Lecture 04: Group actions of p-groups

Tuesday, October 9, 2018 8:26 AM

In the previous lecture we mentioned the following theorem.

Theorem. Suppose G is a group, $|G| = p^n$ where p is prime, and $G \curvearrowright X$ and $|X| < \infty$. Then

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

Pf. We know $|X| = |X^G| + \sum_{\substack{G\cdot x \in G\backslash X \\ |G\cdot x| > 1}} [G : G_x]$. (I)

$[G:G_x] \mid |G| \Rightarrow [G:G_x]$ is a power of p.

$\Rightarrow$ if $1 < [G:G_x]$, then $p \mid [G:G_x]$. (II)

By (I), (II), we deduce $|X| \equiv |X^G| \pmod{p}$. ■

Theorem. Suppose G is a group, $|G| = p^n$ where p is prime, and $n > 0$. Suppose $1 \neq N \trianglelefteq G$. Then $N \cap Z(G) \neq 1$.

Pf. Consider $G \curvearrowright N$ by conjugation; notice

$$N^G = \{h \in N \mid \forall g \in G,\ g h g^{-1} = h\} = N \cap Z(G).$$

Deduce that $|N| \equiv |N \cap Z(G)| \pmod{p}$; therefore

$p \mid |N \cap Z(G)|$. ($|N| \mid |G| \Rightarrow |N|$ is a power of p) ■

Lecture 04: Further properties of p-groups

Tuesday, October 9, 2018 8:35 AM

Corollary. Suppose G is a group, $|G|=p^n$ where p is prime, $n>0$. Then $Z(G)\neq 1$.

Pf. $1\neq G \trianglelefteq G \Rightarrow Z(G)=Z(G)\cap G\neq 1$. ∎

Theorem. $\left.\begin{array}{l} H\leq G,\ |H|=p^m \\ p \mid |G/H| \end{array}\right\} \Rightarrow p \mid |N_G(H)/H|$.

Pf. $H \curvearrowright G/H$ by left translations.

$$\Rightarrow |G/H| \equiv |(G/H)^H| \pmod p.$$

$$(G/H)^H = \{gH \mid \forall h\in H,\ hgH=gH\}.$$
$$=\{gH \mid \forall h\in H,\ g^{-1}hg\in H\}$$
$$=\{gH \mid g^{-1}Hg\subseteq H\}$$
$$=\{gH \mid g^{-1}Hg=H\} = N_G(H)/H;$$

and claim follows. ∎

Theorem. (Cauchy) G: finite gp; p: prime; $p \mid |G|$.

$$\Rightarrow \exists g\in G,\ o(g)=p.$$

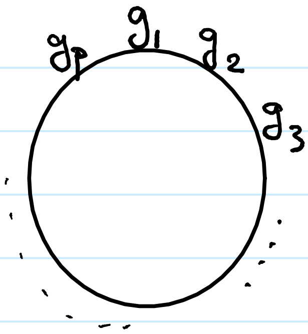
Pf. Let $X:=\{(g_1,\ldots,g_p)\in G\times\cdots\times G \mid g_1\cdots g_p=e\}$.

Notice that $g_1\cdot\cdots\cdot g_p=e$ implies $g_p\cdot g_1 g_2\cdots g_{p-1}=e$

Lecture 04: Cauchy's theorem

Tuesday, October 9, 2018 8:52 AM

and so on;



we can start from any point on this circle and the product will be e.

Hence $\mathbb{Z}/p\mathbb{Z} \curvearrowright X$ by shifting the indexes. (why?)

Therefore $|X| \equiv |X^{\mathbb{Z}/p\mathbb{Z}}| \pmod p$. We notice that

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

is a bijection; and so $|X| = |G|^{p-1}$ is divisible by p.

$\Rightarrow p \mid |X^{\mathbb{Z}/p\mathbb{Z}}| = |\{(g,\ldots,g) \mid g^p = e\}|$.

Since $(e,\ldots,e)$ is in the above set and $p \nmid 1$,

$\exists g\in G$, $g\neq e$ and $g^p=e$. Thus $o(g)=p$. ■

<u>Def.</u> G is called a p-group if $\forall g\in G$, $o(g)$ is a power of p.

<u>Proposition</u>. Suppose G is a finite p-group. Then $|G|=p^n$.

<u>Pf.</u> If not, $\exists$ a prime $\ell \mid |G|$. So by Cauchy's theorem, $\exists g\in G$, $o(g)=\ell$ which contradicts the assumption. ■

Lecture 04: 1st Sylow theorem

Tuesday, October 9, 2018 9:03 AM

<u>Theorem</u>. $\left.\begin{array}{l} G: \text{finite group} \\ p^m \mid |G| \end{array}\right\} \Rightarrow \exists\ P_1 \lhd P_2 \lhd \cdots \lhd P_m \leq G$ s.t. $|P_i| = p^i$ for $1 \leq i \leq m$.

