Last time

$|G| = 45 = 3^2 \cdot 5$

$P \leq G$ w/ $|P| = 9 = 3^2$

$\Longrightarrow G$ abelian

$|P|$ is a maximal 3-divisor of $|G|$

Def^n $p^\alpha \mid n$ is a max'l p-divisor of n if

* $p^{\alpha+1} \nmid n$
* $n = p^\alpha m$ & $p \nmid m$

Note

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

& p_i's all distinct

$p_i^{\alpha_i}$ are the max'l p-divs.

Examples

1) $p \nmid n \Rightarrow 1 = p^0$ is the maximal p-divisor.
2) $n = p^\alpha$. Then p^α is the max'l p-divisor
3) $n = 12 = 2^2 \cdot 3$
   4 max 2-div
   3 max 3-div
   1 max p-div $\forall$ others
4) $n = 100 = 2^2 \cdot 5^2$
   4, 25, 1

Looking for $H \leq G$ where $|H|$ is a maximal p-div of $|G|$ for some p.

Def G a group. p prime.

1) A group of order p^α some α is called a p-group.
2) $H \leq G$ & H p-group $\Rightarrow H$ a p-subgroup
3) $H \leq G$ a p-subgroup & $|H| = p^\alpha$ is a max p-divisor of $|G|$ then H is a Sylow p-subgroup
4) $Syl_p(G) = \{$Sylow p-subs in $G\}$

$n_p(G) = n_p = |Syl_p(G)|$

Examples

1) $p \nmid |G| \Rightarrow \{1\} \in Syl_p(G)$
2) $|G| = p^\alpha \Rightarrow G \in Syl_p(G)$
3) Example from last time, $P \in Syl_3(G)$.
4) $|S_3| = 6 = 2 \cdot 3$

$Syl_2(S_3) = \{\langle(1\,2)\rangle, \langle(1\,3)\rangle, \langle(2\,3)\rangle\}$

$n_2 = 3$

$Syl_3(S_3) = \{\langle(1\,2\,3)\rangle\}$

$n_3 = 1$

Theorem (Sylow's Thm).

① Sylow p-subgroups exist.

② $P \in Syl_p(G)$, Q any p subgroup $\Rightarrow Q \leq gPg^{-1}$ some $g \in G$

Rmk $|gPg^{-1}| = |P| = p^\alpha$

③ $n_p \equiv 1 \pmod p$

In fact, if $P \in Syl_p G$, $n_p = |G : N_G(P)|$.

Rmk

* Sort of a converse to Lagrange
  (p^α max p-d.v $\Rightarrow \exists\ |H| = p^\alpha$)

Lemma $P \in Syl_p(G)$, Q any p subgroup.

$H = Q \cap N_G(P) = Q \cap P$

Rmk $|g| = p^t$ & $gPg^{-1} = P \Rightarrow g \in P$.

Pf/ Clear $Q \cap P \leq H$ ✓

Clear $H \leq Q$

Suffices $H \leq P$

Claim PH is p-subgroup of G.

Note Claim $\Rightarrow$ lemma.

if $P \leq PH$

$|PH| = p^\beta$ w/ $p^\beta \mid |G|$

$|P| = p^\alpha$ max p-d.v.

$\Rightarrow P = PH$

$\Rightarrow H \leq P$ & Done.

Proof of Claim

$H \leq N_G(P)$ & 2 iso thm

$\Rightarrow PH \leq G$. [Cor Is Sec 3.2]

$|PH| = \frac{|P| \cdot |H|}{|P \cap H|} = \frac{p^\alpha \cdot p^\beta}{p^\gamma} = p^{\alpha+\beta-\gamma}$

Recall G gp.

$g_1, \dots, g_r$ reps of conjugacy classes not in center.

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

Proof of Sylow's Thm

① Sylow p subgps exist.

Induct on $|G| = p^\alpha m$ [p^α-max]

Base $|G| = 1$ Trivial ✓

Inductive Assume all H w/ $|H| < |G|$ have Syl$_p$ subs.

