Let $\text{Friday, November 15, in the beginning of the recitation. } NO\ LATE\ HOMEWORK\ WILL\ BE\ ACCEPTED.$

1. This problem is a continuation of problem 4 on Homework 7. Let $G$ be a a finite group and $H \leq G$ be a subgroup.
   (a) Let $p$ be the smallest prime which divides $|G|$ and assume that $|G : H| = p$. Prove that $H$ is a normal subgroup of $G$ (compare to problem 2 on page 53 of Herstein, which was part of Homework 5).
   Hint: Using the notation of problem 4 on Homework 7, show that $|G/K|$ divides $p!$. What does this say about the relation between $K$ and $H$?
   (b) Show that if $|G|$ does not divide $|G : H|$ and $H \neq G$ then $G$ is not a simple group.
   (c) Let $p$ be a prime and $G$ a group of order $p^n$. Show that any subgroup of $G$ of order $p^{n-1}$ is normal in $G$.

2. Let $G$ be a finite group and $p$ a prime which divides $|G|$. This problem gives a different proof of Cauchy’s theorem, which also gives some information on the number of elements of order $p$ in $G$.
   (a) Let $S = \{ (x_1, \ldots, x_p): x_1, \ldots, x_p \in G, x_1 \cdots x_p = e \}$ denote the set of all ordered $p$-tuples of elements of $G$ whose product is the identity. Show that $|S| = |G|^{p-1}$.
   (b) Define $T : S \to S$ by $T(x_1, \ldots, x_p) = (x_p, x_1, \ldots, x_{p-1})$ ($T$ is often called the cyclic right shift). Show that $T \in A(S)$ and that if $p \neq 2$ or there is some $a \in G$ with $a^2 \neq e$ then the order of $T$ in $A(S)$ equals $p$.
   (c) Let $H = \langle T \rangle$ be the subgroup of $A(S)$ that is generated by $T$. For $(x_1, \ldots, x_p), (y_1, \ldots, y_p) \in S$ write $(x_1, \ldots, x_p) \sim (y_1, \ldots, y_p)$ if there is some $R \in H$ such that $(y_1, \ldots, y_p) = R(x_1, \ldots, x_p)$. Show that $\sim$ is an equivalence relation on $S$ and that the equivalence classes have order either $p$ or 1.
   Hint: for the second assertion fix $(x_1, \ldots, x_p) \in S$ and define $K = \{ R \in H : R(x_1, \ldots, x_p) = (x_1, \ldots, x_p) \}$. Show that $K$ is a subgroup of $H$. What are the possible values of $|K|$?
   (d) Write $|S|$ as the sum of the sizes of equivalence classes of $\sim$. What can you say about the number of equivalence classes of order 1? Deduce that the number of elements of order $p$ in $G$ is of the form $-1 + kp$ for some integer $k$.

3. Let $G$ be a group and $p$ a prime such that $p^n$ divides $G$ but $p^{n+1}$ does not divide $G$. Fix an integer
   $1 \leq k \leq n$. Prove that any group $A \leq G$ of order $p^k$ is contained in a Sylow $p$-subgroup of $G$.
   Hint: Adapt the proof of Sylow’s second theorem from class (which is identical to the proof of
   Theorem 2.12.2 on page 99 of Herstein) to establish this assertion. Namely, use the same reasoning
   to show that if $B$ is a Sylow $p$-subgroup of $G$ then there must be some $x \in G$ such that $A \subseteq xBx^{-1}$.

4. Sylow’s first theorem does not extend to subgroups whose order is not a power of a prime: show that $A_4$ does not have a subgroup of order 6 even though 6 divides $|A_4| = 12$. Does $A_5$ have a subgroup of order 30?

5. Let $p$ be a prime. We proved in class that any group of order $p^2$ must be Abelian. Show that this is not necessarily true for groups of order $p^3$ by considering

$$G = \left\{ \begin{pmatrix} 1 & [x] & [z] \\ 0 & 1 & [y] \\ 0 & 0 & 1 \end{pmatrix} : [x], [y], [z] \in \mathbb{Z}_p \right\}.$$ 

Show that $G$, equipped with the usual matrix multiplication, is a group. Show that $|G| = p^3$ and that $G$ is not Abelian.