March9

Tuesday, March 9, 2021 1:59 PM

Example

Groups of order 45. (Compare to HW7#6)

Let G a group $|G| = 45 = 3^2 \cdot 5$

* Suppose $\exists\ P \trianglelefteq G$ w/ $|P| = 9$. * ←

Then G is abelian.

Proof

→ $P \trianglelefteq G \implies G \circlearrowright P$ by conjugation by auts.

$$\implies G \xrightarrow{\phi} \mathrm{Aut}(P).$$

$$\mathrm{Kernel}\ \phi = \{g \in G \mid gxg^{-1} = x \quad \forall x \in P\}$$

$$= C_G(P)$$

First iso thm

$$G/C_G(P) \hookrightarrow \mathrm{Aut}(P)$$

Lagrange

$$\underline{|G/C_G(P)|} \,\Big|\, |\mathrm{Aut}(P)| \leftarrow 6, 48$$

$|P| = 3^2$

$\rightsquigarrow P \simeq \mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$

① or ~~5~~

$\underline{P \text{ abelian}}$ $\quad \mathrm{Aut}(P) \simeq \underline{(\mathbb{Z}/9\mathbb{Z})^\times}$ or $\underline{\overset{\text{HW}}{GL_2(\mathbb{F}_3)}}$

$$* \; \underset{9}{P} \leq \underbrace{C_G(P)}_{\substack{\uparrow \\ 45 \text{ or } 9}} \underset{=}{\leq} \underset{45}{G}$$

$5 \nmid 6$ & $5 \nmid 48$ *

Thus $C_G(P) = G$ so $P \leq Z(G)$.

$$* \; P \leq \underbrace{Z(G)}_{\substack{\uparrow \\ 45 \text{ or } 9.}} \leq G$$

If $|Z(G)| = 45 \implies G$ abelian.

$|Z(G)| = 9.$

$\rightsquigarrow |G/Z(G)| = 45/9 = 5$

$\rightsquigarrow G/Z(G) \simeq \mathbb{Z}_5$ THI 4a

G abelian HW6 $\boxed{2(b)?}$

$\longrightarrow$ we win $\emptyset$

Upshot

* Having large normal subgroup P was a very strong structural property for G.

  * P exists ← converse to lagrange.
  * P normal ← Nice to know how to measure.

Today

Prove a theorem to tell us

1) About existence of large subgroups

numerical ⇝ 2) Conditions for normality.

We will show

$$|G| = 45 \implies \exists\, P \trianglelefteq G \text{ w/ } |P| = 9$$

$$\implies G \text{ abelian.}$$

Defn

Let n be an integer & p a prime. A maximal p-divisor of n is a integer p^α s.t. $p^\alpha | n$ & $p^{\alpha+1} \nmid n$.

Equivalently $n = p^\alpha \cdot m$ w/ $p \nmid m$.

Ex $45 = 3^2 \cdot 5$

so 9 max'l 3-divisor
5 max'l 5-divisor
1 max'l p-divisor $\forall p \neq 3, 5$.

Def^n G a finite group. p a prime.

① A group H of order p^α is called a p-group.

② A p-group H w/ $H \leq G$ is called a p-subgroup.

③ Suppose p^α max'l p-divisor of $|G|$, and $H \leq G$ is a p-subgroup w/ $|H| = p^\alpha$. Then H is called a Sylow p-subgroup.

④ $Syl_p(G) := \{$set of sylow p-subgroups of $G\}$
$n_p(G) = n_p = \# Syl_p(G)$.

Examples

① $p \nmid |G|$. Then $Syl_p(G) = \{1\}$.

② $|G| = p^\alpha$. Then $Syl_p(G) = \{G\}$.

③ $|G| = 45$. $P \leq G$ w/ $|P| = 9$.
$P \in Syl_3(G)$

④ $|S_3| = 2 \cdot 3$

$\mathrm{Syl}_2(S_3) = \{\langle (1\,2)\rangle, \langle (1\,3)\rangle, \langle (2\,3)\rangle\}$

$\mathrm{Syl}_3(S_3) = \{\langle (1\,2\,3)\rangle\}$

$n_2 = 3$ $\quad$ $n_3 = 1$

Theorem (Sylow's Theorem)

Let G a group. $|G| = p^\alpha m$ for $p \nmid m$.

Sylow 1 (Sylow p-subgroups exist)

$\mathrm{Syl}_p(G) \neq \emptyset$.

