Lecture 08: Groups of order pq

Friday, October 13, 2017 12:45 AM

In the previous lecture we showed, if $|G|=pq$ where $p<q$ are primes, then there is only one Sylow q-subgroup Q_0. And so $Q_0 \triangleleft G$.

Now let P_0 be a Sylow p-subgroup. Then $P_0 \cap Q_0 = \{1\}$ as $\gcd(|P_0|,|Q_0|)=1$, and $|P_0 \cap Q_0| \mid |P_0|$ and $|P_0 \cap Q_0| \mid |Q_0|$. Thus $|P_0 Q_0| = |P_0||Q_0| = |G|$; therefore $G = P_0 Q_0$.

Suppose $P_0 = \{e, g_0, \ldots, g_0^{p-1}\}$ and $Q_0 = \{e, h_0, \ldots, h_0^{q-1}\}$. Then $G = \{g_0^i h_0^j \mid 0 \le i < p,\ 0 \le j < q\}$. Moreover, since $Q_0 \triangleleft G$, $g_0 h_0 g_0^{-1} = h_0^{k_0}$. Comparing the order of both sides, we get that $q = q/\gcd(k_0,q)$ (why?); and so $\gcd(k_0,q)=1$. Moreover, since $P_0 \to \mathrm{Aut}(Q_0)$, $g_0 \mapsto$ conjugation by g_0 is a group homomorphism, we get that $h_0 \overset{\varphi}{\longmapsto} h_0^{k_0}$ is an automorphism of Q_0, and $\varphi^p = I_{Q_0}$.

Hence $h_0^{k_0^p} = h_0$; which happens exactly when $k_0^p \equiv 1 \pmod q$. $\circledast$

Having a $\underline{k_0}$ which satisfies $\circledast$ uniquely determines the group structure of G. In particular, if $\underline{p \nmid q-1}$, then $k_0 \equiv 1 \pmod q$: $\mathrm{ord}_q k_0 \mid p$ and $q-1 \Rightarrow \mathrm{ord}_q k_0 = 1$. And so $g_0 h_0 = h_0 g_0$; and $\mathrm{ord}(g_0 h_0) = pq$; which implies $G \simeq \mathbb{Z}/pq\mathbb{Z}$.

Lecture 08: Groups of order p(p-1) and p(p+1)

Thursday, October 12, 2017 10:00 PM

<u>Problem</u>. Suppose p is prime, and G is a finite group of order $p(p-1)$. Prove that G has a normal subgroup of order p.

<u>Pf</u>. Let $n_p := |\mathrm{Syl}_p(G)|$. By Sylow's theorems, we have

$n_p \mid p-1$ and $n_p \equiv 1 \pmod{p}$. If $n_p \neq 1$, then

$p \mid n_p - 1$ implies that $p \leq n_p - 1$; and so $p+1 \leq n_p$ $\circledast$

On the other hand, $n_p \mid p-1$ implies $n_p \leq p-1$; which contradicts $\circledast$ ∎

<u>Problem</u>. Suppose p is prime, and G is a finite group of order $p(p+1)$. Prove that G has a normal subgroup of order either p or $p+1$.

<u>Pf</u>. Let $n_p = |\mathrm{Syl}_p(G)|$. If $n_p = 1$, then by Sylow's 2^{nd} theorem G has a normal subgroup of order p. So without loss of generality we can and will assume that $n_p \neq 1$. As $n_p = [G : N_G(P_0)]$ (where P_0 is a Sylow p-subgroup), we have $n_p \mid p+1$. By Sylow's 3^{rd} theorem, $n_p \equiv 1 \pmod{p}$. As $p \mid n_p - 1$ and $n_p > 1$, we get that $n_p \geq p+1$. Since $n_p \mid p+1$ and $n_p \geq p+1$, we

Lecture 08: Groups of order p(p+1)

