Homework #5 - Challenges key

Here are proofs for each of the parts of the challenge problems that are proof-based. I have written them to purposefully be a bit annoying; your job is to use the data-claim-warrant structure to validate the proofs, and also to say what is annoying about them.

At least one of these proofs has a subtle error in it (that I originally made by honest accident but then decided to leave in for pedagogical purposes). Can you find it?

Problem 1. Here we shall track down the details from our discussion of the mystery group of order 16 from class on Wednesday.

(a) Let $g \in G$ and suppose that $\langle g \rangle$ is a normal subgroup of order 2. Prove that $g \in Z(G)$.

Proof. Let $x \in G$. $x\langle g \rangle x^{-1} = \langle g \rangle$, so either $xgx^{-1} = e$, in which case $xg = x$, so $g = 1$, which certainly isn't true, or else $xgx^{-1} = g$. Then $xg = gx$, so $g \in Z(G)$.

Claims:

(1) $x\langle g \rangle x^{-1} = \langle g \rangle$

(2) either $xgx^{-1} = e$ or $xgx^{-1} = g$

(3) (Case 1: $xgx^{-1} = e$) $xg = x$

(4) $g = 1$

(5) which certainly isn't true

(6) (Case 2: $xgx^{-1} = g$) $xg = gx$

(7) $g \in Z(G)$

□

(b) Suppose that G is generated by two generators, say $G = \langle g, h \mid \ldots \rangle$. Prove that if $g \in Z(G)$, then $h \in Z(G)$.

Proof. A generic element of G looks like $s_1^{p_1} s_2^{p_2} \ldots s_k^{p_k}$, where $p_i \in \mathbb{Z}$ and each s_i is either g or h. Therefore, it's enough to show that $h \cdot g^p = g^p \cdot h$. But since $g \in Z(G)$, $hg = gh$, so $hg^p = g^p h$. Therefore, $h \in Z(G)$.

Claims:

(1) A generic element of G looks like...

(2) It's enough to show that...

(3) $hg = gh$

(4) $hg^p = g^p h$

(5) $h \in Z(G)$

□

(c) Let G be a finitely generated group, say $G = \langle g_1, \ldots, g_n \mid \ldots \rangle$. (Note that G doesn't have to be finite – the integers, for example, are finitely generated.) Prove that if all the generators $g_i \in Z(G)$, then G is abelian.

Proof. A generic element of G looks like $s_1^{p_1} s_2^{p_2} \ldots s_k^{p_k}$, where $p_i \in \mathbb{Z}$ and each s_i is one of the generators g_i. Therefore, it's enough to show for generic generators g_i and g_j that $g_i \cdot g_j^p = g_j^p \cdot g_i$. Since $g_i \in Z(G)$, $g_i g_j = g_j g_i$. Therefore, $g_i g_j^p = g_j^p g_i$, so G is abelian.

Claims:

(1) A generic element of G looks like...

(2) It's enough to show ...

(3) $g_i g_j = g_j g_i$.

(4) $g_i g_j^p = g_j^p g_i$

(5) G is abelian.

□

(d) Now, getting more specific: in the mystery group, we knew that $s^2 = r^8 = 1$. How did we know those two things?

Proof. (Well, not really a proof, more of just an observation.)
By looking at the lattice, $|\langle s \rangle| = 2$ and $|\langle r \rangle| = 8$. □

(e) Suppose that $\langle s \rangle$ and $\langle r^4 s \rangle$ *aren't* normal; therefore they must be conjugate. Prove that $srs = r^5$. (Hint: conjugate by r.)

Proof. First, note that $r \notin \langle r^4 s \rangle$. Therefore, $r\langle r^4 s \rangle r^{-1} = \langle s \rangle$. Either $r(r^4 s)r^{-1} = s$, in which case $r^5 s = sr$ so $r^5 = srs$, or $r(r^4 s)r^{-1} = 1$, in which case $r^5 s = r$, so $s = r^4$. But s certainly doesn't equal r^4, so $srs = r^5$.

Claims:

(1) $r \notin \langle r^4 s \rangle$

(2) $r\langle r^4 s \rangle r^{-1} = \langle s \rangle$

(3) Either $r(r^4 s)r^{-1} = s$ or $r(r^4 s)r^{-1} = 1$

(4) (Case 1: $r(r^4 s)r^{-1} = s$) $r^5 s = sr$

(5) $r^5 = srs$

(6) (Case 2: $r(r^4 s)r^{-1} = 1$) $r^5 s = r$

(7) $s = r^4$.

(8) s certainly doesn't equal r^4

□

Problem 2. Write down a full proof of Lagrange's theorem:

$$\text{if } H \leq G, \text{ then } |H| \text{ divides } |G|, \text{ and further, } |G| = [G : H] \cdot |H|.$$

(This just entails stringing together the arguments we made on the slides before the Lagrange's theorem slide, but I think it's moderately nice to see it all written out.)

Proof. It's nice to split this proof up into three little lemmas:

- First, note that for any $g \in G$, $|gH| = |H|$. To prove this, consider the function $\phi : gH \longrightarrow H$ defined by $\phi(gh) = h$. This function is injective (aka 1-1): if $gh_1 = gh_2$, then $h_1 = h_2$, so $\phi(gh_1) = \phi(gh_2)$. This function is also surjective (aka onto): if $h \in H$, then $\phi(gh) = h$. Therefore, this function is a bijection, so $|gH| = |H|$.
- Next, note that distinct cosets are disjoint. For suppose $g \in g_1H$ and $g \in g_2H$. Then there exist $h_1, h_2 \in H$ such that $g_1h_1 = g = g_2h_2$. Therefore, $g_1 = g_2(h_2h_1^{-1})$, so $g_1H = g_2H$.
- Finally, note that the cosets cover all of G, because if $g \in G$, then $g \in gH$.

So: if $|H| = m$ and $[G : H] = n$, then G is made up of n sets of m elements, so $|G| = mn$. $\square$

Problem 3. Prove that $|\operatorname{cl}_G(H)| = [G : N_G(H)]$.

Proof. (Signposts: The human-words translation of this sentence is that the number of subgroups conjugate to H is the same as the number of cosets of $N_G(H)$. Indeed, any element that makes a nontrivial conjugate of H is precisely *not* in the normalizer, so it'll make a nontrivial coset of the normalizer.)
Because I am already annoyed at typing $N_G(H)$ repeatedly, let's just call it N. Let's establish a bijection between cosets of N and conjugate subgroups of H; specifically, let's map xN to xHx^{-1}.

- This map is clearly surjective.
- This map is injective: if $xHx^{-1} = yHy^{-1}$, then $(y^{-1}x)H(y^{-1}x)^{-1} = H$, so $y^{-1}x \in N$. This means that the coset $y^{-1}xN$ is the identity coset N. Therefore, $yN = y\left(y^{-1}xN\right) = xN$.
- (A secret third thing should be here. Do you know what it is?)

$\square$