Lecture 8: Sylow Theorems

Fix G finite group acting on a set X : $G \circlearrowright X$.

Counting Lemmas: (1) $|G| = |G\cdot x|\,|\mathrm{Stab}_G(x)|$ $\forall x \in X$

(2) $$|X| = \sum_{x_\alpha \in G\backslash X} |G\cdot x_\alpha| = \sum_{x_\alpha \in G\backslash X} \frac{|G|}{|\mathrm{Stab}_G(x_\alpha)|}$$

Burnside' Lemma (Frobenius, 1887).

$$|G\backslash X| = \frac{1}{|G|} \sum_{g\in G} |X^g| = \frac{1}{|G|}\sum_{x\in X} |\mathrm{Stab}_G(x)|$$

§1 Applications to p-groups: p = positive prime number

Def: A group G is a p-group if $G = p^k$ for some $k \in \mathbb{Z}_{\geq 1}$.

Eg: $G = \mathbb{Z}/p^k\mathbb{Z}$ is a p-group.

Lemma: Let G be a p-group acting on a finite set X. Then
$$|X| \equiv |X^G| \mod p.$$

Here: $X^G = \bigcap_{g\in G} X^g = \{x \in X : g\cdot x = x \ \forall g \in G\}$ $\leftrightarrow$ size 1 orbits.

Proof: By Counting Lemma: $$|X| = \sum_{\alpha \in G\backslash X} |G\cdot x_\alpha| = \underset{\text{orbits of size 1}}{|X^G|} + \underbrace{\sum_{\substack{\alpha\in G\backslash X\\ |G\cdot x_\alpha|>1}} |G\cdot x_\alpha|}_{p\,|}$$

$\Rightarrow |X| \equiv |X^G| \mod (p)$.

since $1 < |G\cdot x_\alpha| \,\big|\, |G| = p^k$

Prop: Given any prime $p \in \mathbb{Z}_{\geq 2}$ & $m \in \mathbb{Z}_{\geq 1}$, we have $\binom{p^r m}{p^r} \equiv m \pmod p$

Proof: (1) Induct on r

(2) Use group actions! Take $G = \mathbb{Z}/p^r\mathbb{Z}$, $X = \{x_1, \ldots, x_m\}$ any set with m elements.

- E = set of all p^r element subsets of $G \times X$. $\rightsquigarrow |E| = \binom{p^r m}{p^r}$

- $G \circlearrowright G \times X$ by $\sigma(g,x) = (\sigma \cdot g, x)$

So $G \circlearrowright E$ by $\sigma\{e_1, \dots, e_{p^r}\} = \{\sigma(e_1), \sigma(e_2), \dots, \sigma(e_{p^r})\} \in E$ ✓

(axioms for left action are satisfied)

- By Lemma: $\boxed{|E| \equiv \#(\text{of orbits with exactly one element}) \pmod p}$

Let's count how many such orbits we have: 2^{nd} entry of each member of the orbit is fixed & $G \circlearrowright G$ is transitive.

$\Rightarrow$ Orbits are $\{(g,x_1) : g \in G\}, \{(g,x_2) : g \in G\}, \dots \{(g,x_m) : g \in G\}$

$\Rightarrow$ m of them!

We get $\binom{p^r m}{m} = |E| \equiv m \mod (p)$ $\square$

§2 Sylow Theorems:

Fix $p > 0$ prime & write $n = p^r m$ with $(m:p) = 1$.

Let G be a group of order n.

Definition: A subgroup $P < G$ of order p^r is called a Sylow p-subgp of G

Sylow Theorems: (A) Sylow p-subgroups exist.

(B1) If $H < G$ is a p-group, then there exists a Sylow p-subgroup $P < G$ with $H \subseteq P$.

(B2) Any two Sylow p-subgroups $P, Q < G$ are conjugate to each other (i.e. $\exists\, g \in G$ with $Q = gPg^{-1}$)

(C) Let n_p = number of Sylow p-subgroups of G. Then (i) $n_p \equiv 1 \mod (p)$
(ii) $n_p \mid m$

We will prove these theorems using group actions. An alternative proof will be discussed in HW3

§3 Proof of Sylow Thm (A):

Let $\mathcal{E} = \{ Y \subset G \text{ subset} : |Y| = p^r \}$ ⇝ p-Sylow subgroup = a stabilizer

$G \circlearrowright \mathcal{E}$ induced by left multiplication action $G \circlearrowright G$, ie:

Given $g \in G$ & $Y = \{y_1, \ldots, y_{p^r}\} \in \mathcal{E}$ ⇝ $\boxed{g \cdot Y} = \{g \cdot y_1, \ldots, g \cdot y_{p^r}\} \in \mathcal{E}$

<u>Claim</u>: There exists $X \in \mathcal{E}$ whose orbit has cardinality <u>not</u> divisible by p.