Sylow 2 (Sylow p-subgroups are conjugate)

Let $P \in \mathrm{Syl}_p(G)$. $Q \leq G$, any p-subgroup.

Then $\exists\, g \in G$ s.t. $Q \leq gPg^{-1}$

(in part, $P, Q \in \mathrm{Syl}_p(G)$, $\exists\, g$ s.t. $Q = gPg^{-1}$)

Sylow 3 (Numerics of n_p)

(a) $n_p \equiv 1 \mod p$ ←

(b) If $P \in \mathrm{Syl}_p(G)$, then

$$n_p = [G : N_G(P)]$$

(in particular, $n_p \mid m$) ←

Proof of green

$$n_p = [G : N_G(P)] = \frac{|G|}{|N_G(P)|} = \frac{p^\alpha m}{p^\alpha t} = \frac{m}{t}$$

$$P \le N_G(P)$$

$$\Longrightarrow \quad t \cdot n_p = m \qquad \varnothing.$$

Remark

Sylow 1 is a partial of converse to Lagrange's Theorem.

Exercise

Sylow 1 $\Longrightarrow$ all $p^d \mid |G|$ $\exists$ $H \le G$ s.t. $|H| = p^d$

$\Longrightarrow$ Cauchy's Theorem. (HW 7 #36)

Consequence of Sylow

Prop $|G| = 45$. Then G abelian.

$\uparrow 3^2 \cdot 5$

proof

Sylow 1 $\Longrightarrow$ $\exists$ $P \in Syl_3(G)$ $|P| = 9$.

If normal, we're done.

Sylow 3

$n_p \equiv 1 \mod 3$

$n_p \in \{\boxed{1}, \cancel{4}, \cancel{7}, \cancel{10}, \cancel{13}, \dots\}$

& $n_p \mid 5$

P unique sub of order 9.

But $g \in G$. $gPg^{-1} \leq G$ another subgroup of order 9.

$$gPg^{-1} \in Syl_3(G) = \{P\}$$

$$\Longrightarrow gPg^{-1} = P$$

Proof of Sylow's Theorems

Proof of Sylow 1

Proceed by induction on $|G| = p^a m$ $p \nmid m$.

Base $|G| = 1$ ✓

Inductive Step

* Assume $\forall$ H w/ $|H| < |G|$, H has a Sylow p-subgroup.*

2 cases

a) $p \mid |Z(G)|$ ✓

b) $p \nmid |Z(G)|$

Case (a)

$Z(G)$ abelian. Have Cauchy for abelian groups, so $\exists\ N \le Z(G)$ w/ $|N| = p$.

$$N \le Z(G) \xrightarrow{\text{HW6 2(a)}} N \trianglelefteq G.$$

Let $\overline{G} = G/N$. $\quad |\overline{G}| = \frac{p^\alpha m}{p} = p^{\alpha-1}m.$

Induction* $\exists\ \overline{P} \le \overline{G}$ w/ $|\overline{P}| = p^{\alpha-1}$

4th iso thm

$$\left\{\begin{matrix}\text{subs}\\ N\le H\le G\end{matrix}\right\} \xleftrightarrow{\text{HW\#5.1}} \left\{\begin{matrix}\text{subs}\\ \overline{H}\le \overline{G}\end{matrix}\right\}$$

$$N \le P \le G \longleftarrow\!\!\shortmid\ \overline{P}$$

HW7 #3(a)

$$\frac{p^\alpha m}{|P|} = [G:P] = [\overline{G}:\overline{P}] = \frac{p^{\alpha-1}m}{p^{\alpha-1}} = m$$

$\rightsquigarrow |P| = p^\alpha \rightsquigarrow P \in Syl_p(G).$

Case (b) $\quad p \nmid |Z(G)|$

Class Equation

✓

$$\underset{\substack{\uparrow \\ \text{div by} \\ p}}{|G|} = \underset{\substack{\uparrow \\ \text{not div} \\ \text{by } p}}{|Z(G)|} + \sum \underset{\substack{\uparrow \\ \text{Not all div by} \\ p}}{|G : C_G(g_i)|}$$

div by p + not div by p $\Longrightarrow$ Not all div by p

$\exists$ a $g_i \in G$ $\quad H = C_G(g_i)$ s.t.

1) $|G:H| = \ell \leftarrow$ not div by p

2) $H \neq G \leftarrow g_i \notin Z(G)$.