<u>Pf</u>. We proceed by induction on i. Cauchy's theorem gives us the base case. Suppose we have already found $P_1, \ldots, P_k$. If $k=m$, we are done. If $k<m$, then

$$\left.\begin{array}{l} |P_k| \text{ is a power of } p \\ p \mid |G/P_k| \end{array}\right\} \Rightarrow p \mid |N_G(P_k)/P_k|$$

$$\left.\begin{array}{l} N_G(P_k)/P_k \text{ is a finite gp} \\ p \mid |N_G(P_k)/P_k| \end{array}\right\} \Rightarrow \text{by Cauchy's theorem, } \exists\, gP_k \in N_G(P_k)/P_k \text{ s.t. } o(gP_k) = p.$$

$\langle gP_k \rangle = P_{k+1}/P_k$ where P_{k+1} is a subgroup of G and $P_k \lhd P_{k+1}$.

Moreover $|P_{k+1}/P_k| = |\langle gP_k \rangle| = p$; and so

$|P_{k+1}| = |P_k| \cdot p = p^{k+1}$. ∎

Lecture 04: Sylow subgroups, and 2nd Sylow theorem

Tuesday, October 9, 2018 9:10 AM

<u>Def</u> G: finite p-gp; $p^n \mid |G|$, $p^{n+1} \nmid |G|$. Then a subgp P of G is called a Sylow p-subgroup if $|P| = p^n$.

we let $\mathrm{Syl}_p(G)$ be the set of all Sylow p-subgps and $s_p := |\mathrm{Syl}_p(G)|$.

<u>Theorem</u> (2^{nd} Sylow thm) G: finite group.

$$\left.\begin{array}{l} Q \le G,\ Q: p\text{-group}. \\ P_0 \in \mathrm{Syl}_p(G) \end{array}\right\} \Rightarrow \exists g \in G,\ g^{-1} Q g \subseteq P_0.$$

<u>Pf.</u> $Q \curvearrowright G/P$ by the left translations. Since Q is a p-gp, $|G/P_0| \equiv |(G/P_0)^Q| \pmod p$ $(*)$

Since $P_0 \in \mathrm{Syl}_p(G)$, $p \nmid |G/P_0|$. Therefore by $(*)$ $(G/P_0)^Q \neq \emptyset$. Suppose $gP_0 \in (G/P_0)^Q$. Then

$\forall q \in Q$, $qgP_0 = gP_0 \Rightarrow g^{-1} Q g \subseteq P_0$ ∎

<u>Corollary.</u> $G \curvearrowright \mathrm{Syl}_p(G)$ transitively via conjugation.

<u>Pf.</u> $|gPg^{-1}| = |P| \Rightarrow G$ does act on $\mathrm{Syl}_p(G)$ by conjugation. Let $P, P' \in \mathrm{Syl}_p(G)$. Then $\exists g$, $g^{-1}Pg \subseteq P'$,

Lecture 04: More Sylow subgroups

Tuesday, October 9, 2018 9:22 AM

and so $g^{-1}Pg = P'$. ■

<u>Cor.</u> If $P \in Syl_p(G)$, then $|Syl_p(G)| = [G : N_G(P)]$.

<u>Pf.</u> By the previous theorem,

$$|Syl_p(G)| = \#\text{ of conjugates of } P = [G : N_G(P)]. \quad ■$$

<u>Theorem.</u> $\forall P \in Syl_p(G)$, $Syl_p(N_G(P)) = \{P\}$.

<u>Pf.</u> . $P \subseteq N_G(P)$, and $|P|$ is a power of p (I)

$$\left.\begin{array}{l} \cdot\ |N_G(P)/P| \mid |G/P| \\ P \in Syl_p(G) \Rightarrow p \nmid |G/P| \end{array}\right\} \Rightarrow p \nmid |N_G(P)/P| \quad (\text{II})$$

. (I), (II) imply $P \in Syl_p(N_G(P))$.

. $N_G(P) \curvearrowright Syl_p(N_G(P))$ transitively

$$\Rightarrow Syl_p(N_G(P)) = \{gPg^{-1} \mid g \in N_G(P)\} = \{P\}. \quad ■$$

<u>Remark.</u> $\forall \theta \in Aut(G)$, $\theta(N_G(H)) = N_G(\theta(H))$.

$$g \in \theta(N_G(H)) \Leftrightarrow \theta^{-1}(g) \in N_G(H) \Leftrightarrow H = \theta^{-1}(g)\, H\, \theta^{-1}(g)^{-1}$$

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

Lecture 04: Normalizer of normalizer

Tuesday, October 9, 2018 2:09 PM

<u>Thm.</u> Suppose $P \in Syl_p(G)$. Then $N_G(N_G(P)) = N_G(P)$.

<u>Pf.</u> $\forall g \in G$, $Syl_p(g N_G(P) g^{-1}) = Syl_p(N_G(gPg^{-1}))$

$$= \{gPg^{-1}\}.$$

So $\forall g \in N_G(N_G(P))$,

$$Syl_p(g N_G(P) g^{-1}) = Syl_p(N_G(P))$$

$$\{gPg^{-1}\} \qquad \{P\}.$$

Hence $gPg^{-1} = P$. Therefore $N_G(N_G(P)) \subseteq N_G(P)$.

Since $N_G(P) \subseteq N_G(N_G(P))$, we deduce

$$N_G(P) = N_G(N_G(P)). \qquad \blacksquare$$

In the next lecture we will prove 3^{rd} Sylow theorem:

$$|Syl_p(G)| \equiv 1 \pmod p.$$