March 28^{th}

Recall: (Sylow's Theorem) Let G be a group with $|G| = p^n m$ and $p \nmid m$.

1) If $1 \leq k \leq n$, then G has a subgroup of order p^k. In particular, $Syl_p(G) \neq \emptyset$.
2) If $P \in Syl_p(G)$ and Q is any p-subgroup of G, then there exists an element $g \in G$ so that $Q \leq gPg^{-1}$. In particular, all p-Sylow subgroups are conjugate.
3) We have $n_p(G) \equiv 1 \pmod p$. Moreover,

$$n_p(G) = \frac{G}{|N_G(P)|} \text{ for any } P \in Syl_p(G),$$

where $N_G(P) = \{g \in G : gPg^{-1} = P\}$. Furthermore, $n_p(G) \mid m$.

Example: Let G be a group of order $63 = 3^2 \cdot 7$. We know (From 1.) there is a $P \in Syl_7(G)$. Similarly, $n_7(G) \equiv 1 \pmod 7$ and $n_7(G) \mid 9$. From this, we must have that $n_7(G) = 1$, so $Syl_7(G) = \{P\}$. But also $gPg^{-1} \in Syl_7(G)$. In particular, $gPg^{-1} = P$ (From 2.) $\forall g \in G$. Thus $P \trianglelefteq G$, so G/P is a group of order 9. Hence $G/P \cong \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Corollary: Let G be a finite group and $P \in Syl_p(G)$ for $p \mid |G|$. Then $P \trianglelefteq G$ iff $Syl_p(G) = \{P\}$.

Proof. ($\Rightarrow$) Assume $P \trianglelefteq G$. Let $Q, P \in Syl_p(G)$. So $\exists g \in G$ s.t. $Q \leq gPg^{-1}$. But $|Q| = |gPg^{-1}| = p^n$ if $|G| = p^n m$ w/ $p \nmid m$. Hence $Q = gPg^{-1}$. However, we also have that $P \trianglelefteq G$, hence $P = gPg^{-1}$. So $Q = P$.
($\Leftarrow$) Assume $Syl_p(G) = \{P\}$. We have $gPg^{-1} \in Syl_p(G)$ $\forall g \in G$. So $gPg^{-1} = P$ $\forall g \in G$. Hence $P \trianglelefteq G$. $\square$

Definition: We say a group is <u>simple</u> if it has no proper normal subgroups.

Example: There are no simple groups of order $56 = 2^3 \cdot 7$.
Let $|G| = 56$. We have:

$$n_7(G) \equiv 1 \pmod 7 \text{ and } n_7(G) \mid 8,$$

which implies $n_7(G) = 1$ or $n_7(G) = 8$.
Case 1: $n_7(G) = 1$. This implies G has a unique normal 7-sylow subgroup. The previous corollary gives it must be normal, so G is not simple.
Case 2: $n_7(G) = 8$; i.e., $Syl_7(G) = \{P_1, \dots, P_8\}$. Recall that $P_i \cap P_j$ is a subgroup of P_i and P_j. Thus, $|P_i \cap P_j| \cdot |P_i| = 7$. So $|P_i \cap P_j| = 1$ or 7.
↳ Subcase 1: $|P_i \cap P_j| = 7$. This implies $P_i = P_j$, so if $P_i \neq P_j$, then the only element they share is e_G.
If $g \in P_i$ and $g \neq e_G$, then $|g| = 7$.
We have each P_i contains 6 elements of order 7. Since $P_i \cap P_j = \{e_G\}$, this gives $8 \cdot 6 = 48$ elements of order 7 in G.

We know $Syl_2(G) \neq \emptyset$. If $Q \in Syl_2(G)$, then $|Q| = 8$. Elements of Q must have order dividing 8. The elements of order 7 along with Q gives 56 elements.
I don't Understand this, see note from March 28^{th}.

Definition: Let H, K be subgroups of G, $|G| < \infty$. We define the product of groups HK as:

$$HK = \{hk : h \in H, k \in K\}.$$

Lemma: Let H, K be subgroups of G, $|G| < \infty$. If $H \cap K = \{e_G\}$, then $|HK| = |H| \cdot |K|$.

Proof. Claim: if $h_1 k_1 = h_2 k_2$, then $h_1 = h_2$ and $k_1 = k_2$. Once this claim is shown, we see that $|HK| = |H| \cdot |K|$.
If $h_1 k_1 = h_2 k_2$, then $h_2^{-1} h_1 k_1 = k_2$. Moreover, $h_2^{-1} h_1 = k_2 k_1^{-1}$. But $h_2^{-1} h_1 \in H$ and $k_2 k_1^{-1} \in K$. Thus $h_2^{-1} h_1, k_2 k_1^{-1} \in H \cap K = \{e_G\}$. Hence $h_2^{-1} h_1 = e_G$ and $k_2 k_1^{-1} = e_G$.
Thus $h_1 = h_2$ and $k_1 = k_2$. Why does this imply $|HK| = |H| \cdot |K|$. $\square$.

Proposition: Let $H, K \trianglelefteq G$. Then $HK \trianglelefteq G$ iff $HK = KH$.
Proof. ($\Rightarrow$) Let $x \in HK$. Since $HK \leq G$, $x^{-1} \in HK$. Write $x^{-1} = hk$ for some $h \in H$ and $k \in K$. Then $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1} h^{-1} \in KH$. Thus $HK \subseteq KH$. The same argument works for $KH \subseteq HK$. Hence $HK = KH$.
($\Leftarrow$) Since $H, K \leq G$, $e_G \in H$ and $e_G \in K$. Hence $e_G = e_G \cdot e_G \in HK$, so $HK \neq \emptyset$.
Let $x, y \in HK$. We can write $x = h_1 k_1$ and $y = h_2 k_2$.
We have $xy^{-1} = h_1 k_1 (h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$. Note that $k_1 k_2^{-1} h_2^{-1} \in KH$, but since $KH = HK$, $k_1 k_2^{-1} h_2^{-1} = h_3 k_3$ for some $h_3 \in H$, $k_3 \in K$.
Thus, $xy^{-1} = h_1 h_3 k_3 \in HK$. Thus $HK \leq G$.