Lecture XIV: p-groups and Sylow Theorems

§14.1 Counting Fix point sets:

Recall (Proposition 2 §11.2) For $p \in \mathbb{Z}_{\geq 2}$ prime and $r, m \in \mathbb{Z}_{\geq 0}$, we have:

$$\binom{p^r m}{p^r} \equiv m \pmod p$$

The following crucial idea was used in the proof:

Lemma: If $G \circlearrowright X$ and $|G| = p^r$ (a power of a prime), then $|X| \equiv |X^G| \bmod p$

Here, $X^G := \{x \in X : g \cdot x = x \ \forall g \in G\}$ $\left(= \bigcap_{g \in G} X^g\right)$

Proof: As X breaks into a disjoint union of G-orbits:

$$|X| = \sum_{\substack{\mathcal{O}:\text{orbit} \\ \text{under } G\text{-action}}} |\mathcal{O}|$$

For each orbit $\mathcal{O}$, $|\mathcal{O}|$ divides $|G| = p^r$. since $|G| = |G \cdot x| \, |\mathrm{Stab}_G(x)| \ \forall x \in X$.

Thus, $|\mathcal{O}| = 1$ or $|\mathcal{O}| \equiv 0 \pmod p$.

Hence, we get $|X| \equiv \#\text{ orbits of size } 1 \pmod p$

Orbits of size 1 $= \{x \in X \mid g \cdot x = x \ \forall g \in G\} = X^G$

Conclusion: $|X| \equiv |X^G| \pmod p$ $\square$

§14.2 Application: p-groups

Definition: Fix p prime. A finite group G is called a <u>p-group</u> if $|G| = p^r$ for some $r \geq 1$.

Theorem: If $|G| = p^r$ is a p-group, then $|Z(G)| = p^s$ for some $1 \leq s \leq r$.

Proof: We let G act on itself by conjugation.

By the Lemma, $\underset{\substack{\parallel \\ \{x \in G \,:\, gxg^{-1} = x \ \forall g\} \,=\, Z(G)}}{\#\text{ fixed points}} \equiv |G| = 0 \pmod p$, so $p \mid |Z(G)|$

Since $|Z(G)| \mid |G| = p^r$, we conclude $|Z(G)| = p^s$ for $1 \leq s \leq r$. $\square$

Note: $Z(G) \trianglelefteq G$ is a normal abelian subgroup of G.

So it seems we have some "inductive" statement for every p-group.

G p-group of size p^r
$\trianglerighteq$
$Z(G)$ abelian, normal p-subgroup of size p^s $(1 \leq s \leq r)$

$\rightsquigarrow$ $\overline{G} = G/Z(G) =: G_1$ is either trivial or a strictly smaller p-group of size p^{r-s} $(1 \leq s \leq r)$

Proposition: Let G be a p-group. Then, there exists a chain of normal subgroups

$$\{e\} \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \cdots \trianglelefteq Z_s = G$$

such that each quotient Z_{i+1}/Z_i $(1 \leq i \leq s-1)$ is an abelian p-group

Proof: By induction on r if $|G| = p^r$

Base case: $p = 1 \Rightarrow G \simeq \mathbb{Z}/p\mathbb{Z}$ ($Z(G) = G$ by Theorem and is cyclic by Application § 5.2) Take $s = 1$ in the statement.

Inductive Step: Consider $Z_1 = Z(G)$.

- If G is abelian, then $s = 1$ works.
- Otherwise, $G_1 = G/Z(G)$ is a p-group.

By inductive hypotheses, $\exists$ $\overline{Z}_1 = \{\bar{e}\} \trianglelefteq \overline{Z}_2 \trianglelefteq \overline{Z}_3 \trianglelefteq \cdots \trianglelefteq \overline{Z}_s = G_1$ where each quotient $\overline{Z_{i+1}}/\overline{Z_i}$ is an abelian p-group.

