Comments on HW Set 2

Problem 2.

We have a group G and a normal subgroup H. Suppose that $\mathcal{K}$ is a conjugacy class in G. If $\mathcal{K} \cap H$ is non empty, choose $x \in \mathcal{K} \cap H$. Then $gxg^{-1} \in gHg^{-1} = H$ for all $g \in G$, and therefore $\mathcal{K} \subset H$. Therefore if H contains any element of a G-conjugacy class, it contains the entire G-conjugacy class.

Choose $\mathcal{K} \subset H$. The conjugation action of H on $\mathcal{K}$ preserves $\mathcal{K}$ because if two things are H-conjugate then they are G-conjugate. So $\mathcal{K}$ breaks up into H-orbits under conjugation.

If $x \in \mathcal{K}$, then the size of the H-orbit of x is $[H : C_H(x)]$ by the Orbit-Stabilizer theorem. Also, $C_H(x) = H \cap C_G(x)$, since if an element of H commutes with x then it is certainly in $G_G(x)$.

Let $x' = gxg^{-1}$ is a representative of a different H-orbit in $\mathcal{K}$. If $h \in C_H(x)$, then a calculation shows that ghg^{-1} is in $C_H(x')$. Since conjugation is bijective this shows that $C_H(x') = gC_H(x)g^{-1}$. In particular these groups have the same order and so all of the H-orbits in $\mathcal{K}$ have the same size $[H : C_H(x)]$. It follows that the number of such orbits is

$$k = [G : C_G(x)]/[H : C_H(x)].$$

The isomorphism theorems say that

$$[H : C_H(x)] = [H : H \cap C_G(x)] = [HC_G(x) : C_G(x)]$$

and then

$$k = [G : C_G(x)]/[HC_G(x) : C_G(x)] = [G : HC_G(x)].$$

Alternatively, let $\mathcal{H}$ be an H-orbit inside $\mathcal{K}$ with representative x. If $\mathcal{H}'$ is another such orbit, with representative $x' = gxg^{-1}$, then one can show that conjugation by g gives a bijection between $\mathcal{H}$ and $\mathcal{H}'$. Therefore G permutes the H-classes transitively. By the generalized version of the Orbit-Stabilizer theorem (Proposition 6) one gets that the number of orbits is $[G : N_G(\mathcal{H})]$. But g stabilizes $\mathcal{H}$ provided that $gxg^{-1} = hxh^{-1}$ for some $h \in H$. This means that $h^{-1}g$ is in $C_G(x)$ or $g \in HC_G(x)$. Conversely, if $g \in HC_G(x)$, then $g = hz$ and $gxg^{-1} = hzxz^{-1}h^{-1} = hxh^{-1}$ so $g \in N_G(\mathcal{H})$. Therefore $N_G(\mathcal{H}) = HC_G(x)$ and the orbit stabilizer theorem gives

$$k = [G : HC_G(x)].$$

Problem 4. I've already explained the counting part of this problem, so we know that if $\sigma : S_n \to S_n$ is an automorphism, and n is not 6, then σ carries transpositions to transpositions.

The trickiest part of this problem is to prove that if $\sigma : S_n \to S_n$ is an automorphism, then $\sigma((1j)) = (ab_j)$ where the b_j are distinct.

I think a proper proof of this needs an inductive argument. Assume σ is an automorphism that carries transpositions to transpositions. (This is forced unless $n = 6$ but we can assume it for this problem in general.) Suppose that $n = 3$. In this case there are only three transpositions, and $\sigma((12))$ and $\sigma((13))$ have to be different. But any two distinct transpositions in S_3 overlap in one place, so we get what we want. Now suppose that $n = 4$. Suppose that $\sigma((12)) = (ab_2)$. If $\sigma((13))$ were disjoint from (ab_2), then it would commute with (ab_2). But (12) and (13) do not commute, and σ is a homomorphism, so $\sigma((13))$ must overlap with $\sigma((12))$; we can assume that $\sigma((13)) = (ab_3)$. Now $\sigma((14))$ does not commute with either (12) or (13) so it must overlap with both (ab_2) and (ab_3). At first glance we could have $\sigma((14)) = (ab_4)$ OR $\sigma((14)) = (b_2b_3)$. But notice that $(12)(13)(12) = (23)$ so $\sigma((23)) = (b_2b_3)$. Since σ is bijective, the only possibility is that $\sigma((14)) = (ab_4)$.

Now assume that $n \geq 5$ and we know that, for $2 \leq j \leq n$, we must have $\sigma((1j)) = (ab_j)$ for some $1 \leq a \leq n$ and distinct b_j in that range. What about $\sigma((1, n+1))$? It must overlap with each of (ab_j) for $j = 1, \ldots, n$. If it doesn't have an "a", then it must be of the form (b_jb_k). But then there is a third index s in the range and (b_jb_k) does not overlap with (ab_s). So $\sigma((1n+1))$ must be of the form (ab_{n+1}) where $b_{n+1})$ is distinct from all of the previous b_j.

This completes the inductive argument.

There is one other comment about this problem. At the end, one shows that there are at most $n!$ automorphisms of S_n (except when $n = 6$). Then one argues that the inner automorphism group of S_n is S_n which has $n!$ elements, so all automorphisms must be inner.

In general, $\mathrm{Inn}(G)$ is isomorphic to $G/Z(G)$, since elements of the center of G give trivial inner automorphisms. Thus, to conclude that $\mathrm{Inn}(G) = S_n$, you need to use the fact that the center $Z(S_n)$ is trivial. This result can be found in DF. A truly complete proof needs to mention this fact.

Problem 5. The most common mistake in this problem came in the proof that H and K commute. The Sylow theorems tell you that H is normal, but it isn't necessarily the case from Sylow that K is normal. You can show that $HK = G$ and also that $HK = KH$ using the normality of H, but *this does not mean that G is abelian.* Even the fact that the orders of H and K are relatively prime isn't enough. For example, S_3 has a normal subgroup H of order 3, and a non-normal Sylow 2-subgroup K of order 2, and $HK = KH = S_3$, but S_3 is not abelian. To prove the group in the homework problem is abelian, you need to consider the fact that K acts by conjugation on H so there is a map $K \to \mathrm{Aut}(H)$. Since you know H is cyclic of order 187, it's automorphism group has order $\phi(187) = 160$. But K has order 9, and since 160 is not divisible by 3 the only map from K to $\mathrm{Aut}(H)$ is trivial. Therefore elements of K commute with elements of H and from that you see that G is abelian.

If, in the argument above, you knew that K was a normal subgroup, then you could argue that the commutator subgroup of H and K is a subgroup of $H \cap K$, therefore trivial, and so the group is abelian; but you don't know just from Sylow that K is normal.