Lecture 26: Cauchy's theorem and $p$-groups.

Recall. $G \triangleleft X \Rightarrow \forall x_0 \in X, \ G/G_{x_0} \rightarrow O(x_0)$

$$g_{G_{x_0}} \rightarrow g \cdot x_0$$

is a (well-defined) bijection.

$$\Rightarrow |O(x_0)| = [G : G_{x_0}] .$$

$$\Rightarrow |X| = \sum_{O(x) \in G_X} |O(x)| = |X^G| + \sum_{O(x) \in G_X} [G : G_{x}]$$

where $X^G := \{ x \in X | \forall g \in G, g \cdot x = x \}$

**Thm.** If $|P| = p^n$ and $P \triangleleft X$, then

$$|X| \equiv |X^P| \pmod{p} .$$

**Pr.** $x \notin X \Rightarrow P \neq P_x$

$$\Rightarrow [P : P_x] \neq 1 \text{ or } [P : P_x] | |P| = p^n$$

$$\Rightarrow [P : P_x] = p^k \text{ where } 1 \leq k \leq n$$

$$\Rightarrow p | [P : P_x] .$$

$$|X| = |X^P| + \sum_{x \in X^G} [P : P_x] \equiv |X^P| .$$

**Thm.** Let $P$ be a group. Suppose $|P| = p^n \neq 1$. 
\[
\Rightarrow Z(P) \neq 1 \text{ for some } g \in G.
\]

**Proof.** Let \( P \triangleleft G \) by conjugation, i.e. \( g.g' = g g' g^{-1} = g g g^{-1} = 1 \).

The set of fixed points of this action

\[
\{ g' \in P \mid \forall g \in P, \ g.g' = g'g' = g g' = 1 \}
\]

\[
= \{ g' \in P \mid \forall g \in P, \ g.g' = g g' = Z(P) \}
\]

By the previous theorem, \( |P| \equiv |Z(P)| \mod p \)

\[
\Rightarrow p \mid |Z(P)| \Rightarrow p \leq |Z(P)| \Rightarrow Z(P) \neq 1 \quad \forall e \in Z(P)
\]

**Cauchy's theorem.** Suppose \( G \) is a finite group and \( p \mid |G| \)

where \( p \) is prime. Then \( \exists g \in G, \ o(g) = p \).

**Cor.** Suppose \( G \) is a finite group and it is a \( p \)-group, i.e. \( \forall g \in G, \ o(g) = p^m \) for some \( m \in Z^\mathbb{Z} \).

Then

\[
|G| = p^n \quad \text{for some } n \in Z^\mathbb{Z}.
\]

**Proof.** If \( |G| \) is not a power of \( p \), \( \exists \) a prime \( p' \neq p \) that divides \( |G| \). So by Cauchy's theorem, \( \exists g \in G, \ o(g) = p' \), which
contradicts our assumption that \( G \) is a \( p \)-group.

\[\text{Proof of Cauchy’s theorem}\]

Let \( X = \{ (g_1, g_2, \ldots, g_p) \in G \times \cdots \times G \mid g_1 \cdot g_2 \cdots g_p = e^G \} \).

So \( G \times \cdots \times G \overset{\text{p-1 times}}{\rightarrow} X, (g_1, \ldots, g_{p-1}) \mapsto (g_1, \ldots, g_{p-1}, g_1^{-1} \cdots g_{p-1}^{-1}) \)

is a bijection. In particular, \( |X| = |G|^{p-1} \). Since \( p \mid |G| \),

\( p \mid |X| \).

Let \( \mathbb{Z}_p \cap X, [i] \cdot (g_1, \ldots, g_p) = (g_{i+1}, \ldots, g_p, g_1, \ldots, g_i) \).

Well-defined. \( g_1 \cdots g_p = e \Rightarrow (g_1 \cdots g_i) = (g_{i+1} \cdots g_p)^{-1} \)

\[\Rightarrow (g_{i+1} \cdots g_p)(g_1 \cdots g_i) = e.\]

It is clear that it satisfies the properties of an action.

So by the above theorem \( |X| \equiv |\text{The set of fixed pts}| \)

\[\Rightarrow p \mid |\text{The set of fixed pts}| = \]

\[
\left| \{(g, \ldots, g) \mid g \cdots g = e^G \} \right| = \left| \{ g \in G \mid g^p = e_G \} \right| \]

\( p \)-times

Since \( e^p = e \), this set has at least one element. Thus
it has at least \( p \) elements. Any \( g \neq e \) in this set has order \( p \). 

\[ \]