Let $G$ be a group of order $p^nt$, where $p$ is prime to $t$ and $n \geq 1$. As in class, we let $S$ be the set of subsets of $G$ having $p^n$ elements and we view $S$ as a $G$-set in the natural way. (If $X \in S$, $gX$ is the set of $gx$ with $x \in X$.) Recall from class that the size of the orbit of $X$ is either exactly $t$ or else is a multiple of $p$. Show that every orbit of size $t$ contains exactly one $p$-Sylow subgroup of $G$ and deduce the congruence $\#(S) \equiv st \mod p$, where $s$ is the number of $p$-Sylow subgroups of $G$.

If $P$ is a $p$-Sylow subgroup of $G$, let $O(P) \subseteq S$ be the orbit of $P$, where we consider $P$ as an element of $S$. This construction gives us a map from the set of $p$-Sylow subgroups of $G$ to the set of orbits for the action of $G$ on $S$. The stabilizer of $P \in S$ clearly contains $P$. By what we saw in our class discussion, the stabilizer must be exactly $P$ and $O(P)$ must contain exactly $t$ elements. We need to check that the map from the set of Sylow subgroups to the set of orbits with $t$ elements is 1-1 and onto. If $P$ and $P'$ are $p$-Sylow subgroups such that $O(P) = O(P')$, then $P' = gP$ for some $g \in G$. Since $gP$ contains the identity element of $G$, the inverse of $g$ must be in $P$. Thus $g \in P$ and $P' = gP = P$. Hence the map is 1-1. To see surjectivity, suppose that the orbit of $X \in S$ has $t$ elements. Then the stabilizer of $X$ is a $p$-Sylow subgroup $P$. Take $x \in X$; then we get $X = Px$. The orbit of $X$ is also the orbit of $x^{-1}X = x^{-1}Px$, so it's $O(Q)$ where $Q$ is the $p$-Sylow subgroup $x^{-1}Px$.

The indicated congruence follows immediately because $S$ is the disjoint union of its orbits under the action of $G$. The orbits whose orders are not divisible by $p$ all have $t$ elements. There are $s$ such orbits.

Let $G = S_p$ be the symmetric group on $p$ letters, where $p$ is a prime number. Show that $G$ has $(p - 2)!$ $p$-Sylow subgroups and deduce the congruence $(p - 1)! \equiv -1 \mod p$, which is known as Wilson’s Theorem. Find the number of $p$-Sylow subgroups of $S_{2p}$ if $p$ is an odd prime (i.e., $p \neq 2$).

An important point is that the number of elements of order $p$ in a group is $p - 1$ times the number of subgroups of order $p$ in the group. Indeed, each subgroup of order $p$ has $p - 1$ elements of order $p$ in it, and an element of order $p$ is in a unique subgroup of order $p$, namely the group that it generates. In $S_p$, there are $(p - 1)!$ elements of order $p$. To see this, we think about the cycle decomposition of an element of order $p$ and realize that the elements of order $p$ in $S_p$ are exactly the $p$-cycles. A $p$-cycle is described by a list $(a_1, \ldots, a_p)$, where the $a_i$ are just the numbers from 1 to $p$, listed in some order. There are $p!$ lists, but each $p$-cycle is described by $p$ different lists because lists should really be viewed as lying on a circle. Hence there are $(p - 1)!$ elements of order $p$ and thus $(p - 2)!$ $p$-Sylow subgroups of $S_p$. We get $(p - 2)! \equiv 1 \mod p$ by the Sylow theorems; Wilson’s theorem follows on multiplying by $p - 1$. (See also http://planetmath.org/encyclopedia/GroupTheoreticProofOfWilsonsTheorem.html.)