2 cases

Case 1: $p \mid |Z(G)|$

Cauchy's Thm For Abelian

$\exists\, x \in Z(G)$ w/ $|x| = p$

$N = \langle x \rangle$, $N \trianglelefteq G$ $(N \leq Z(G))$

Let $\bar{G} = G/N$

Note $|\bar{G}| = \frac{|G|}{|N|} = \frac{p^\alpha m}{p} = p^{\alpha-1} m < |G|$

By induction

$\exists\, \bar{P} \leq \bar{G}$ w/ $|\bar{P}| = p^{\alpha-1}$

4 iso thm

$\exists\, P$ w/ $N \leq P \leq G$ & $P/N \cong \bar{P}$

$\Rightarrow \frac{|P|}{|N|} = |\bar{P}| \Rightarrow |P| = p \cdot p^{\alpha-1} = p^\alpha$

$P \in Syl_p(G)$ ✓

Case 2 $p \nmid |Z(G)|$.

Class eqn

$|G| = |Z(G)| + \sum |G : C_G(g_i)|$

$\Rightarrow \exists\, i$ w/ $|G : C_G(g_i)| = \ell$ not div by p

Call $H = C_G(g_i)$. $(k = m/\ell)$

$|H| = \frac{|G|}{\ell} = p^\alpha \cdot k$ some $k < m$ w/ $p \nmid k$.

Ind $\exists\, P \leq H \leq G$ w/ $|P| = p^\alpha$

$P \in Syl_p(G)$.

A few calculation

$P \leq G$ be p-Sylow.

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

All Sylow p-subs

If $Q \leq G$ any p sub

$Q \circlearrowright S$

$g * P_i = gP_ig^{-1}$

orbits $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_s$

Reorder P_i s.t. $P_i \in \mathcal{O}_i$

Recall $Q \circlearrowright S$

$|\mathcal{O}_i| = |Q : Q_{P_i}| = |Q : N_Q(P_i)|$

Note (lemma)

$N_Q(P_i) = N_G(P_i) \cap Q = P_i \cap Q$

Claim $r \equiv 1 \bmod p \Leftarrow$ ③

Pf/ $Q = P_1$

$\Rightarrow \mathcal{O}_1 = \{P_1\}$

$i = 2, \dots, s$ $\quad P_i \neq P_1$

$|\mathcal{O}_i| = |P_1 : P_1 \cap P_i| > 1$

Lagrange $\Rightarrow |P_1 \cap P_i| = p^\beta$

$\Rightarrow |P_1 : P_1 \cap P_i| = \frac{|P_1|}{p^\beta} = p^{\alpha-\beta} > 1$

$|\mathcal{O}_i|$ div by p

$S = \bigcup_{i=1}^s \mathcal{O}_i$

$|S| = r = \underbrace{|\mathcal{O}_1|}_{1} + (\underbrace{|\mathcal{O}_2| + \cdots + |\mathcal{O}_s|}_{\text{div by } p})$

$\equiv 1 \bmod p$

Pf of pt 2

$Q \leq G$ any p-subgroup

If $Q \not\leq P_i$ for any i

$\Rightarrow Q \cap P_i \lneq Q \ \forall i$

$\Rightarrow |Q : Q \cap P_i| > 1$

$\Rightarrow$ div by p

$\Rightarrow |\mathcal{O}_i|$ div by p

$\Rightarrow r = |\mathcal{O}_1| + \cdots + |\mathcal{O}_s| \equiv 0 \pmod p$

$Q \leq P_i = gPg^{-1}$

Proof of part 3

$n_p = \#Syl_p(G) \equiv 1 \bmod p$.

Show $n_p = r$

ie. $\forall$ sylow p subs are conj

$P, Q \in Syl_p(G)$

By pt 2

$Q \leq gPg^{-1}$

But both have order p^α

$\Rightarrow Q = gPg^{-1}$

$S = \{gPg^{-1} \mid g \in G\} = Syl_p(G)$

order $r = n_p \equiv 1 \bmod p$

$G \circlearrowright Syl_p(G)$ by conj w/ one orbit.

$|Syl_p(G)| = |G : G_P| = |G : N_G(P)|$.

Corollary

All sylow p-subs of G are isom.

Pf/ $P, Q \in Syl_p(G)$

$Q = gPg^{-1}$

$P \xrightarrow{\ \cong\ } Q$

$x \longmapsto gxg^{-1}$