M621 Quiz 1, 09.22 **Selected solutions 9.25**

Some comments:

0. As a class, you did just fine. Continue to work hard.

1. If asked to provide a "specific counterexample", you're meant to provide a specific group or groups, specific elements, subsets, or whatever constitutes a specific counterexample.

2. Use quantifiers, and in connection with that, when you introduce a symbol, be sure to indicate a set it's contained in.

3. Get in the habit of *writing* proofs—they're explanations. Be clear about what you're doing. Keep the reader informed.

Quiz 1.

Some of the questions below involve the notion of order of an element of a group. Let's recall that definition. Let G be a group, let $g \in G$, and let e be the identity of G. The *order* of g, denoted $|g|$, is defined:

$$|g| = \begin{cases} \min\{k \in \mathbb{N} : g^k = e\}, \text{ if } & \{k \in \mathbb{N} : g^k = e\} \neq \emptyset \\ \infty, & \text{otherwise} \end{cases}$$

Recall also the statement of the *Division Theorem* (a.k.a. Division Algorithm): Suppose $a \in \mathbb{N}$, and $b \in \mathbb{Z}$. Then there exist unique integers q and r with $a > r \geq 0$ such that $b = aq + r$.

1. (15 points at most) True or false? If false, provide a *specific counterexample (1.5 point).* If you get five correct, you receive full credit on the problem.

   (a) If G is a group, $g \in G$, n is a positive integer, and $g^n = e \in \mathbb{N}$, then $|g| = n$.

   False. Let $G = (\mathbb{Z}, +)$, and let $g = 0$. So $|g| = 1$, but $g^2 (= g + g) = e$.

   (b) If G is a group, $g \in G$, and $|g| = 6$, then $(g^3)^{-1} = g^3$.

   True.

   (c) If G is a group and g, h are elements of G, then $|g| = |hgh^{-1}|$.

   True.

   (d) If G is a group having subgroups H and K, then $H \cup K$ is a subgroup of G.

   False. Let $G = (\mathbb{Z}, +)$, let $H = 2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$, and let $K = 3\mathbb{Z} = \{3z : z \in \mathbb{Z}\}$. Both H and K are subgroups of $\mathbb{Z}$, but $H \cup K$ is not closed under the operation—e.g. $\{2, 3\} \subseteq H \cup K$, but $2 + 3 = 5 \notin H \cup K$—it's not a subgroup of G.

   (e) Suppose G, K are groups, if $\Gamma : G \to K$ is a homomorphism of groups, and G is Abelian, then K is Abelian.

   False. Let $G = (\mathbb{Z}, +)$, let $H = S_3$, and let $\Gamma(z) = e$ (the identity of S_3) for all $z \in \mathbb{Z}$. Then Γ is a homomorphism, but S_3 is non-Abelian.

(f) Let n be a positive integer with $n \geq 2$:
For any $\beta \in S_n$, $\beta(12)\beta^{-1} = (\beta(1)\beta(2))$.

True.

2. (10 points) Let G be a group, let $g \in G$, and suppose that $|g| = n \in \mathbb{N}$. **Prove** that for all $k \in \mathbb{Z}$, we have $g^k = e$ implies that $n|k$.

   Proof. Suppose $g^k = e$ with $k \in \mathbb{Z}$, and $|g| = n \in \mathbb{N}$. We'll show that $n|k$.

   By the Division Theorem, there exist $q, r \in \mathbb{Z}$ such that $k = nq + r$, where $0 \leq r < n$. So $g^k = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r$. Since r is non-negative, strictly less than n, and the order of g is n, it follows that $r = 0$. But this means that $k = nq$, which gives us that $n|k$.

3. (5 points) Suppose a group G has the following presentation:
$< a, b : a^3 = b^2 = a^2 = b^3 >$. Show that G is the trivial group.

   That $a^3 = a^2$ implies (by cancellativity) that $a = e$. In like manner, $b = e$. Thus, G is generated by e, which implies $G = \{e\}$—G is trivial.

4. (8 points) Recall that a group G *acts on a set* A if the following axioms are satisfied. Let e be the identity of G.

   (a) (Axiom 0) For all $g \in G$ and all $a \in A$, $g \cdot a \in A$.
   (b) (Axiom 1) For all $g, h \in G$, and all $a \in A$, $(gh) \cdot a = g \cdot (h \cdot a)$.
   (c) (Axiom 2) For all $a \in A$, $e \cdot a = a$.

   Recall also that for each $g \in G$, a function $\sigma_g : A \to A$ is defined as follows: For all $a \in A$, $\sigma_g(a) = g \cdot a$.

   Prove, using the above axioms, that for all $g \in G$, σ_g is a permutation of A. That is, prove σ_g is one-to-one and onto.

   Proof. We must show that σ_g is both one-to-one and onto.

   We show σ_g is one-to-one. For this, it suffices to show that if a and b are in A, and $\sigma_g(a) = \sigma_g(b)$, then $a = b$. If $\sigma_g(a) = \sigma_g(b)$, then $g \cdot a = g \cdot b$. So $\sigma_{g^{-1}}(g \cdot a) = \sigma_{g^{-1}}(g \cdot b)$, or $g^{-1} \cdot (g \cdot a) = g^{-1} \cdot (g \cdot b)$. By Axiom 1, we now have that $(g^{-1}g) \cdot a = (g^{-1}g) \cdot b$. Thus $e \cdot a = e \cdot b$. Applying Axiom 2, we have $a = b$.

   We show σ_g is onto. For this, it suffices to show that if $b \in A$, there exists $a \in A$ such that $\sigma_g(a) = b$. Observe that $\sigma_g(g^{-1}(b)) = g \cdot (g^{-1}(b)) = (gg^{-1}) \cdot b = e \cdot b = b$, using Axiom 1 and Axiom 2 for the right-most two equalities. Let $a = g^{-1} \cdot b$, and observe that $\sigma_g(a) = b$.