The problem about $S_{2p}$ looked harder than I intended, so I decided to take it out. On reflection, I decided that the best way to do the problem is to write down one $p$-Sylow subgroup $P$ of $S_{2p}$, calculate the order of the normalizer $N$ of $P$, and then realize that the answer is the index of $N$ in $S_{2p}$. Take $P$ to be the group of order $p^2$ that is generated by the two $p$-cycles $(1 \cdots p)$ and $(p + 1 \cdots 2p)$. The only $p$-cycles in $P$ are the various non-trivial powers of the two generators. If $\sigma$ conjugates $P$ to $P$, then it has to map $(1 \cdots p)$ either to a power of itself or to a power of $(p + 1 \cdots 2p)$, and it has to map $(p + 1 \cdots 2p)$ either to a power of itself or to a power of $(1 \cdots p)$.

There are two types of $\sigma$: those that map $\{1, \ldots, p\}$ to itself and those that map $\{1, \ldots, p\}$ to $\{p+1, \ldots, 2p\}$. Say $\sigma$ is going to preserve $\{1, \ldots, p\}$ and will map each of $(1 \cdots p)$ and
If $X$ is a subset of a group $G$, let $C(X)$ be the centralizer of $X$, i.e., the group of those elements of $G$ that commute with all elements of $X$. Show that $C(X) = C(C(C(X)))$.

This one turned out to be a matter of simple logic, with no deep mathematics involved. If $X$ is a subset of $G$, then $X$ commutes with all elements in $C(X)$, so $X$ belongs to the commutator of $C(X)$: we have $X \subseteq C(C(X))$. Apply this with $X$ replaced by $C(X)$; we get $C(X) \subseteq C(C(C(X)))$. Because $X$ is in $C(C(X))$, the condition of commuting with $C(C(X))$ is at least as stringent as the condition of commuting with $X$, so that $C(C(C(X))) \subseteq C(X)$.

Let $G$ be a group whose order is twice an odd number. For $g \in G$, let $\alpha_g$ be the permutation of $G$ given by the formula $x \mapsto gx$. Show that $\alpha_g$ is an even permutation if and only if $g$ has odd order. Conclude that the elements of $G$ with odd order form a subgroup $H$ of $G$ with $(G : H) = 2$. Explain in your solution why it makes sense to talk about the sign of the permutation $\alpha_g$; the potentially complicating issue is that $G$ is not an ordered set.

Let $G$ be a group with $n$ elements, and let $g$ be an element of $G$. After we order the elements of $G$, multiplication by $g$ (i.e., the map $\alpha_g$) becomes a permutation $\sigma$ of $\{1, \ldots, n\}$. If we re-order the elements of $G$, we change $\sigma$ into a permutation of the form $\tau \sigma \tau^{-1}$, with $\tau \in S_n$. Since $\sigma$ and $\tau \sigma \tau^{-1}$ have the same sign, we can declare the sign of $\alpha_g$ to be the sign of $\sigma$; this number in $\{\pm 1\}$ will be well defined.

Suppose that $g$ has order $m$; note that $m$ divides $n$. The cycle decomposition of $\alpha_g$ reflects the decomposition of $G$ into orbits under the action of the subgroup of $G$ consisting of the powers of $\alpha_g$. These orbits will have length $m$, and there will be $n/m$ orbits. The sign of $\alpha_g$ is thus $((-1)^{m+1})^{n/m}$. Hence $\alpha_g$ is an odd permutation if and only if $m$ is even and $n/m$ is odd.

In the situation of the problem, the order of $G$ is twice an odd number. Hence if $m$ is even, $n/m$ is automatically odd. Thus the elements with even order are exactly those whose signs are odd; the elements of odd order are exactly those with even sign. (We declare the sign of $g$ to be the sign of $\alpha_g$.) The odd-order elements constitute the kernel of the map $G \rightarrow \{\pm 1\}$ defined by $g \mapsto \text{sign } g$. Therefore, they form a subgroup of $G$.

Let $G$ be a group of order $2p$, where $p$ is an odd prime number. Show that $G$ is cyclic if and only if the 2-Sylow subgroup of $G$ is normal.

If $G$ is cyclic, then it has a unique 2-Sylow subgroup: finite cyclic groups have at most one subgroup of a given order. Thus the 2-Sylow of $G$ will be normal. Suppose now $G$ has a normal 2-Sylow subgroup $H$. It will also have a normal $p$-Sylow subgroup $P$. (A subgroup of index 2 in a finite group is always normal.) It follows that $G = HP$ is isomorphic to the product $H \times P$. (Recall problem 13 of Chapter I, which appeared on the previous assignment.) The groups $H$ and $P$ are cyclic groups of co-prime order, so their product is again cyclic.

