MATH 1530 Problem Set 3

Tanish Makadia
(Collaborated with Esmé, Marcos, Edward, and Kazuya)

February 2023

Problem 1. Please complete the mid-semester survey. Write "I have completed the mid-semester survey" and sign your name.

Problem 2. Let a be an element of a group G. Prove that $\langle a^m \rangle \cap \langle a^n \rangle$ is cyclic, where n, m are integers. What is its generator?

Proof. Let $a^k \in \langle a^m \rangle \cap \langle a^n \rangle$. We have that $a^k \in \langle a^m \rangle \implies a^k = a^{ms}$ where $s \in \mathbb{Z}$. We also have that $a^k \in \langle a^n \rangle \implies a^k = a^{nt}$ where $t \in \mathbb{Z}$. Together, we have

$$a^k = a^{ms} = a^{nt} \implies k = ms = nt$$

In other words, k must be a common multiple of both m and n. Since every common multiple of m and n is itself a multiple of $\mathrm{lcm}(m, n)$, we have that $\langle a^m \rangle \cap \langle a^n \rangle$ is equal to $\{(a^{\mathrm{lcm}(m,n)})^c \mid c \in \mathbb{Z}\} = \langle a^{\mathrm{lcm}(m,n)} \rangle$. $\square$

Problem 3. Let a and b belong to a group. If $|a|$ and $|b|$ are relatively prime, prove that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Proof. Let G be a group containing elements a, b. Let $m = |a|$ and $n = |b|$. We can now express $\langle a \rangle$ and $\langle b \rangle$ as:

$$\langle a \rangle = \{e, a^1, \ldots, a^{m-1}\} \qquad\qquad \langle b \rangle = \{e, b^1, \ldots, a^{n-1}\}$$

Because the identity element of G is unique, we have that $e \in \langle a \rangle \cap \langle b \rangle$.

Next, we will show that for all $a^k \in \langle a \rangle$ such that $a^k \neq e$, we have that $a^k \notin \langle b \rangle$. By (Gallian, 4.2 Corollary 1), we know that if $a^k \in \langle a \rangle$, then $|a^k|$ divides m. Additionally, since $a^k \neq e$, we know $|a^k| > 1$. If $a^k \in \langle b \rangle$, $|a^k|$ must divide n. But since $|a|$ and $|b|$ are relatively prime, we have that $\gcd(m, n) = 1$. Because $|a^k| \neq 1$, we have shown that $a^k \notin \langle b \rangle$. The same process can be used to show that for all $b^k \in \langle b \rangle$ such that $b^k \neq e$, we have that $b^k \notin \langle a \rangle$.

Therefore, we have proven that $\langle a \rangle \cap \langle b \rangle = \{e\}$. $\square$

Problem 4. Let G be an Abelian group of order 77, and assume that for all $x \in G$, we have that $x^{77} = e$. Prove that G is cyclic.

Proof. For all $x \in G$, we have $x^{77} = e$ which implies that $|x|$ divides 77. Thus, for all $x \in G$, we have that $|x| \in \{1, 7, 11, 77\}$. To prove that G is cyclic, we must show that G has an element of order 77.

Suppose that every element of G besides $e \in G$ has order 7. Because G is closed, it must contain every cyclic subgroup generated by these elements. For all $x \in G$, we have $|x| = |\langle x \rangle|$ and $e \in \langle x \rangle$. This implies that each cyclic subgroup generated by an element of order 7 contains 6 distinct non-identity elements. Thus, the number of distinct elements in G is $|G| = 77 = 1 + 6n$ where $n \in \mathbb{Z}$. This is a contradiction since $6 \nmid 76$.

Alternatively, suppose every element of G besides $e \in G$ has order 11. We have that each cyclic subgroup generated by an element of order 11 contains 10 distinct non-identity elements. In this case, $|G| = 77 = 1 + 10n$ where $n \in \mathbb{Z}$. This is also a contradiction since $10 \nmid 76$.

We are therefore left with the following cases:

- **Case 1 (G has an element of order 7 and order 11):** Let $a, b \in G$ such that $|a| = 7$ and $|b| = 11$. Thus, $a^{77} = a^7 = e$ and $b^{77} = b^{11} = e$. This implies that $(ab)^{77} = a^{77}b^{77} = e^2 = e$. Hence, we have that $|ab|$ divides 77, giving us the following four cases:
  - **Case 1 ($|ab| = 1$):** This implies $ab = e$ which is a contradiction since a and b do not have the same order.
  - **Case 2 ($|ab| = 7$):** This implies $e = (ab)^7 = a^7b^7 = e \cdot b^7 = b^7$. This is a contradiction since $|b| = 11$.
  - **Case 3 ($|ab| = 11$):** This implies $e = (ab)^{11} = a^{11}b^{11} = a^{11} \cdot e = a^{11}$. This is a contradiction since $7 \nmid 11$.
  - **Case 4 ($|ab| = 77$):** By process of elimination, we have that $|ab| = 77$.
- **Case 2 (G has an element of order 77):** We have that G can be generated by this element and we are done.

Since both cases lead to the existence of an element of order 77 in G, we have proven that G is cyclic. $\square$