Fix $\pi: G \longrightarrow G/Z(G) = G_1$. Then, by the 2^{nd} isomorphism Theorem,

$Z_i := \pi^{-1}(\overline{Z}_i)$ with $i = 1, \ldots, s$ satisfies $Z_i \leq G$ and $Z_i \leq Z_{i+1}$ $\forall i$

Claim: For $i = 1, \ldots, s-1$ $\overline{Z_i} \trianglelefteq \overline{Z_{i+1}} \Rightarrow Z_i \trianglelefteq Z_{i+1}$

Pf/ $g \in Z_{i+1}$ $x \in Z_i$ $\Rightarrow$ $(g x g^{-1}) Z_1 = \underset{\overline{Z_{i+1}}}{\underset{\cap}{gZ_1}} \; \underset{\overline{Z_i}}{\underset{\cap}{xZ_1}} (gZ_1)^{-1} \in \overline{Z_i}$

$\Rightarrow g x g^{-1} \in Z_i$ so $Z_i \trianglelefteq Z_{i+1}$.
$\downarrow$
$Z_1 \subseteq Z_{i+1}$

- By restricting π to Z_{i+1}, using the 3^{rd} Isomorphism Theorem, we conclude that $Z_{i+1}/Z_i \simeq \overline{Z_{i+1}}/\overline{Z_i}$, so we conclude the quotients are abelian p-groups. $\square$

§ 14.3 Sylow Theorems:

The next results are a first approximation towards a classification theorem of finite groups, by understand G through its p-subgroups for each prime p with $p \mid |G|$.

Fix $|G| = n$ and p a prime number with $p \mid n$. Write $n = p^r m$ with $\gcd(p,m)=1$, $r \geq 1$.

Definition: A Sylow p-subgroup of G is any subgroup $H \leq G$ with $p \mid |G|$ & $p \nmid [G:H]$ (equivalently, $|H| = p^r$ if p^r is the maximal power of p dividing $|G|$)

Notation: $\mathrm{Syl}_p(G) :=$ set of Sylow p-subgroups of G

Theorem (Sylow): Let G be a finite group and p prime with $p \mid |G|$. Write $|G| = p^r m$ with $p \nmid m$.

(1) There exists a subgroup $P \leq G$ such that $|P| = p^r$ (p-Sylow subgroups exist)

(2) Let P_1, P_2 be two Sylow p-subgroups of G. Then, there exists $g \in G$ such that $P_2 = g P_1 g^{-1}$ ($G \circlearrowright \mathrm{Syl}_p(G)$ by conjugation is transitive)

(3) Let $n_p = \#\{\text{Sylow } p\text{-subgroups of } G\}$. Then
- $n_p \equiv 1 \mod (p)$
- $n_p \mid m$ $\quad (n = p^r m \quad p \nmid m)$

We prove each part separately:

Proof of (1): We let $X :=$ set of all p^r-element subsets of G & let $G \circlearrowright X$ via $g \cdot \{\sigma_1, \ldots, \sigma_{p^r}\} = \{g\cdot\sigma_1, \ldots, g\cdot\sigma_{p^r}\}$ with $G \circlearrowright G$ by left multiplication

Observation 1: If $H = \{h_1, \ldots, h_{p^r}\} \in X$, then $\mathrm{Stab}_G(H) = \{g : g\cdot H = H\}$

In particular, $g h_1 = h_i$ for some $1 \leq i \leq p^r$, meaning $g = h_i h_1^{-1}$ for some $1 \leq i \leq p^r$

$\Rightarrow \mathrm{Stab}_G(H) \subseteq \{e, h_2 h_1^{-1}, \ldots, h_{p^r} h_1^{-1}\}$, hence

$$\boxed{|\mathrm{Stab}_G(H)| \leq p^r \quad \forall H \in X}$$

Note: if $=$ holds, then $\mathrm{Stab}_G(H)$ is a p-Sylow subgroup of G.

Observation 2: $|X| = \binom{p^r m}{p^r} \equiv m \pmod p \not\equiv 0 \mod (p)$.

As $|X| =$ sum of orbit sizes, there must be some orbit, say $\mathcal{O} \in {}_G\backslash X$, such that $|\mathcal{O}| \not\equiv 0 \mod (p)$.

Pick $H \in \mathcal{O}$. Then, $|\mathrm{Stab}_G(H)| = \dfrac{|G|}{|\mathcal{O}|} = \dfrac{p^r m}{|\mathcal{O}|}$ & $p \nmid |\mathcal{O}|$ forces

$$\boxed{|\mathrm{Stab}_G(H)| = p^r m' \quad \text{with} \quad m' = \frac{m}{|\mathcal{O}|}}$$

Combining Observations 1 and 2, we get $m' = 1$ & $|\mathrm{Stab}_G(M)| = p^r$, as we wanted

Next Time: Proof of (2) and (3)