Math 504, 10/3

Last time we stated the Sylow theorems, which you will prove in homework for this week; now we apply them. Let p, q be distinct primes with $p < q$ and G a group of order pq. Then the numbers n_p, n_q of p-Sylow and q-Sylow subgroups of G are congruent to 1 mod p, q, respectively, and divide q, p, respectively. It follows at once that $n_q = 1$: the only divisor of p that is congruent to 1 mod q is 1, whence the q-Sylow subgroup is unique and normal (since any conjugate of it is also a q-Sylow subgroup). The same is true of the p-Sylow subgroup if q is not congruent to 1 mod p. In this case then the p- and q-Sylow subgroups are both normal and have trivial intersection, whence by counting their product is all of G. By a standard result in undergraduate group theory, G must be the direct product of these subgroups, which are both cyclic, whence in fact G itself is cyclic, of order pq. This actually holds if the p-Sylow subgroup is normal, even if q is congruent to 1 mod p. Now suppose that q is congruent to 1 mod p and a p-Sylow subgroup is *not* normal. Letting Q be the q-Sylow subgroup and P be any p-Sylow subgroup, we again have that Q and P intersect trivially and $G = QP$, but now the elements of P need not commute with those of Q. We still get an *action* of P on Q by group automorphisms, via conjugation: if $x \in P, y \in Q$, then $xyx^{-1} \in Q$, and if x is fixed the map sending any y in Q to xyx^{-1} is an automorphism of Q. In this situation we say that G is the *semidirect* product of P and Q, notated either as $P \ltimes Q$ or $P \rtimes Q$. More generally, let N, H be any two groups such that H acts on N by group automorphisms; if $h \in H, n \in N$, denote the action of h on n by $h \cdot n$. Then we can make the Cartesian product $N \times H$ into a group via $(n_1, h_1)(n_2, h_2) = (n_1 h_1 \cdot n_2), h_1 h_2)$. One checks immediately that the group axioms are satisfied; here the multiplication is the same as for the direct product of N and H in the second coordinate, but is "twisted" in the first coordinate by replacing n_2 by $h_1 \cdot n_2$. We denote this group as $N \ltimes H$ or $N \rtimes H$ (or $H \rtimes N$ or $H \ltimes N$) and call it the semidirect product of N and H. Whenever a group G has a normal subgroup N and another subgroup H such that $G = NH$ and H and N intersect trivially, then G can always be viewed as the semidirect product of N and H. In our current example, the full automorphism group of the cyclic group $\mathbf{Z}_q$ of order q is known to be itself cyclic of order $q - 1$ (we will learn this later) and so admits a cyclic subgroup of order p whenever p divides $q - 1$, which can be used to define a nontrivial action of the cyclic group $\mathbf{Z}_p$ of order p on $\mathbf{Z}_q$ by automorphisms. The upshot is that *any group of order pq with p, q distinct primes is cyclic if neither of p, q is congruent to 1 mod the other, but a nonabelian group of order pq exists whenever p, q are distinct primes with q congruent to 1 mod p.*

Sometimes the Sylow theorems force one of the Sylow subgroups to be normal, but don't tell us which one it is (because either one can be). For example, in homework this week, you are asked to show that, given a group G of order 56, either its 2-Sylow or its 7-Sylow subgroup must be normal; but either possibility can occur. The key idea is to argue that if there is more than one 7-Sylow subgroup (or equivalently, no 7-Sylow subgroup is normal), then you can count how many elements of order 7 there are in G, and this turns out to be so many

that the 2-Sylow subgroup is forced to be normal.

We conclude our brief treatment of Sylow theory with an illustration of how it can be used to analyze the structure of certain groups even if they are simple (so contain no nontrivial normal subgroups). Let G be a simple group of order 60. The number n_5 of 5-Sylow subgroups must then be 1 or 6, whence by simplicity it must be 6. Then G acts on its six 5-Sylow subgroups by conjugation and the action is faithful since G is simple. Since the alternating group A_6 is also simple, it follows easily that G is isomorphic to a subgroup of it. This subgroup H has six left cosets in A_6, one of which is H itself; the others are permuted by H. Simplicity of both G and A_5 then forces G to be isomorphic to A_5: *up to isomorphism, A_5 is the only simple group of order 60.*

We look at one more example, without proving it in detail. Let G be a simple group of order 168. As above we see that it must have exactly 8 7-Sylow subgroups; it acts on the set of these by conjugation. This time however G is much too small to act by all even permutations on 8 elements. To pin down its structure, start with the set $\mathbf{Z}_7$ of integers mod 7 and add a new element ∞ (infinity), calling the resulting set $P = \mathbb{P}^1(\mathbf{Z}_7)$. For $a, b, c, d \in \mathbf{Z}_7$ with $ad - bc = 1$, define the fraction $(az + b)/(cz + d)$ for z in P by decreeing it to be a/c if $z = \infty$ and c is not 0; while it is ∞ if $c = 0$ (note that then a cannot be 0). Analogously, define $(az + b)/(cz + d)$ to be ∞ if its numerator is 0 (since then its denominator cannot be 0). The set of all maps sending $z \in P$ to $(az + b)/(cz + d)$ forms a group under composition, called the group of linear fractional transformations. This group is isomorphic to the quotient $PSL(2, \mathbf{Z}_7)$ of 2 x 2 matrices over $\mathbf{Z}_7$ of determinant 1, modulo the scalar matrices ± 1; the order of this group is 168, as desired. Then it turns out (though we will not prove this) that G is necessarily isomorphic to this group.