s$.

By orbit-stabilizer, $|\mathcal{O}_i| = [Q : N_Q(P_i)]$.

Note $N_Q(P_i) = N_G(P_i) \cap Q$, thus by the lemma

$$N_G(P_i) \cap Q = P_i \cap Q \implies |O_i| = [Q : P_i \cap Q]$$

$1 \leq i \leq s$.

<u>Prop</u> $r \equiv 1 \pmod{p}$

<u>Pf</u> In the above, take $Q = P_1$. Then

$$|O_1| = [Q : Q \cap Q] = 1.$$

For $i > 1$, $P_1 \neq P_i$ so $P_1 \cap P_i \subsetneq P_1$.

Thus $[P_1 : P_1 \cap P_i] > 1$. In particular,

$|O_i| = [P_1 : P_1 \cap P_i]$ is divisible by p for $2 \leq i \leq s$.

Thus $r = |O_1| + (|O_2| + \cdots + |O_s|)$

$= 1 + pk$ for some integer k.

I.e. $r \equiv 1 \pmod{p}$. $\square$