Then $$\underset{\substack{\uparrow \\ P \in Syl_p(H)}}{|H|} = \frac{p^\alpha m}{\ell} = p^\alpha \cdot \underset{\substack{\uparrow \\ \text{int}}}{\frac{m}{\ell}} < |G|$$

* **Induction** $\quad \exists \quad P \leq H \leq G$

& $\quad |P| = p^\alpha \quad$ so $\quad P \in Syl_p(G)$ $\varnothing$

To prove 2 & 3, use group actions

Following: (Keith Conrad, Sylow Theorems).

Def^n (Fixed Points of an action)

Let G act on a set A. The fixed points of the action are

$$A^G = \mathrm{Fix}_G(A) = \{x \in A \mid g \cdot x = x \quad \forall g \in G\}$$

Ex

- $G \circlearrowright A$ trivially. $A^G = A$

- $S_n \circlearrowright \underbrace{\{1, 2, \ldots, n, n+1\}}_{A} \rightsquigarrow \mathrm{Fix}_{S_n}(A) = \{n+1\}$

- $G \circlearrowright G$ by conjugation.

$$\mathrm{Fix}_G(G) = \{x \in G \mid gxg^{-1} = x \quad \forall g \in G\}$$
$$= Z(G).$$

Theorem (Fixed Point Congruence)

Let G be a p-group.
Let A be a finite set.
Let $G \circlearrowright A$.

$$|A^G| \equiv |A| \mod p.$$

pf/

$$A = A^G \cup \underbrace{G * a_1 \cup \cdots \cup G * a_n}_{\text{union of orbits.}}$$

$$\rightsquigarrow |A| = |A^G| + \underline{|G * a_1| + \cdots + |G * a_n|}$$

Notice orbit stabilizer

$$|G * a_i| = |G : G_{a_i}| \equiv 0 \mod p$$

$$\uparrow$$

divides $|G| = p^n$

Corollary

G a p-group acting on a finite set A. If $p \nmid |A|$ then the action has a fixed point.

Pf/ $|A^G| \equiv |A| \mod p$

$$\uparrow \ne 0.$$

Proof of Sylow 2

$P \in Syl_p(G)$ $\quad Q \le G$ a p-subgroup.

If $|Q| = 1 \rightsquigarrow Q \le P$ done.

So Q nontrivial p-group.

$Q \circlearrowright G/P$ by left mult.

$$q \cdot (xP) = qxP.$$

But $|G/P| = \frac{p^a m}{p^a} = m$ & $p \nmid m$

So action has a fixed pt xP.

$$qxP = xP \qquad \forall\ q \in Q$$

$$\text{so} \quad qx \in xP \qquad \forall\ q \in Q$$

$$\text{so} \quad q \in xPx^{-1} \qquad \forall\ q \in Q$$

$$\text{so} \quad Q \le xPx^{-1}$$

Proof of Sylow 3

(a) Fix $P \in Syl_p(G)$. Let

$$P \circlearrowright Syl_p(G) \text{ by conjugation:}$$

$$Q \in Syl_p(G), \quad x \in P$$

$$x * Q = xQx^{-1} \in Syl_p(G).$$

$$\underset{\equiv}{n_p} = |Syl_p(G)| \equiv |\{\text{fixed pts}\}| \mod p$$

Goal If I show 1 fixed point,

$$\implies n_p \equiv 1 \mod p. \leftarrow$$

Lemma $\{\text{Fixed pts}\} = \{P\} \leftarrow$

$\supseteq$ ✓ $(x \in P \implies xPx^{-1} = P$

$\subseteq$ $Q \in Syl_p(G)$ & $xQx^{-1} = Q \quad \forall\ x \in P.$

$\implies P \le N_G(Q)$ & $Q \le N_G(Q)$

& $P, Q \in Syl_p(N_G(Q))$

Sylow 2 $\implies \exists\ g \in N_G(Q)$ s.t.

$$gQg^{-1} = P$$

But wait $Q \trianglelefteq N_G(Q)$

So $gQg^{-1} = Q$. So $P = Q$

Sylow 3 (b)

Goal $n_p = |Syl_p(G)|$ $P \in Syl_p(G)$

$\rightsquigarrow n_p = [G : N_G(P)]$

$G \circlearrowleft Syl_p(G)$ by conjugation.

