Sylow Theorems (II)

Thursday, 24 February 2022 11:57

Recall: G finite, p prime

$|G| = p^n \cdot m$, p doesn't divide m $n \geq 0$.

A p-Sylow subgp is a subgp of size p^n

1^{st} Sylow: Every G has a p-Sylow subgp

Prop ☆: If X is G-set and $|G| = p^k$, then $|X_G| \equiv |X| \pmod p$

Normalizer: $N[H] := \{g \in G \mid gHg^{-1} = H\}$

$H \trianglelefteq N[H] < G$

Second Sylow Theorem: Any two p-Sylow subgps are conjugate of each other.

Proof: Let P_1, P_2 are two (distinct) p-Sylow subgps of G.

$X = \{\text{Left cosets of } P_1\}$

P_2 acts on X, by $y \cdot (xP_1) = (yx)P_1$

$$|X_{P_2}| \equiv |X| \equiv (G : P_1) \equiv \frac{p^n m}{p^n} \equiv m \pmod p$$
$$\not\equiv 0 \pmod p$$

In particular $|X_{P_2}| \neq 0$.

So $\exists\, xP_1 \in X_{P_2}$, i.e.

$yxP_1 = xP_1 \quad \forall y \in P_2$

$\Rightarrow x^{-1}yxP_1 = P_1 \quad \forall y \in P_2$

$\Rightarrow x^{-1}yx \in P_1 \quad \forall y \in P_2$

Now $\varphi : P_2 \to P_1$ given by $y \mapsto x^{-1}yx$.

φ is injective and φ is between P_1, P_2 of the same size p^n.

$\therefore$ φ is bijective

$\Rightarrow \varphi(P_2) = P_1 \Rightarrow x^{-1}P_2x = P_1$ $\square$

Third Sylow Theorem: Let n_p be the # of p-Sylow subgps.

(1) $n_p \equiv 1 \pmod p$

(2) n_p divides $|G| = p^n \cdot m \iff n_p$ div m.

Proof: Fix a p-Sylow subgp P.

$X = \{$ p-Sylow subgps of $G \}$

P acts on X by conjugation:

$x \cdot T = x T x^{-1}$. ← Still a p-Sylow subgp

What is X_P? Suppose $T \in X_P \subseteq X$.

$gTg^{-1} = T, \forall g \in P$

$\Rightarrow P \leq N[T], \; T \leq N[T]$.

$\Rightarrow P, T$ are p-Sylow subgps of $N[T]$. ($T \leq N[T] \leq G$
p^n divides $\underbrace{|N[T]|}_{p^n \cdot m'}$ divides $p^n \cdot m$)

By 2^{nd} Sylow in $N[T]$,

$P = gTg^{-1}$ for some $g \in N[T]$
$= T$ (T is normal in $N[T]$)

$\Rightarrow X_P = \{P\}$

By Prop ☆, $n_p = |X| \equiv |X_P| \equiv 1 \pmod{p}$

$X = \{p\text{-Sylow subgps}\}$

G acts on X by $g \cdot P = gPg^{-1}$.

By 2^{nd} Sylow, the orbit of P is the whole of X.

$n_p = |X| = |\mathcal{O}_P| = \dfrac{|G|}{|G_P|}$ divides $|G|$.

$\square$

Example: Suppose $|G| = 15 = 3 \times 5$.

What is n_5?

$n_5 \equiv 1 \pmod{5}$ $n_5 = 1, 6, 11, 16, \ldots$

n_5 divides $15 \Rightarrow n_5 = 1$

Let P be the 5-Sylow subgp

P is normal (because gPg^{-1} is also 5-Sylow, must be P)

So G is not simple

(Simple means no proper normal subgp)

G/P is well-defined

$P \cong \mathbb{Z}_5$, $G/P \cong \mathbb{Z}_3$.

"G is formed by $\mathbb{Z}_3$ and $\mathbb{Z}_5$".

Def: A group G is solvable if there is a chain of subgps

$$G = G_k > G_{k-1} > G_{k-2} > \dots > G_0 = \{e\}.$$

such that G_i is normal in G_{i+1} and G_{i+1}/G_i is abelian, $\forall i$.

