........How to.....

GET MORE OUT OF THE SYLOW THEOREMS

BACKGROUND:

The usual application of the Sylow theorems is to determine how many conjugate Sylow subgroups there are for the various prime divisors of the order of a given group. The third theorem gives number-theoretic criteria for determining all possibilities, and then we usually appeal to element-counting arguments to whittle these down to the actualities. A complication that doesn't seem to arise in lower level textbook problems is the situation where conjugate Sylow subgroups may intersect nontrivially. This drastically affects our ability to count elements with any confidence, so we need another window on what is happening. For simple groups, there are techniques for deciding if various small values of the number of conjugates are feasible. They are based on the requirement that no proper nontrivial normal subgroup can ever appear.

DEFINITIONS:

1) A *p-Sylow subgroup* (p-SSG) is a group guaranteed to exist by virtue of Sylow's First Theorem. The constraints on how many conjugate p-Sylow subgroups may exist, usually denoted by N_p, is contained in Sylow's Third Theorem.

4) The *normalizer* of a subgroup $H \leq G$, denoted by $N_G(H)$, is the largest subgroup of G in which H is normal.

5) The *centralizer* of an element $x \in G$, denoted by $C_G(x)$, is the subgroup of G consisting of all elements that commute with x.

6) A *simple* group is one with no proper nontrivial normal subgroup.

7) A *group homomorphism* is an operation preserving mapping between two groups, specifically if G and H are groups and $\phi : G \to H$, then ϕ is a homomorphism iff for all $x, y \in G$ it is true that $\phi(xy) = \phi(x)\phi(y)$. Another way to state the operation preserving property is to say that the group operations and the mapping commute.

8) The *kernel* of a homomorphism is the preimage of the identity element in the range group.

KEY FACTS:

1) The number of conjugates of $H \leq G$ in G is given by $[G : N_G(H)]$

2) Representation on Cosets Theorem: If G is a group and $H \leq G$ with $[G : H] = n$, there is a homomorphism $\phi : G \to S_n$ with $\ker \phi \leq H$.

3) The kernel of a homomorphism is always a normal subgroup of the domain.

4) A simple group cannot have a homomorphisms to another group that admits a nontrivial kernel.

OBSERVATIONS:

1) In the event that a Sylow p-subgroup has order p and not a higher power of p, any non-trivial element shared by two conjugate subgroups would generate each group, so the groups would be identical. So we may always rely on the fact that if there are N_p Sylow p-subgroups of order p, then there must be $N_p(p-1)$ nontrivial elements among them (they all must share the identity, of course). Not so for higher powers, unfortunately.

2) Sylow's Third Theorem states that the number N_p of conjugate Sylow p-subgroups of G

satisfies $N_p \equiv 1 \bmod p$ and $N_p \mid |G|$. This usually cuts down the possibilities quite a bit. If you know that the group you are analyzing is simple, then any value of N_p that forces a nontrivial normal subgroup to appear can be ruled out. Two ways this can happen are (i) some homomorphism can be constructed that has a nontrivial kernel in G, or (ii) the center of G is discovered to be nontrivial.

3) In the first instance, we know that $N_p = [G : N_G(P)]$, where P is a p-SSG. The Representation on Cosets Theorem says that there must be a homomorphism $\phi : G \to S_{N_p}$ where $\ker\phi$ is inside $N_G(P) \leq G$. If $\ker\phi$ is not trivial, since $\ker\phi \lhd G$, G could not be simple, which contradicts our assumption. However, trivial kernels turn homomorphisms into injections, and then we would have G mapped injectively into S_{N_p}. If G is big and N_p is small, this may not be possible, and then that candidate value for N_p can be tossed out. Here are some examples:

(a) Suppose we have a simple group of order $60 = 2^2 \cdot 3 \cdot 5$. A number theoretic analysis reveals that $N_2 = 3$ is possible. This would require $[G : N_G(P_2)] = 3$, where P_2 is a Sylow 2-subgroup. By the Representation on Cosets argument above, there would have to be an injection from G to S_3.There is no room to do this (it's a blivic),.therefore $N_2 = 3$ is really not a candidate.

(b) Suppose we have a simple group G of order $108 = 2^2 \cdot 3^3$. The possibilities include $N_3 = 4$. In principle, there could be four 3-SSGs that shared a subgroup with 9 elements. We would not be able to rule anything out on the basis of an element counting argument. But again, $[G : N_G(P_3)] = 4$ implies there is an injection (homomorphism with trivial kernel) from G to S_4. Since $|S_4| = 24$, this cannot happen.

(c) Suppose we have a simple group G of order $180 = 2^2 \cdot 3^2 \cdot 5$. A possible outcome is $N_2 = 5$. Then $[G : N_G(P_2)] = 5$, where P_2 is a Sylow 2-subgroup, and by the now familiar argument there would be a homomorphism from G to S_5. Since the kernel would have to be trivial to avoid creating a proper nontrivial normal subgroup, we would have an injection of G with $|G| = 180$ into S_5 with $|S_5| = 120$. Not going to happen.

4) In the second instance, returning to example 3(a), it appears that $N_2 = 15$ is possible, as well. Suppose there are two 2-SSGs with an element in common besides the identity. Let x be such an element. Now both P and Q have order 4, so they are abelian in any case. All the elements in P and Q combined commute with x. So $P \cup Q \subset C_G(x)$. Recall that $\langle P \cup Q \rangle$ strictly contains $P \cup Q$ unless one of P or Q contains the other, so $|C_G(x)| > |P \cup Q| > 4$. On the other hand, $P \leq C_G(x)$ implies by Lagrange's Theorem that $\big|P\,|= 4\big|\,|C_G(x)|$. Moreover, $|C_G(x)| \mid |G|$. Thus $|C_G(x)|$ is a multiple of 4 between 8 and 60 which divides 60. The possibilities are 12, 20, and 60. We can dispose of $|C_G(x)| = 60$ by observing that since x evidently commutes with all elements of G, $x \in Z(G)$, and since x was a nonidentity, $|Z(G)| > 1$. Now $Z(G)$ cannot be G, because then G would be abelian and any proper nontrivial subgroup would be normal, contradicting simplicity. But then we are stuck with $Z(G)$ being a proper nontrivial normal subgroup anyhow. So $|C_G(x)| = 60$ is out. If $|C_G(x)| = 20$, we have a subgroup of index 3 in G, and the same argument used above for $[G : N_G(P_2)] = 3$ precludes $|C_G(x)| = 20$. It follows that $|C_G(x)| = 12$, and $P \cap Q = \{e\}$. Then we may count elements with the knowledge that the 2-SSGs are almost disjoint (share only the identity). Fifteen of them would account for $(4-1) \cdot 15 = 45$ elements of order 2 or 4. The smallest N_5 would be 6. This adds $(5-1) \cdot 6 = 24$ elements of order 5. We have already broken the bank on elements, so $N_2 \neq 15$.

TB 11–8-10