Counterexamples to common errors on Takehome 4

Hi Folks, there were a a couple of very common errors on Takehome 4. These were difficult to discuss in full on gradescope, so instead I figured I would write up the counterexamples to various common assumptions here.

Question 1c: Ignorning that the g_i must commute.

A very common error in question 1c boiled down to the following false assumption that a map $Z_{n_1} \times \cdots \times Z_{n_r} \to G$ is the same as a set of maps $Z_{n_i} \to G$ for each i. That is, all we have to do is choose where the generator of each cyclic factor goes, and as long as they go to elements of the correct order, we get a well defined group homomorphism. This is not true. It is important that the images of the generators of the cyclic factors *commute with eachother*. Otherwise we won't get a homomorphism. Let's illustrate this with an example.

Example 1. *Let $G = D_8 = \langle r, s \mid r^4 = s^2 = 1,\ rs = sr^{-1}\rangle$, and consider maps $Z_4 \times Z_2 \to D_8$. Let $Z_4 = \langle x \rangle$ and $Z_2 = \langle y \rangle$. We can consider the maps sending $x \mapsto r$ and $y \mapsto s$ respectively. Indeed, by 1(a) this gives well defined (and even injective) homomorphism $Z_4 \to D_8$ and $Z_2 \to D_8$. But this does not induce a map $\Phi : Z_4 \times Z_2 \to D_8$. Indeed, one could ask, where does (x, y) go? Well, on one hand:*

$$\Phi(x, y) = \Phi((x, 1)(1, y)) = \Phi(x, 1)\Phi(1, y) = rs,$$

and on the other,

$$\Phi(x, y) = \Phi((1, y)(x, 1)) = \Phi(1, y)\Phi(x, 1) = sr.$$

But in D_8 we know $rs \neq sr$. This is a contradiction and so Φ cannot be a well defined homomorphism.

So we see here that it is in fact *crucial* not only that the generators go to elements of the right order (as in 1(a)), but also that their images commute.

Question 2 parts a(iii),b(ii),b(iii): Overpowered Sylow's Theorem

I will adress the a(iii) case, and remark that the other two cases are identical but with p's and q's swapped around. Let me begin by summarizing the incorrect argument.

Fake Proof. *We have $p < q$ and $p|q - 1$. If $n_p = q$ then this does not contradict that $p|q - 1$, so pick a group with $n_p = q$. The P is not normal so the product is not abelian.*

What's going wrong here? Sylow's theorems tell us that if n_p is the number of Sylow p-subgroups, it satisfies certain divisibility and congruence conditions. *The converse is not true!* That is, if some number a satisfies the numerical divisibility and congruence conditions established in Sylow's theorems, this does not imply that there is some group G with $n_p = a$. In fact there is a following theorem from the sixties:

Theorem 1 (Hall 1967)**.** *There are no finite groups with $n_3 = 22$, $n_5 = 21$ or $n_p = 1 + 3p$ for $p \geq 7$.*

The proof of this theorem uses more advanced methods than we have defined, and goes beyond the scope of this course, it allows us to produce the following counterexample to the train of thought use in the fake proof above.

Example 2. *Conseder* $66 = 3 * 22$. *The maximal 3-divisor is* 3. *Furthermore, if* $a = 22$ *then* $a \equiv 1 \mod 3$ *and* $a|22$. *Therefore a satisfies all the congruence conditions established in Sylow's theorems, but by Theorem 1 there is no group of order 66 with* $n_3 = 22$.

The point here is not that you should know Hall's theorem. I'm just using it to provide an example. The point here is that one should not automatically assume every theorem has a converse. Sylow's theorem is *not* an if and only if statement. It says that if a group exists certain congruence conditions are met, it does not assert the existence of groups meeting these conditions.

I should point out that 22 is not prime. If the other number was prime, you could use the semidirect product formalism and Cauchy's theorem to construct a group with the right number of Sylow q-subgroups. In fact, one could interpret the problem as showing that in this special case the converse to Sylow's theorem *is true!* But that is in some sense what the content of the problem is, it is still up to you to build the group!

Questions 3 and 4: Reinventing the Wheel

Did it feel like you were doing the same thing over and over again? It's probably because you did! And you didn't have to. That is: the reason we did all that work in question 2 was so that we wouldn't have to do it again in 3 and 4. That is, almost everybody did question 2 over again in problems 3 and 4 (replacing p and q with the numbers in the problem). There was a reason I asked in part (a) of both 3 and 4 which part from 2 that it fell under. So that you could USE everything you proved in problem 2. For example: In problem 2(b) you showed that if $|G| = p^2q$ with $p > q$ then $G \cong P \rtimes Q$. Then in problem 4 you have $|G| = 75 = 5^2 * 3$ with $5 > 3$. Awesome, so 2(b) applies and $G \cong P \rtimes Q$. You don't need to prove this again. You alread did!! I didn't take off points for this (often called "reinventing the wheel"), but some instructors will will, and for good reason. Writing this way this has more important drawbacks. First of all, it makes it harder to write, and much harder to read, and of course writing is about communicating clearly. Second, we do things generally not only to avoid writing the same thing over and over again, but also to see what is a general property of groups and what is specific about certain numbers. That is, is this splitting into a semidirect product a general p^2q fact or is it a fact about 3 and 5? We'd like to know the difference.