MATH 1530 Problem Set 4

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.

I have completed the mid-semester survey -Tanish Makadia

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. Let $K = \{k \mid k = ms = nt\}$ and let $L = \{b \cdot \mathrm{lcm}(m, n) \mid b \in \mathbb{Z}\}$. We will now prove that $K = L$.

Of course, $\mathrm{lcm}(m, n) = ms = nt$ for some $s, t \in \mathbb{Z}$. Thus, for all $b \in \mathbb{Z}$, we have that $b \cdot \mathrm{lcm}(m, n) = msb = ntb \implies b \cdot \mathrm{lcm}(m, n) = ms' = nt'$ where $s', t' \in \mathbb{Z}$. Therefore, $L \subset K$.

For contradiction, suppose $\mathrm{lcm}(m, n) \nmid k$. This implies that

$$k = b \cdot \mathrm{lcm}(m, n) + r \qquad \text{such that } b \in \mathbb{Z} \text{ and } 0 < r < \mathrm{lcm}(m, n)$$

From this relation, we have that $r = k - b \cdot \mathrm{lcm}(m, n)$. We have that m and n both divide k and $b \cdot \mathrm{lcm}(m, n)$. Thus, m and n both divide r, which means r is a common multiple of m and n. This is a contradiction because we had that $r < \mathrm{lcm}(m, n)$. Therefore, for all common multiples k, we have that $\mathrm{lcm}(m, n) \mid k \implies k = b \cdot \mathrm{lcm}(m, n)$. We can conclude that $K \subset L$, completing the double inclusion.

Since $K = L$, $\langle a^m \rangle \cap \langle a^n \rangle = \{a^k \mid k = ms = nt\} = \{(a^{\mathrm{lcm}(m,n)})^b \mid b \in \mathbb{Z}\} = \langle a^{\mathrm{lcm}(m,n)} \rangle$. $\square$

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:

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

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.

By (Gallian, 4.4), we have that $\phi(7) = 6$ divides the number of elements of order 7 in G. Thus, the non-identity elements of G cannot all be of order 7 since $6 \nmid 76$. For the same reason, the non-identity elements of G cannot all be of order 11 either since $\phi(11) = 10 \nmid 76$.

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. $\square$

Let G be a group, and suppose G has two distinct elements of order 2.

1. Prove that G is not cyclic.

Proof. Suppose G is cyclic. Since G has an element of order 2, we have that 2 divides $|G|$. By (Gallian, 4.3), G must have exactly one subgroup of order 2. However, G has two distinct elements of order 2 which implies that G has two distinct subgroups of order 2. This is a contradiction. Therefore, G is not cyclic. $\square$

2. Prove that $U(2^n)$ is not cyclic for $n \geq 3$.

Proof. We will show that $U(2^n)$ contains two distinct elements of order 2.

First, we will prove that $2^n - 1,\ 2^{n-1} - 1 \in U(2^n)$.

- $2^n - 1 \in U(2^n)$: Since the linear combination $2^n - (2^n - 1)$ equals 1, we have that $2^n - 1$ and 2^n are relatively prime.
- $2^{n-1} - 1 \in U(2^n)$: Consider the prime factorizations of 2^n and $2^{n-1} - 1$. Of course, $2^n = 2 \cdots 2$. Let $2^{n-1} - 1 = p_1 \cdots p_m$ where p_i is a prime number. Since 2^{n-1} is even, it must be the case that $2^{n-1} - 1$ is odd. Therefore, $p_1, \ldots, p_m$ are odd. Because the product of even numbers is always even, all divisors of 2^n besides 1 must be even. Additionally, since the product of odd numbers is always odd, all divisors of $2^{n-1} - 1$ must be odd. Therefore, we have that $\mathrm{gcd}(2^n,\ 2^{n-1} - 1) = 1$ which means 2^n and $2^{n-1} - 1$ are relatively prime.

Now, we will show that $|2^n - 1| = |2^{n-1} - 1| = 2$.

$$\begin{aligned}(2^n - 1)^2 &= (2^{2n} - 2(2^n) + 1) \bmod 2^n \\ &= (2^n(2^n - 2) + 1) \bmod 2^n \\ &= 1 = e\end{aligned}$$

$$\begin{aligned}(2^{n-1} - 1)^2 &= (2^{2n-2} - 2(2^{n-1}) + 1) \bmod 2^n \\ &= (2^n(2^{n-2} - 1) + 1) \bmod 2^n \\ &= 1 = e\end{aligned}$$

Therefore, we have that $|2^n - 1| = |2^{n-1} - 1| = 2$. Since two distinct elements of order 2 exist in $U(2^n)$, by (1), we have proven that $U(2^n)$ is not cyclic for $n \geq 3$. $\square$