M621 Quiz 1 "quiz-like problems": Problem set 1

1. Let a and b be positive integers, and let $X = \{sa + tb : sa + tb > 0 \text{ and} \{s, t\} \subseteq \mathbb{Z}\}$. Let $d = \min\{c : c \in X\}$, the minimum (or "least") element in X.

   Prove that $d|a$. Suggestion. Use the Division Theorem: There exists $q, r \in \mathbb{Z}$ such that $a = dq + r$, where $0 \leq r < d$. Show r must be 0.

2. Let n be a positive integer. Define a binary relation $\equiv_n$ on $\mathbb{Z}$ as follows: For $s, t \in \mathbb{Z}$, $s \equiv_n t$ if $n|s - t$.
   (a) Show that $\equiv_n$ is an equivalence relation.
   (b) Show that $a \equiv_n b$ and $c \in \mathbb{Z}$ implies that $a + c \equiv_n b + c$, and $ca \equiv_n cb$.

3. Find two different partitions $\mathcal{P}_\infty$ and $\mathcal{P}_\in$ of $\mathbb{Z}$ so that $\mathcal{P}_\rangle$ (for i = 1,2), we have
   (a) $\mathcal{P}_\rangle$ partitions $\mathbb{Z}$ into two disjoint subsets A and B having $0 \in A$, $1 \in B$, and
   (b) $\mathcal{P}_\rangle$ is compatible with multiplication.

4. Let G be a group, and let $g \in G$. Recall that order of g, denoted $|g|$, is

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

   (a) Using the definition given above, prove that if $|g| = n \in \mathbb{N}$, then $\{e, g, \ldots, g^{n-1}\}$ consist of n distinct elements of G.
   (b) Suppose $|g| = \infty$. Show that for any integers $j, k \in \mathbb{Z}$, $g^j = g^k$ if and only if $j = k$.
   (c) Using the definition of order given above, prove that for any $h \in G$, $|hgh^{-1}| = |g|$.
   (d) Prove that if $\{g^k : k \in \mathbb{N}\}$ is a finite subset of G, then $|g|$ is finite. Suggestion: Use the Pigeonhole Principle, then use the cancellation property of groups, and finish by using the definition of order.

5. Let $G = (G, *)$ and $K = (K, \circ)$ be groups. Recall that a function $\Gamma : G \to K$ is a homomorphism of groups if it is compatible with the operations—that is, for all $y, z \in G$, $\Gamma(y * z) = \Gamma(y) \circ \Gamma(z)$.
   (a) Show that $\Gamma(e_G) = e_K$.
   (b) Show that for all $g \in G$, $\Gamma(g^{-1}) = (\Gamma(g))^{-1}$.
   (c) Suppose $g \in G$, and $|g| = n \in \mathbb{N}$. Show that $|g| \geq |\Gamma(g)|$.

(d) Recall that we use "$Y \leq Z$" to indicate that Y is a subgroup of a group Z.

Suppose $H \leq G$. Prove that $\Gamma(H) \leq K$.

(e) Suppose $A \leq K$. Prove that $\Gamma^{-1}(A) \leq G$.

(f) Prove that $ker(\Gamma) \leq G$.

(g) Suppose $\Gamma : G \to K$ is an isomorphism of groups. Since Γ is an isomorphism, it is a bijection, and since it is bijection, it has an inverse, $\Gamma^{-1} : K \to G$, a function that satisfies $\Gamma^{-1} \circ \Gamma = id_G$ and $\Gamma \circ \Gamma^{-1} = id_K$. (To denote the identity function on a set U, I sometimes use "id_U".)

Prove that $\Gamma^{-1} : K \to G$ is an isomorphism. (You just need to show that Γ^{-1} is compatible with the operations on G and K.)

(h) Show that if $\Gamma : G \to K$ is an isomorphism. Using (iii.) and (vii.), show that for all $g \in G$, $|g| = |\Gamma(g)|$.

6. Let G be a group, and let A be a set. Suppose G acts on A. That is, the following are satisfied.

Axiom 0: For all $g \in G$, all $a \in A$, $g \cdot a \in A$.

Axiom 1: For all $g, h \in G$, all $a \in A$, $(gh) \cdot a = g \cdot (h \cdot a)$.

Axiom 2: For all $a \in A$, $e \cdot a = a$.

For $g \in G$, let $\sigma_g : A \to A$ be defined as follows: For all $a \in A$, $\sigma_g(a) = g \cdot a$.

(a) Prove the following using the above axioms.

i. For all $g \in G$, σ_g is a permutation of A.

ii. Let $\sigma : G \to S_A$ be defined as follows: For all $g \in G$, $\sigma(g) = \sigma_g$. Prove that σ is a homomorphism.

(b) Let $G = D_8$, and let $B = \{\{1,3\},\{2,4\}\}$.

i. Explain why for all $g \in G$, $g(B) = B$. (That is, show that $g(\{1,3\} \in B$ and $g(\{2,4\}) \in B$.)

ii. From (b)i., it follows that G acts on B—no need to prove that formally.

Let $\sigma : G \to S_2$, where $\sigma(g) = \sigma_g$, the action of g on B. As you proved above, $\sigma : G \to S_2$ is a homomorphism. **Determine** $ker(\sigma)$, listing the elements of D_8 in cycle notation.

(c) Let D_8 act on the set $C = \{\{i,j\} : 4 \geq j > i \geq 1\}$, the set of all six 2-element subsets of $\{1,2,3,4\}$, under the following action: For all $g \in D_8$, and $\{i,j\} \in C$, $g \cdot \{i,j\} := \{g(i), g(j)\}$.

It is not difficult to see that the above is an action of D_8 on C—you are not asked to prove that. Answer the following.

i. Determine the kernel of the above action (i.e., determine $ker(\sigma)$, where $\sigma : D_8 \to S_6$).

ii. Explain why σ is **not** an onto map.

7. Let $n \in \mathbb{N}$ with $n \geq 2$. Let $\beta \in S_n$.

   (a) Prove that $\beta(12)\beta^{-1} = (\beta(1)\beta(2))$.

   (b) Suppose $\{a_1, \ldots, a_k\}$ are $k \leq n$ distinct elements of $\{1, \ldots, n\}$. Prove for any $\beta \in S_n$ that $\beta(a_1 \ldots a_k)\beta^{-1} = (\beta(a_1)\beta(a_2) \ldots \beta(a_k))$.

   (c) Let G be a group. Suppose that H and K are both subgroups of G. Show that $H \cap K$ is a subgroup of G.

   Now suppose we have a possibly infinite collection of subgroups of G indexed by a set I, $\{H_i : H_i \leq G, \text{ for all } i \in I\}$. Show that $\cap_{i \in I} H_i$ is a subgroup of G.

   (d) Let G be a group. Suppose that H and K are both subgroups of G. Show that $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.

   (e) Let A, B be groups, and let $G = A \times B$. (We showed that G is a group with identity (e_A, e_B).)

   i. Let $\pi_1 : A \times B \to A$ be defined as follows: For all $(a, b) \in A \times B$, $\pi_1(a, b) = a$. Show that π_1 is a homomorphism, and describe $ker(\pi_1)$.

   ii. Find a one-to-one homomorphism $\iota : A \to A \times B$. Define ι in a clear way, and show it is a homomorphism, and explain why it is one-to-one.