Pf/ By the Counting Lemma 1: $|\mathcal{E}| = \sum_{\alpha \in G \backslash \mathcal{E}} |G \cdot x_\alpha|$

By Lemma (page 1): $|\mathcal{E}| = \binom{p^r m}{p^r} \equiv m \pmod p$

But $m \not\equiv 0 \mod (p)$ so $p \nmid |G \cdot x_\alpha|$ for some α. □

• Pick X from the Claim & let $H_X := \mathrm{Stab}_G(X) < G$

Then $|G \cdot X| = \dfrac{|G|}{|H_X|} \not\equiv 0 \mod (p)$. Thus, $p^r \mid |H_X|$.
(by Claim)

• To finish, choose $x_0 \in X$ and define $\varphi: H_X \longrightarrow X$ (set map)

$g \longmapsto g \cdot x_0$ (by definition of stabilizer)

The map φ is <u>injective</u> since $g x_0 = h x_0$ in $G \Rightarrow g = h$.

$\Rightarrow |H_X| \leq |X| = p^r$

Thus $|H_X| = p^r$ and hence H_X is a Sylow p-subgroup of G □

§4 Proof of Sylow Theorem (B):

(B1) Let $H < G$ be a p-subgroup of G, so $|H| = p^k$ with $k \leq r$.

Let Q be a Sylow p-subgroup of G (which exists by Thm (A))

We consider the action of H on the set $X := G/Q$: $h \cdot gQ = (hg)Q$.

By Lemma (page 1): $|X^H| \equiv |X| \pmod p$. As $|X| = m \not\equiv 0 \pmod p$

then $X^H \neq \emptyset$, so $\exists\, gQ \in X^H$, that is $hgQ = gQ \quad \forall h \in H$

We conclude $g^{-1}hg \in Q \quad \forall h \in H$ so $\boxed{H \subseteq gQg^{-1}}$

- Take $\boxed{P = gQg^{-1}.}$ Since $|gQg^{-1}| = |Q| = p^r$, then P is a Sylow p-subgroup of G & $H \subseteq P$.

(B2) To prove B2 we take $H = P$ and Q any p-Sylow subgroup
By (B1) we can find $g \in G$ with $P \subseteq gQg^{-1}$
But since $|P| = p^r = |gQg^{-1}|$, then $P = gQg^{-1}$ so Q & P are conjugate to each other. $\square$

<u>Obs:</u> The proof of Sylow Thm (A) is not constructive (in practice), but the proof of Sylow Thm (B1) yields a potential algorithm. Start with an x of order p^k for some $k > 0$ & set $H = \langle x \rangle$. Then, try to add elements to it (again, of order a power of p) to extend H to a Sylow p-subgroup of G.

<u>§5. Proof of Sylow Thm (C):</u>

Let $\mathcal{S}$ be the set of all Sylow p-subgroups of G.
By Thm (A), $\mathcal{S} \neq \emptyset$. By definition, $|\mathcal{S}| = n_p$.

By Thm (B), we know that $G \circlearrowright \mathcal{S}$ by conjugation is transitive
$(x \cdot Q = xQx^{-1})$.

Consider $P \in \mathcal{S}$ & restrict the action to $P \circlearrowright \mathcal{S}$.

<u>Claim:</u> $\mathcal{S}^P = \{P\}$

By Lemma (page 1): $|\mathcal{S}^P| \equiv |\mathcal{S}| \pmod p$. Thus, Claim yields

$$\boxed{n_p = |\mathcal{S}| \equiv |\mathcal{S}^P| = 1 \mod p.}$$

__Proof of Claim__: By construction $P \in \mathcal{S}^P$, so $\mathcal{S}^P \neq \emptyset$. Fix $Q \in \mathcal{S}^P$; ie Q is a Sylow p-subgroup of G with $xQx^{-1} = Q \quad \forall x \in P$.

Define $\boxed{N_Q} = \{g \in G : gQg^{-1} = Q\} < G$ (normalizer of Q in G)

$= \mathrm{Stab}_G(Q)$ under action by conjugation

Then $Q, P \subset N_Q$ & $|N_Q| \,\big|\, |G| = p^r m$ so P & Q are two Sylow p-subgroups of N_Q.

By (B2) P & Q are conjugate in N_Q so $\exists\, x \in N_Q$ with $xQx^{-1} = P$. But $xQx^{-1} = Q$ since $x \in N_Q$.

We conclude $\boxed{P = Q}$ $\square$

- It remains to show that $n_p \mid m$. To do so, we consider $G \curvearrowright \mathcal{S}$ by conjugation (This action is transitive by (B2)). Choose $P \in \mathcal{S}$ & use Counting Lemma 1:

$$n_p = |\mathcal{S}| = |G \cdot P| = \frac{|G|}{|\mathrm{Stab}_G(P)|} = \frac{|G|}{|N_P|}$$

Since $P < N_P < G \Rightarrow |N_P| = p^r m'$ for some $m' \mid m$.

Then $n_p = \dfrac{m}{m'}$ & so $\boxed{n_p \mid m}$. $\square$