Lecture 05: 3rd Sylow theorem

Thursday, October 11, 2018 9:12 AM

<u>Thm (3rd Sylow theorem)</u>. $|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$.

<u>Pf.</u> Let $P_0 \in \mathrm{Syl}_p(G)$. If $P_0 = \{1\}$, then $|\mathrm{Syl}_p(G)| = 1$; and there is nothing to prove. Otherwise $|P_0| = p^k$ for some $k \in \mathbb{Z}^+$.

Consider $P_0 \curvearrowright \mathrm{Syl}_p(G)$ by conjugation. By the main theorem of group actions of finite p-groups,

$$|\mathrm{Syl}_p(G)| \equiv |\mathrm{Syl}_p(G)^{P_0}| \pmod p. \quad (*)$$

$$\begin{aligned} P \in \mathrm{Syl}_p(G)^{P_0} &\Leftrightarrow P_0 \subseteq N_G(P) \\ &\Leftrightarrow P_0 \in \mathrm{Syl}_p(N_G(P)) = \{P\} \\ &\Leftrightarrow P_0 = P. \end{aligned}$$

Hence $|\mathrm{Syl}_p(G)^{P_0}| = 1$; and by $(*)$ claim follows. ■

Sylow theorems are extremely useful to describe possible gp structures of a group with a given order.

<u>Problem</u>. Describe possible group structures of a group of order pq where $p<q$ are primes.

<u>Solution</u>. Let $s_q := |\mathrm{Syl}_q(G)|$. Then by the 1st and 2nd Sylow

Lecture 05: Groups of order pq

Thursday, October 11, 2018 9:24 AM

$s_q = [G : N_G(Q)]$ where $Q \in Syl_q(G)$. And so

$s_q \mid [G:Q] = p$. $\Rightarrow s_q = 1$ or p $\Big\}\Rightarrow s_q = 1 \Rightarrow Q \triangleleft G$.

$s_q \equiv 1 \pmod q$ (by 3rd Sylow thm)

$p < q$

Notice $[G:Q]=p$ is the smallest prime factor of $|G|$. Hence by a result we proved earlier $Q \triangleleft G$.

- $|P| = p$, $|Q| = q$ are prime $\Rightarrow P$ and Q are cyclic.
- $|P \cap Q| \mid \gcd(|P|, |Q|) = 1 \Rightarrow P \cap Q = \{e\}$.

<u>Lemma</u>. $H, K \leq G$. Then $HK \curvearrowleft K$, and the following is a bijection $H/_{H\cap K} \xrightarrow{\Phi} HK/_K$, $h(H\cap K) \mapsto hK$; moreover when H and K are finite, $|HK| = \dfrac{|H|\,|K|}{|H\cap K|}$.

(Think about $HK/_K$ as the set of K-orbits of the action $HK \curvearrowleft K$.)

<u>Pf.</u> $G \curvearrowleft K$ and $HK \cdot K = HK$ is K-invariant $\Rightarrow HK \curvearrowleft K$.

- $\Phi(h_1(H\cap K)) = \Phi(h_2(H\cap K)) \Rightarrow h_1 K = h_2 K \Rightarrow h_2^{-1} h_1 \in K$

$\Rightarrow h_2^{-1} h_1 \in H \cap K \Rightarrow h_1(H\cap K) = h_2(H\cap K)$

- $\forall h \in H$, $k \in K$, $hk K = hK = \Phi(h(H\cap K)) \Rightarrow \Phi$ is onto.

Lecture 05: Groups of order pq

Thursday, October 11, 2018 1:59 PM

By Lemma that is not Burnside's,

$$|HK/K| = \frac{1}{|K|} \sum_{k\in K} |HK^k|.$$

For $k\in K\setminus\{e\}$, $(HK)^k=\emptyset$ (left trans. action); and

$(HK)^e = HK$. Therefore $|HK/K| = \dfrac{|HK|}{|K|}$.

(One does not need the above lemma; since the action is free, any K orbit has $|K|$-many elements; and K-orbits form a partition; hence $|HK| = |HK/K|\,|K|$.)