Then $G * P = Syl_p(G)$ (by Sylow 2)

$$n_p = |Syl_p(G)| = |G * P| \underset{\substack{\uparrow \\ \text{orbit} \\ \text{stab}}}{=} [G : G_P] \underset{\uparrow}{=} [G : N_G(P)]$$

$G_P = \{g \in G \mid gPg^{-1} = P\} = N_G(P)$

Corollary All Sylow p-subgroups are isomorphic.

Pf/ Conjugate subgroups are isomorphic so done by Sylow 2.

Corollary G a finite group. $P \in Syl_p(G)$.

$$P \trianglelefteq G \iff n_p = 1.$$

Proof

$$Syl_p(G) = \{gPg^{-1} \mid g \in G\} \qquad \underline{\text{Sylow } 2}$$

↑ only 1 $\iff$ P normal

⊘

Examples

① G abelian, then exists a unique sylow p-subgroup for all p.

Proof

$P \in Syl_p(G)$, G abelian $\Longrightarrow P \trianglelefteq G$

$\Longrightarrow n_p = 1$ ⊘

② $|S_3| = 2 \cdot 3$

$\mathrm{Syl}_2(S_3) = \{\langle(1\,2)\rangle, \langle(1\,3)\rangle, \langle(2\,3)\rangle\}$

$n_2 = 3 \equiv 1 \mod 2.$

$n_2 \mid 3$

③ $|S_4| = 2^3 \cdot 3$

Sylow 3-subs

$n_3 \mid 8$ & $n_3 = \{\cancel{1}, \textcircled{4}, \cancel{7}, \cancel{10}, \dots\}$

So $n_3 = 1, 4$

$\langle(1\,2\,3)\rangle \le S_4$ order 3

$\not\ni$

$(1\,2\,4)$ ← a conjugate by some shape.

$n_p \neq 1$

$$\mathrm{Syl}_3(S_4) = \left\{ \begin{matrix} \langle(1\,2\,3)\rangle & \langle(2\,3\,4)\rangle \\ \langle(1\,2\,4)\rangle & \langle(1\,3\,4)\rangle \end{matrix} \right\}$$

Sylow 2 subgroups (order 8)

HW 3 #5

$D_8 \longrightarrow S_4$

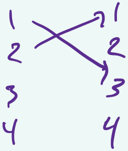
So all Sylow 2 subs in S_4 are $\cong D_8$

$n_2 = \{ \cancel{1}, 3, \cancel{5}, \cancel{7}, \dots \}$ $\quad n_2 | 3$

$(1\ 2\ 3\ 4) \in D_8$

$\big\downarrow$ conjugate

$(1\ 3\ 4\ 2) \notin D_8$



$D_8 \ntrianglelefteq S_4$

3 subs of S_4 $\cong D_8$

Groups of order pq

$|G| = pq \qquad p < q \qquad$ prime.

Fix $\quad P \in Syl_p(G) \quad \& \quad Q \in Syl_q(G)$

Claim 1 $\quad Q \trianglelefteq G.$

pf/ $n_q \equiv 1 \mod q \quad \& \quad n_q | p < q \Rightarrow n_q = 1.$

Claim 2

$$P \trianglelefteq G \iff G \simeq \mathbb{Z}_{pq}$$

Pf/ $\Leftarrow$ ✓

$\Rightarrow$

$G \curvearrowright P$ by conj

$$\begin{tikzcd} G \arrow[r] \arrow[d] & \mathrm{Aut}(P) \simeq (\mathbb{Z}/p\mathbb{Z})^{\times} \\ G/C_G(P) \arrow[ur, hook] & \end{tikzcd}$$

oder $p-1$

$$P \le C_G(P) \le G$$

p, pq

order ① or p $\quad p > p-1$

$$C_G(P) = G \implies P \le Z(G) \le G$$

$\dashrightarrow$ G abelian (exercise).

An abelian group order pq cyclic.

$\exists\, x, y \in G \quad |x| = p \quad |y| = q$

show $|xy| = pq$.

Corollary $p \nmid q-1 \implies G \simeq \mathbb{Z}_{pq}$

Pf/ $n_p = 1 + kp$ & divides q

so $n_p = 1$ or ~~$\underline{\underline{q}}$~~ $\implies \underline{\underline{kp = q-1}}$

$\lightning$.

Remains:

Classification of

1) finite abelian groups

2) Small groups.

Direct & Semidirect Product.