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 \( P_0 \cap Q_0 = \mathbb{Z} \) as \( \gcd (|P_0|, |Q_0|) = 1 \), and \( |P_0 \cap Q_0| = |P_0| \) and \( |P_0 \cap Q_0| = |Q_0| \). Thus \( |P_0| = |P_0 \cap Q_0| = |G| \); therefore \( G = P_0 Q_0 \).

Suppose \( P_0 = \{ e, g_1, \ldots, g_{p-1} \} \) and \( Q_0 = \{ e, h_0, \ldots, h_{q-1} \} \). Then \( G = \{ g_i h_j : 0 \leq i < p, 0 \leq j < q \} \). Moreover, since \( Q_0 \triangleleft G \), \( g_i h_j g_i^{-1} = h_{k_j} \). Comparing the order of both sides, we get that \( q = \frac{q}{\gcd (k_j, q)} \) (why ?); and so \( \gcd (k_j, q) = 1 \). Moreover, since \( P_0 \to \text{Aut}(Q_0) \), \( g_i \mapsto \) conjugation by \( g_i \) is a group homomorphism, we get that \( h_0 \mapsto h_{k_0} \) is an automorphism of \( Q_0 \), and \( q^P = 1 \).

Hence \( h_0 \equiv h_{k_0} \pmod{q} \), which happens exactly when \( k_0 \equiv 1 \pmod{q} \).

Having a \( k_0 \) which satisfies \( \circ \) uniquely determines the group structure of \( G \). In particular, if \( p \nmid q-1 \), then \( k_0 \equiv 1 \pmod{q} \): \( \text{ord}_q k_0 = p-1 \) and \( q-1 = \text{ord}_p q \). And so \( g_0 h_0 = h_0 g_0 \); and \( \text{ord}(g_0 h_0) = pq \); which implies \( G \cong \mathbb{Z}/pq \mathbb{Z} \).
Problem. Suppose $p$ is prime, and $G$ is a finite group of order $p(p-1)$. Prove that $G$ has a normal subgroup of order $p$.

**Pf.** Let $n_p = |Syl_p(G)|$. By Sylow's theorems, we have

$$n_p | p-1 \quad \text{and} \quad n_p \equiv 1 \pmod{p}.$$ 

If $n_p \neq 1$, then $p | n_p - 1$ implies that $p \leq n_p - 1$; and so $p+1 \leq n_p \times 2$. On the other hand, $n_p | p-1$ implies $n_p \leq p-1$; which contradicts $\times 2$.

Problem. 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 $p+1$.

**Pf.** Let $n_p = |Syl_p(G)|$. If $n_p = 1$, then by Sylow's 2nd 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 $n_p = |G : N_G(P)|$ (where $P_o$ is a Sylow $p$-subgroup), we have $n_p | p+1$. By Sylow's 3rd theorem, $n_p \equiv 1 \pmod{p}$. As $p | n_p - 1$ and $n_p \neq 1$, we get that $n_p \geq p+1$. Since $n_p | p+1$ 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 $\text{Syl}_p(G) = \{P_0, P_1, \ldots, P_g\}$. Since $P_i$'s have prime order, for $i \neq j$ we have $P_i \cap P_j = \{e\}$. Hence

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

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

$$ G = \{x \in G \mid o(x) = p\} \cup H \quad \text{where} \quad |H| = p(p+1) - (p^2 - 1) = p+1. $$

Notice that if $H \leftrightarrow o(h) 
eq p$. 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

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

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

Proof. Comparing their cardinality, it is enough to show

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

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

$$ h \in C_G(<g_0>) \subseteq N_G(<g>) \quad \text{in the other hand,} \quad |G : N_G(<g>)| = p+1 \quad \text{Sylow p-group.} $$
This implies $N_G(G_0) = \langle g \rangle$. Therefore $h \in \langle g \rangle$, which contradicts the assumption that $h \neq e$ and $o(h) \neq p$.

**Claim.** $C_G(h) = H$.

**Pf.** $|G : C_G(h)| = |Cl(h)| = |H \setminus g \mathbb{Z}_p| = p$.

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

So $|C_G(h)| = p + 1$. Hence $C_G(h) \subseteq G \setminus \{g \in G | o(g) = p^c\}$. 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 $G \setminus \bigcup \mathbb{Z}_p$ 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 $n \in \mathbb{Z}^+$.
When we were classifying groups of order \(pq\), we used the following formula for \(\text{lHKl}\) where \(H\) and \(K\) are subgroups of \(G\):

\[
\text{lHKl} = \frac{\text{lHl} \text{lKl}}{\text{lHnKl}}.
\]

We pointed out that this can be proved showing

\[
\frac{H}{HnK} \rightarrow HK/K, \quad h(HnK) \mapsto hK
\]

is a bijection.

Knowing the above map is a bijection, we get that

\[
\left|\frac{H}{HnK}\right| = \left|\frac{HK}{K}\right|; \quad \text{hence} \quad \text{lHKl} = \left|\frac{HK}{K}\right| \text{lKl}
\]

\[
= \left|\frac{H}{HnK}\right| \text{lKl}
\]

\[
= \frac{\text{lHl} \text{lKl}}{\text{lHnKl}}.
\]

\[\text{Warning: In general } HK\text{ is not a subgroup.}\]

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 \(HK = KH\).