Lecture 06: p-groups

Thursday, October 5, 2017 10:47 PM

<u>Def.</u> Let p be a prime. A finite group G is called a p-group if $|G| = p^n$ for some $n \in \mathbb{Z}^{\geq 0}$.

<u>Theorem.</u> Let G be a finite p-group. Suppose X is a finite set, and $G \curvearrowright X$. Then $|X| \equiv |X^G| \pmod{p}$.

<u>Pf.</u> $$|X| = |X^G| + \sum_{\substack{G\cdot x \in {}_G\backslash X \\ |G\cdot x| > 1}} |G|/|G_x|. \quad \circledast$$

Notice that, for any $x \in X$, $|G\cdot x| = |G|/|G_x|$ and $|G| = p^n$.

So $|G\cdot x|$ is a power of p; in particular $p \mid |G|/|G_x|$ if $|G\cdot x| \neq 1$.

Hence by $\circledast$ we have $|X| \equiv |X^G| \pmod{p}$. $\blacksquare$

<u>Theorem</u>. Suppose G is a non-trivial p-group. Then $Z(G)$ is non-trivial.

<u>Pf.</u> $G \curvearrowright G$ by conjugation. By the previous theorem

$$|G| \overset{p}{\equiv} |G^G| \text{ where } G^G = \{g \in G \mid \forall g' \in G, g' g g'^{-1} = g\}$$
$$= Z(G).$$

So $p \mid |Z(G)|$; which implies $Z(G)$ is not trivial. $\blacksquare$

Lecture 06: p-groups

Sunday, October 8, 2017 5:11 PM

<u>Theorem.</u> Suppose G is a finite group, H is a p-subgroup, and $p \mid |G/H|$. Then $p \mid |N_G(H)/H|$.

<u>Pf.</u> Let $H \curvearrowright G/H$. Then $|G/H| \equiv (G/H)^H \pmod p$

Since H is a proper subgroup of G, $p \mid |G/H|$. So $p \mid (G/H)^H$.

$gH \in (G/H)^H \Leftrightarrow \forall h \in H,\ hgH = gH \Leftrightarrow \forall h \in H,\ h \in gHg^{-1}$

$\Leftrightarrow H \subseteq gHg^{-1} \Leftrightarrow H = gHg^{-1} \Leftrightarrow g \in N_G(H)$.

So $p \mid |N_G(H)/H|$. So $N_G(H) \neq H$. ■

<u>Corollary.</u> Suppose P is a finite p-group, and H is a proper subgroup. Then $N_P(H) \neq H$.

<u>Pf.</u> Since H is a proper subgroup and P is a p-group, $p \mid |P/H|$. So by the previous theorem we get that

$$N_P(H) \neq H.$$

<u>Theorem.</u> Suppose G is a finite group, and p is a prime factor of $|G|$. Then $\exists g \in G$, $o(g) = p$.

(Cauchy's theorem).

Lecture 06: Cauchy's theorem

Tuesday, October 10, 2017 11:16 PM

<u>Pf.</u> (Very nice and tricky proof)

Let $X := \{(g_0, g_1, \ldots, g_{p-1}) \in G \times \cdots \times G \mid g_0 \cdot g_1 \cdots g_{p-1} = e\}$

Then $|X| = |G|^{p-1}$ (the first $p-1$ components can be freely chosen, and $g_{p-1} = g_{p-2}^{-1} \cdot g_{p-3}^{-1} \cdot \cdots \cdot g_0^{-1}$)

The cyclic group $\mathbb{Z}/p\mathbb{Z} \curvearrowright X$ by shifting the indexes:

$$g_0 \cdot g_1 \cdots g_{p-1} = e \Rightarrow (g_0 \cdot g_1 \cdots g_{i-1}) \cdot (g_i \cdots g_{p-1}) = e$$

$$\Rightarrow (g_0 \cdots g_{i-1}) = (g_i \cdots g_{p-1})^{-1}$$

$$\Rightarrow g_i \cdots g_{p-1} \cdot g_0 \cdots g_{i-1} = e$$

$$\Rightarrow (g_i, g_{i+1}, \ldots, g_{p-1}, g_0, \ldots, g_{i-1}) \in X.$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a p-group,

$$|X| \equiv |X^{\mathbb{Z}/p\mathbb{Z}}| \pmod p.$$

As $p \mid |G|$ and $|X| = |G|^{p-1}$, $p \mid |X|$. Therefore $p \mid |X^{\mathbb{Z}/p\mathbb{Z}}|$.

Notice $X^{\mathbb{Z}/p\mathbb{Z}} = \{(g, \ldots, g) \mid g^p = e\}$. So $(e, \ldots, e) \in X^{\mathbb{Z}/p\mathbb{Z}}$.

Therefore $|X^{\mathbb{Z}/p\mathbb{Z}}| \geq p$; so $\exists\, g \neq e$ s.t. $g^p = e$, which means $o(g) = p$. ∎

Lecture 06: Sylow's theorems

Tuesday, October 10, 2017 11:27 PM

<u>Corollary</u>. Suppose G is a finite group, and order of any element of G is a power of p, where p is a fixed prime. Then G is a p-group.

(Sylow's 1^{st})

<u>Theorem</u>. Suppose G is a finite group, and $p^m \mid |G|$. Then

$$\exists\, P_1 \trianglelefteq P_2 \trianglelefteq \cdots \trianglelefteq P_m \le G \text{ s.t. } |P_i| = p^i \text{ for } 1 \le i \le m.$$

<u>Pf.</u> We proceed by induction on $\underline{m}$.

<u>Base of induction</u> $m=1$; this is Cauchy's theorem.

<u>Induction step.</u> Suppose $p^{k+1} \mid |G|$. By the induction hypothesis

$\exists\, P_1 \trianglelefteq \cdots \trianglelefteq P_k \le G$ s.t. $|P_i| = p^i$ for $1 \le i \le k$.

So P_k is a p-group and $p \mid |G/P_k|$. Hence, by a theorem that we have proved earlier, $p \mid |N_G(P_k)/P_k|$. So $N_G(P_k)/P_k$ is a group and p divides its order. Thus by Cauchy's theorem $N_G(P_k)/P_k$ has a subgroup of order p.

A subgroup of the quotient group $N_G(P_k)/P_k$ is of the form H/P_k where $H \le G$. So $\exists\, P_{k+1} \le G$ s.t. $P_k \triangleleft P_{k+1}$ and $|P_{k+1}/P_k| = p$; therefore $|P_{k+1}| = p^{k+1}$. ∎