Sylow Theorems (I)

Wednesday, 23 February 2022 13:56

Goal: Understand the structure of (finite) groups.

Example (finite abelian groups):

$G \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$.

$G \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8}_{\text{2-Sylow}} \times \underbrace{\mathbb{Z}_3}_{\text{3-Sylow}} \times \underbrace{\mathbb{Z}_{49}}_{\text{7-Sylow}}$

Philosophy:

(1) Understand the "simpler pieces" of the group

(2) Understand how they "paste" together.

FAG: (1) Cyclic subgp of p^r order

(2) Direce product.

General finite groups?

(1) Special subgp

(2) Sec 35, etc

Q. Which subgp can we expect?

Can we expect $H \leq G$, $|G| = 10$, $|H| = 3$?

Lagrange thm: $|H|$ must divide $|G|$.

Converse of Lagrange is not true!

$|A_4| = 12$ has no subgp of size 6.

A. We can expect subgp whose size is p^r, p prime.

Def: G finite. p prime. $n \geq 0$.

$|G| = p^n m$, p doesn't divide m.

$120 = 2^3 \cdot 15$, $1225 = 7^2 \cdot 25$

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

Might not be abelian/cyclic

1st Sylow: Existence

2nd Sylow: Relation

3rd Sylow: Enumeration

$a \equiv b \pmod{p}$

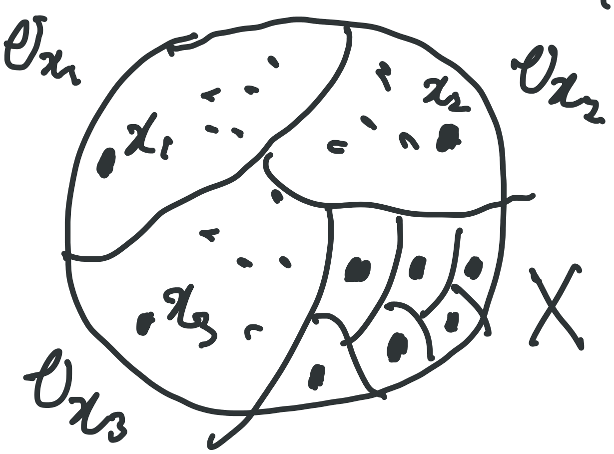
$\Leftrightarrow$ $a-b$ is a multiple of p.

Recall: Let X be a G-set.

$x \in X$. $\mathcal{O}_x = \{g \cdot x \mid g \in G\}$.

$G_x = \{g \mid g \cdot x = x,\ g \in G\}$.

$$|\mathcal{O}_x| = |G| / |G_x| \in \mathbb{N}.$$



$$|X| = \underbrace{|\mathcal{O}_{x_1}| + |\mathcal{O}_{x_2}| + \cdots}_{|\mathcal{O}| \geq 1} + \underbrace{\cdots + |\mathcal{O}_{x_k}|}_{|\mathcal{O}| = 1}$$

$$= \sum_{i=1}^{r} |\mathcal{O}_{x_i}| + |X_G|$$

X_G = all orbits of size $\underline{1}$

$= \{x \mid g \cdot x = x, \forall g \in G\}$

= "Fixed elements".

Proposition ☆: $|G| = p^n$, $n > 0$

X is G-set. Then

$|X| \equiv |X_G| \pmod{p}$.

Proof: $|X| - |X_G| = \boxed{\sum_{i=1}^{r} |\mathcal{O}_{x_i}|}$ multi of p

$|\mathcal{O}_{x_i}| = \frac{|G|}{|G_{x_i}|}$ divides $|G| = p^n$.

If $|\mathcal{O}| > 1$, then $|\mathcal{O}|$ must be a multiple of p. $\square$

X, G, X_G, compute either $|X|$ or $|X_G|$.

Cauchy's Theorem: If p divides $|G|$. Then G has an element of order p, hence, a subgp of size p.

Proof:

$$X = \{(g_1, \dots, g_p) \mid g_i \in G, \underline{g_1 g_2 \dots g_p = e}\}$$

$H = \mathbb{Z}_p$ acts on X by rotation.

$1 \cdot (g_1, \dots, g_p) = (g_2, \dots, g_p, g_1)$

$2 \cdot (g_1, \dots, g_p) = (g_3, g_4, \dots, g_p, g_1, g_2)$

etc

Check $H \curvearrowright X$ is really a group action.

