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

Sunday, December 07, 2014
9:20 PM

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

$$gG_{x_0} \longmapsto g\cdot x_0$$

is a (well-defined) bijection.

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

$\Rightarrow |X| = \sum_{O(x) \in {}_G\backslash X} |O(x)| = |X^G| + \sum_{\substack{O(x) \in {}_G\backslash X \\ x \notin X^G}} [G : G_x]$

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

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

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

Pf. $x \notin X^P \Rightarrow P \neq P_x$

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

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

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

$$|X| = |X^P| + \sum_{\substack{x \notin X^G \\ O(x) \in {}_G\backslash X}} [P : P_x] \overset{p}{\equiv} |X^P|. \quad \blacksquare$$

Thm. Let P be a group. Suppose $|P| = p^n \neq 1$.

$\Rightarrow Z(P) \neq \{e\}$.

Pf. Let $P \curvearrowright P$ by conjugation, i.e. $g \cdot g' := g g' g^{-1}$.

$\Rightarrow$ The set of fixed points of this action

$$\begin{aligned} &\{g' \in P \mid \forall g \in P,\ g \cdot g' = g'\} = \{g' \in P \mid \forall g \in P,\ g g' g^{-1} = g'\} \\ &= \{g' \in P \mid \forall g \in P,\ g g' = g' g\} = Z(P) \end{aligned}$$

By the previous theorem $|P| \equiv |Z(P)| \pmod{p}$

$$\Rightarrow \left.\begin{array}{l} p \mid |Z(P)| \\ e \in Z(P) \end{array}\right\} \Rightarrow p \leq |Z(P)| \Rightarrow Z(P) \neq \{e\}.$$

■

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 $m \in \mathbb{Z}^{\geq 0}$. Then

$$|G| = p^n \quad \text{for some } n \in \mathbb{Z}^{\geq 0}.$$

Pf. 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. ∎

Pf of Cauchy's theorem

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

So $\underbrace{G \times \cdots \times G}_{p-1 \text{ times}} \longrightarrow X$, $(g_1, \cdots, g_{p-1}) \longmapsto (g_1, \cdots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1})$

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

$p \mid |X|$.

Let $\mathbb{Z}_p \curvearrowright X$, $[i] \cdot (g_1, \cdots, g_p) := (g_{i+1}, \cdots, g_p, g_1, \cdots, g_i)$.

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

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

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

So by the above theorem $|X| \overset{p}{\equiv} |\text{The set of fixed pts}|$

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

$$|\{(g, \cdots, g) \mid \underbrace{g \cdot \cdots \cdot g}_{p\text{-times}} = e\}| = |\{g \in G \mid g^p = e\}|$$

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. ∎