Therefore $\dfrac{|H|}{|H\cap K|} = |H/H\cap K| = |HK/K| = \dfrac{|HK|}{|K|}$. ■

By the above lemma, $|PQ| = \dfrac{|P||Q|}{|P\cap Q|} = pq$; and so

$PQ=G$. Suppose $P=\{e, g, \dots, g^{p-1}\}$ and $Q=\{e, h, \dots, h^{q-1}\}$.

Then $G=\{g^i h^j \mid 0\le i<p,\ 0\le j<q\}$.

Since $Q \trianglelefteq G$, $\exists\, 0\le k<q$, $ghg^{-1}=h^k$. As

$o(h) = o(ghg^{-1}) = o(h^k) = \dfrac{o(h)}{\gcd(o(h),k)}$, $\gcd(\underbrace{o(h)}_{q},k)=1$.

Notice that $g^2hg^{-2} = gh^kg^{-1} = (ghg^{-1})^k = (h^k)^k = h^{k^2}$.

Inductively $g^m h g^{-m} = h^{k^m}$; in particular, $h = g^p h g^{-p} = h^{k^p}$.

Lecture 05: Groups of order pq

Thursday, October 11, 2018   2:12 PM

Hence $k^p \equiv 1 \pmod{o(h)} \Rightarrow k^p \equiv 1 \pmod{q}$. Therefore

$\underbrace{\mathrm{ord}_q}\, k \mid p \Rightarrow \mathrm{ord}_q k = 1$ or p.

$\hookrightarrow$ the multiplicative order of k modulo q;

alternatively, this is the order of k in $(\mathbb{Z}/q\mathbb{Z})^\times$ where

$(\mathbb{Z}/q\mathbb{Z})^\times = \{a+q\mathbb{Z} \mid a+q\mathbb{Z}$ has a multiplicative inverse in $\mathbb{Z}/q\mathbb{Z}\}$.

[Recall, $(\mathbb{Z}/q\mathbb{Z})^\times = \{a+q\mathbb{Z} \mid 0<a<q,\ \gcd(a,q)=1\}$.]

So if $\underbrace{p \nmid q-1}$, then $\mathrm{ord}_q k = 1$; hence $k=1$ and $ghg^{-1} = h$. Hence $gh=hg$. This implies

$$o(gh) = \mathrm{l.c.m}(o(g), o(h)) = pq = |G|.$$

Thus G is cyclic.

<u>Summary</u>. $|G| = pq$, $p<q$, $p \nmid q-1 \Rightarrow G$ is cyclic.

Later you will prove:

<u>Thm</u>. $\gcd(n, \phi(n)) = 1 \Leftrightarrow$ any group of order n is cyclic.

Lecture 05: Groups of order p(p-1) and p(p+1)

Thursday, October 11, 2018 2:21 PM

Problem. Suppose G is a group of order $p(p-1)$. Prove that G has a normal subgroup of order p.

Pf. Let $s_p := |Syl_p(G)|$ and $P \in Syl_p(G)$. Then

$$\left.\begin{array}{l} s_p = [G:N_G(P)] \mid [G:P] = p-1 \\ s_p \equiv 1 \pmod p \end{array}\right\} \Rightarrow s_p = 1. \Rightarrow Syl_p(G) = \{P\}.$$

$$\forall g \in G,\ gPg^{-1} \in Syl_p(G) \Rightarrow gPg^{-1} = P \Rightarrow P \triangleleft G. \quad \blacksquare$$

Problem. Suppose G is a group of order $p(p+1)$. Prove that G has a normal subgroup of order either p or $p+1$.

Solution. Let $s_p := |Syl_p(G)|$, and $P \in Syl_p(G)$. Then

$$\left.\begin{array}{l} s_p = [G:N_G(P)] \mid [G:P] = p+1 \\ s_p \equiv 1 \pmod p \end{array}\right\} \Rightarrow s_p = 1 \text{ or } p+1.$$

- If $s_p = 1$, then $Syl_p(G) = \{P\}$; and so $P \triangleleft G$.
- Suppose $s_p = p+1$ and $Syl_p(G) = \{P_1, \ldots, P_{p+1}\}$.