Thursday, October 12, 2017 10:34 PM

that $n_p = p+1$. Suppose $\mathrm{Syl}_p(G) = \{P_0, P_1, \ldots, P_p\}$. Since P_i's have prime order, for $i \neq j$ we have $P_i \cap P_j = \{e\}$. Hence

$$\left|\bigcup_{i=0}^{p} P_i\right| = |\{e\} \sqcup \bigsqcup_{i=0}^{p} (P_i \setminus \{e\})| = 1 + (p+1)(p-1) = p^2.$$

So # of elements of order p in $G = p^2-1$; and so

$$G = \underbrace{\{g \in G \mid o(g) = p\}}_{\left(\bigcup_{i=0}^{p} P_i \setminus \{e\}\right)} \sqcup H \quad \text{where } |H| = p(p+1) - (p^2-1) = p+1.$$

Notice that $h \in H \Leftrightarrow o(h) \neq p$. And so, $\forall g \in G$, $gHg^{-1} = H$.

So it is enough to show H is a subgroup.

Let $h \in H \setminus \{e\}$; and suppose $o(g_0) = p$. Then

$$\{e, h, g_0 h g_0^{-1}, \ldots, g_0^{p-1} h g_0^{-(p-1)}\} \subseteq H.$$

<u>Claim</u>. $H = \{e, h, g_0 h g_0^{-1}, \ldots, g_0^{p-1} h g_0^{-(p-1)}\}$.

<u>Pf</u>. Comparing their cardinality, it is enough to show

$$g_0^i h g_0^{-i} \neq g_0^j h g_0^{-j} \quad \text{if } 0 \leq i < j \leq p-1.$$

If not, $h g_0^k = g_0^k h$ for some $0 < k < p$. Then

$h \in C_G(\underbrace{\langle g_0 \rangle}_{\text{Sylow } p\text{-gp}}) \subseteq N_G(\langle g_0 \rangle)$. On the other hand, $[G : N_G(\langle g_0 \rangle)] = p+1 = [G : \langle g_0 \rangle]$.

This implies $N_G(\langle g_0\rangle) = \langle g_0\rangle$. Therefore $h \in \langle g_0\rangle$, which contradicts the assumption that $h \neq e$ and $o(h) \neq p$.

<u>Claim</u>. $C_G(h) = H$.

<u>Pf</u>. $[G : C_G(h)] = |Cl(h)| = |H \setminus \{e\}| = p$.

by the previous claim and the fact that $gHg^{-1} = H$

So $|C_G(h)| = p+1$. Hence $C_G(h) \subseteq G \setminus \{g \in G \mid o(g) = p\}$; this implies $C_G(h) \subseteq H$. Now comparing their cardinality we get $C_G(h) = H$. ∎

Hence H is a normal subgroup. ∎

Notice that we have proved more (for odd prime p): if $n_p \neq 1$, then $G \setminus \bigcup_{i=0}^{p} P_i$ is a single conjugacy class. Using this you can prove that, if $n_p \neq 1$, then p is a Mersenne prime; that means $p = 2^n - 1$ for some $n \in \mathbb{Z}^+$.

Lecture 08: appendix on the size of HK

Monday, October 16, 2017 10:37 AM

When we were classifying groups of order pq, we used the following formula for $|HK|$ where H and K are subgroups of G:

$|HK| = \frac{|H||K|}{|H\cap K|}$. We pointed out that this can be proved showing

$H/_{H\cap K} \longrightarrow HK/_K$, $h(H\cap K) \longmapsto hK$ is a bijection.

Knowing the above map is a bijection, we get that

$$\left|H/_{H\cap K}\right| = \left|HK/_K\right| \text{; hence} \quad |HK| = \left|HK/_K\right| |K|$$

$$= \left|H/_{H\cap K}\right| |K|$$

$$= \frac{|H||K|}{|H\cap K|}.$$

<u>Warning</u>. In general HK is not a subgroup.

It is a subgroup if and only if it is symmetric; that means $(HK)^{-1} = HK$

Alternatively

HK is a subgroup if and only if $HK = KH$.