How about \(S_3 \times \mathbb{Z}/5\mathbb{Z}\) and the dihedral group of order 30? The first group has only 3 elements of order 2, whereas the second group has 15 elements of order 2.

7. Calculate the order of the conjugacy class of \((1 \ 2)(3 \ 4)\) in the symmetric group \(S_n\) (\(n \geq 4\)). Find the order of the centralizer of \((1 \ 2)(3 \ 4)\) in \(S_n\).

The conjugacy class consists of all products \((\sigma(1) \sigma(2)) (\sigma(3) \sigma(4))\), where \(\sigma\) runs over \(S_n\). Thus the conjugacy class consists of all products of two disjoint transpositions. The number of such products is \(n(n-1)(n-2)(n-3)/8\), if I'm not mistaken: \((a \ b)\) is the same as \((b \ a)\), and \((a \ b)(c \ d) = (c \ d)(a \ b)\). The centralizer of an element is a stabilizer under the action of \(S_n\) on itself by conjugation. I conclude that the centralizer of \((1 \ 2)(3 \ 4)\) has order \(8n!/n(n-1)(n-2)(n-3) = 8(n-4)!\). This makes perfect sense, since the centralizer contains the symmetric group on \(\{5,6,\ldots, n\}\), the 4-cycle \((1 \ 3 \ 2 \ 4)\), and the 2-cycles \((1 \ 2)\) and \((3 \ 4)\).

8. Suppose that \(G\) is a subgroup of the symmetric group \(S_n\) and that the order of \(G\) is a power of a prime number that does not divide \(n\). Show that some element of \(\{1, \ldots, n\}\) is left fixed by all permutations in \(G\).

The order of \(G\) has the form \(p^k\), where \(p\) is a prime number. The assumption of the problem is that \(p\) does not divide \(n\). (Thanks to Chu Wee for clarifying this on the comments page.) The group \(G\) acts on the set \(S = \{1, 2, \ldots, n\}\). We are supposed to show that the set \(S^G\) is non-empty; here, \(S^G\) is the set of elements of \(S\) that are fixed by all elements of \(G\). The congruence \(#(S) \equiv #(S^G)\) mod \(p\) was established in class. The left-hand side, \(#(S) = n\) is prime to \(p\), so the right-hand side, \(#(S^G)\), is non-zero mod \(p\) as well. Consequently, \(#(S^G)\) is non-zero, which means that \(S^G\) is non-empty.

9. Suppose that \(G\) is a group with three normal subgroups \(N_1, N_2, N_3\). Assume that \(G = N_i N_j\) and that \(N_i \cap N_j = \{e\}\) for \(i \neq j\). Show that \(G\) is abelian and that the three normal subgroups are isomorphic to each other.

As in the solution to problem 13 of Chapter I, elements of \(N_i\) commute with elements of \(N_j\) whenever \(i\) and \(j\) are distinct indices and \(1 \leq i,j \leq 3\). Thus elements of \(N_1\), for instance, commute with elements of \(N_2 N_3 = G\). Thus \(N_1\) is in the center of \(G\); so is \(N_2\), by symmetry. Hence \(G = N_1 N_2\) is in the center of \(G\), so that \(G\) is abelian. Now consider the map \(N_1 \to G/N_2\) gotten by composing the inclusion \(N_1 \hookrightarrow G\) and the canonical map \(G \to G/N_2\). This map is an isomorphism of groups because \(G = N_1 N_2\) and \(N_1 \cap N_2 = \{e\}\). Thus \(G/N_2\) is isomorphic to \(N_1\); by symmetry, it is also isomorphic to \(N_3\). The conclusion now follows: \(N_1\) and \(N_3\) are isomorphic, and similarly \(N_1\) and \(N_2\) are isomorphic.

The last 8 problems came from old Math Department prelim exams, by the way.