(i) $e \cdot x = x$ ✓

(ii) $g \cdot (h \cdot x) = (gh) \cdot x$ ✓

(iii) $g \cdot x$ is still inside X. $\quad G \times X \to X$

$g_1(g_2 \dots g_p) = e$

$$g_1 = (g_2 \dots g_p)^{-1}$$

$$(g_2 \dots g_p) g_1 = e$$

$|X| = |G|^{p-1}$ because we can arbitrarily choose $g_1, \dots, g_{p-1}$, and pick g_p uniquely as $(g_1 \dots g_{p-1})^{-1}$.

What is X_H? If $(g_1, \dots, g_p) \in X_H$,

$$\begin{array}{cccc} g_1 & g_2 & \cdots & g_p \\ \shortparallel & \shortparallel & \cdots & \shortparallel \\ g_2 & g_3 & \cdots & g_1 \end{array} \Rightarrow g_1 = \dots = g_p.$$

$$X_H = \{(g, \dots, g) \mid g \in G, g^p = e\}$$

By Prop ☆, $|X_H| \equiv |X| \equiv |G|^{p-1} \equiv 0 \pmod p$

$(e, e, \dots, e) \in X_H \Rightarrow |X_H| > 0 \Rightarrow |X_H| \geq p > 1.$

So $\exists\, (g, \dots, g) \in X_H$, $g \neq e$.

which must have order p. $\square$

Def: A p-group G is a group in which every element's order is a power of p.

Exer: A finite gp G is a p-group $\Leftrightarrow$ $|G| = p^n$.

Normalizer: Let $H \leq G$.

The normalizer $N[H]$ is

$$\{g \in G \mid gHg^{-1} = H\}.$$

Example: If $H \trianglelefteq G$, $N[H] = G$.

Prop: (1) $N[H] \leq G$

(2) $H \trianglelefteq N[H]$. ($N[H]$ is the max subgp w/ this property)

Lemma: Suppose H is finite.

$g \in N[H] \iff ghg^{-1} \in H$ for every $h \in H$.

Proof: "$\Rightarrow$" Easy

"$\Leftarrow$": $\varphi : H \to H$, $\varphi(h) = ghg^{-1}$.

φ is injective $\quad gh_1g^{-1} = gh_2g^{-1}$

$h_1 = h_2$

But an inj map between two finite sets of same size must be bijective. $\varphi(H) = H$ $\square$

Lemma is false in general if H is not finite!

Lemma: If $H \leq G$, $|H| = p^k$, then $(N[H] : H) \equiv (G : H) \pmod p$.

Proof: $X = \{\text{Left cosets of } H \text{ in } G\}$

H acts on X by left translation

i.e. $h \cdot (gH) = (hg) \cdot H$

$|X| = (G:H) = \frac{|G|}{|H|}$.

$$gH \in X_H \iff h \cdot (gH) = gH, \ \forall h \in H$$
$$\iff (g^{-1}hg)H = H, \ \forall h$$
$$\iff g^{-1}hg \in H, \ \forall h$$
$$\iff g^{-1} \in N[H] \quad (\text{Previous lemma})$$
$$\iff g \in N[H] \quad (N[H] \text{ is a subgp})$$
$$\iff gH \text{ is a coset of } H \text{ in } N[H]$$

By Prop ☆,

$$(N[H]:H) = |X_H| \equiv |X| \equiv (G:H) \pmod{p}$$ □

First Sylow Theorem: G finite

$|G| = p^n \cdot m$. Then there exists

a p-Sylow subgp of G.

(a subgp of size p^n).

Stronger statements:

(1) $\forall\, 1 \le i \le n$, G has a subgp of size p^i.

(2) $\forall\, H \le G$, $|H| = p^i$, $i < n$, G has a subgp H' of size p^{i+1}, and $H \lhd H'$.

Proof: Proof by induction on i.

Base case $i=1$ is Cauchy's thm.

By induction, let $H \leq G$ be a subgp of size p^i, $i<n$.

Consider $N[H]$.

$$\begin{aligned}(N[H]:H) &\equiv (G:H) \pmod p\\ &\equiv |G|/|H| \pmod p\\ &\equiv p^{n-i}\cdot m \pmod p\\ &\equiv 0 \pmod p\end{aligned}$$

Now $N[H]/H$ is a legit quotient gp, and p divides $|N[H]/H|$

By Cauchy thm, there exists a subgp $K \leq N[H]/H$ of size p.

Let $\gamma : N[H] \to N[H]/H$ $(g \mapsto gH)$

$H' = \gamma^{-1}(K)$ is a subgp of size p^{i+1} in $N[H]$, hence in G.

$$H \trianglelefteq H' \leq N[H]$$

$$H \trianglelefteq N[H]$$

For (2), in the induction we started with an arbitrary H.

$\square$