Example: A group G of size 15 is solvable, $G > \underset{\text{5-Sylow}}{P} > \{e\}$

$G/P \cong \mathbb{Z}_3$, $P/\{e\} \cong \mathbb{Z}_5$ are abelian

Exer: S_3 is solvable.

$S_3 \triangleright A_3 \triangleright \{e\}$

$S_3/A_3 \cong \mathbb{Z}_2$, $A_3/\{e\} \cong \mathbb{Z}_3$.

Fact: S_4 is solvable

Fact: A_5 is not solvable b/c

A_5 is simple but not abelian

$A_5 \triangleright \{e\}$ $\quad A_5/\{e\}$ " "

S_5 is not solvable

Foreshadowing Galois theory.

Linear eq $ax+b=0$, easy

Quadratic eq $ax^2+bx+c=0$, $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$

Cubic, quartic eq, formulae exist

Quintic eq has no "formula",

So they are not "solvable".

Prop: A finite group is solvable

$\Leftrightarrow \exists\ G = G_k \triangleright G_{k-1} \triangleright \cdots \triangleright G_0 = \{e\}$

$G_{i+1}/G_i \cong \mathbb{Z}_{p_i}$ for some prime p_i.

Prop: A finite p-group G is solvable.

$|G| = p^n$

Proof: From 1st Sylow, there exist G_i's of size p^i s.t. G_i is normal in G_{i+1}, and $G_{i+1}/G_i \cong \mathbb{Z}_p$ $\square$

Thm: Every group of odd size is solvable. (Feit-Thompson '63, 255 pages)

Def: Let $H, K \leq G$.

Then $H \vee K$ is the smallest subgp of G that contains both H and K.

Example: $4\mathbb{Z}, 6\mathbb{Z} \leq \mathbb{Z}$

$J = 4\mathbb{Z} \vee 6\mathbb{Z} = ?$ $\quad \begin{matrix} 6 \in J \\ 4 \in J \end{matrix} \Rightarrow 2 \in J$

$\Rightarrow 2\mathbb{Z} \subseteq J$

But $4\mathbb{Z}, 6\mathbb{Z} \leq 2\mathbb{Z}$, $J \subseteq 2\mathbb{Z}$ b/c J is the smallest, i.e. $J = 2\mathbb{Z}$.

$$H \vee K = \bigcap_{H, K \leq J \leq G} J$$

Prop: Suppose $H, K \trianglelefteq G$, and $H \cap K = \{e\}$, $H \vee K = G$. Then $G \cong H \times K$.

Proof: Skipped (Lemma 37.5) $\square$

Thm: If $p<q$ are primes. Then every G of size pq has a normal subgp of size q.
If furthermore $q \not\equiv 1 \pmod p$, then $G \cong \mathbb{Z}_{pq}$.

Proof: $n_q \equiv 1 \pmod q$ and n_q divides pq (i.e. divides p).
So $n_q = 1$ and the unique q-Sylow subgp Q is normal.
If $q \not\equiv 1 \pmod p$, then $n_p \equiv 1 \pmod p$ and n_p divides pq (i.e. divides q).
So $n_p = 1$ and the unique p-Sylow subgp P is normal.

$|P| = p$, $|Q| = q \Rightarrow P \cong \mathbb{Z}_p$, $Q \cong \mathbb{Z}_q$

Consider $P \cap Q$, any non-identity element of P has order p, similarly for Q, so P and Q have no common elements other than e.

Let $J = P \vee Q$. Because $P, Q \leq J$, by Lagrange thm, $|J|$ is divisible by $|P| = p$, $|Q| = q$, so $|J|$ is at least $\operatorname{lcm}(p, q) = pq$.

Hence $J = G$, i.e., $P \vee Q = G$.

By Prop, $G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q$

$$\cong \mathbb{Z}_{pq} \qquad \square$$

Example: A group of size 15 must be $\cong \mathbb{Z}_{15}$.

$$15 = 3 \times 5$$