Then P_i's are cyclic groups of order p. Hence $\forall g \in P_i \setminus \{e\}$, $o(g) = p$. Hence $i \neq j$, $P_i \cap P_j = \{e\}$. Therefore

Lecture 05: Groups of order p(p+1)

Thursday, October 11, 2018 3:16 PM

$$\left|\bigcup_{i=1}^{p+1}(P_i\setminus\{e\})\right| = (p+1)(p-1) = p^2-1; \text{ and so}$$

$$|H| = p+1 \text{ where } H := G\setminus\left(\bigcup_{i=1}^{p+1} P_i\setminus\{e\}\right).$$

<u>Claim 1.</u> $H = \{g\in G \mid o(g)\neq p\}$.

<u>Pf of Claim 1.</u> . $g\in G\setminus H \Rightarrow \exists i,\ g\in P_i\setminus\{e\} \Rightarrow o(g)=p$

. $o(g)=p \Rightarrow \langle g\rangle \in \mathrm{Syl}_p(G) \Rightarrow \exists i,\ \langle g\rangle = P_i \Rightarrow g\in P_i$.

<u>Cor. of Claim 1.</u> $\forall g\in G,\ gHg^{-1}=H$ as $o(ghg^{-1})=o(h)$ for any h.

[So it is enough to show H is a subgroup. Here is the plan; suppose $h\in H\setminus\{e\}$, we will show $C_G(h)=H$. This will be done by showing $|C_G(h)|=p+1$; this in turn will be handled by showing $|Cl(h)|=p$.]

<u>Claim 2.</u> Suppose $P_1=\{e,g,g^2,\ldots,g^{p-1}\}$. Then for $0\leq i<j<p$ $g^ihg^{-i}\neq g^jhg^{-j}$, for $h\in H\setminus\{e\}$.

<u>Pf of Claim 2.</u> If not, $g^ihg^{-i}=g^jhg^{-j}$. Then $g^{i-j}h=hg^{i-j}$; and so $h\in C_G(\langle g^{i-j}\rangle)=C_G(\langle g\rangle)=C_G(P_1)\subseteq N_G(P_1)$.

Lecture 05: Groups of order p(p+1)

Thursday, October 11, 2018 3:31 PM

$s_p = [G : N_G(P_1)] \Rightarrow |N_G(P_1)| = p = |P_1| \Rightarrow N_G(P_1) = P_1$.

And so $h \in P_1$ which contradicts $h \in H \setminus \{e\}$.

<u>Claim 3.</u> $H \setminus \{e\} = \{h, ghg^{-1}, \ldots, g^{p-1} h g^{-(p-1)}\} = Cl(h)$

<u>Pf of Claim 3.</u> $H \setminus \{e\}$ is closed under conjugation. So

$h \in H \setminus \{e\}$ implies $Cl(h) \subseteq H \setminus \{e\}$. (I)

$\Rightarrow \{h, ghg^{-1}, \ldots, g^{(p-1)} h g^{-(p-1)}\} \subseteq Cl(h) \subseteq H \setminus \{e\}$.

By claim 2, $|\{h, ghg^{-1}, \ldots, g^{(p-1)} h g^{-(p-1)}\}| = p = |H \setminus \{e\}|$

$H \setminus \{e\} = \{h, ghg^{-1}, \ldots, g^{(p-1)} h g^{-(p-1)}\}$. (II)

Hence $H \setminus \{e\} \subseteq Cl(h)$. (III)

By (I), (III), $Cl(h) = H \setminus \{e\}$; and claim follows.

<u>Finishing proof.</u> By Claim 3, $|Cl(h)| = p$. Hence

$[G : C_G(h)] = p$, which implies $|C_G(h)| = p+1$. Therefore

$\forall\, h' \in C_G(h)$, $o(h') \neq p$; and so $C_G(h) \subseteq H$. As

$|C_G(h)| = p+1 = |H|$, we conclude $H = C_G(h)$ is a subgp.

Hence it is a normal subgp of order $p+1$. ∎

Lecture 05: Groups of order p(p+1)

Thursday, October 11, 2018 3:41 PM

<u>Remark</u>. As part of your HW, you will prove that if a group G of order $p(p+1)$ does not have a normal subgp of order p, then $p = 2^n - 1$ is a Mersenne prime. In fact, in this case $G \simeq \mathbb{F}_{2^n}^{\times} \ltimes \mathbb{F}_{2^n}$ where $\mathbb{F}_{2^n}$ is a finite field of order 2^n. (We will learn about finite fields in math 200b.)