

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

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

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

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 $\text{lcm}(m, n)$, we have that $\langle \mathbf{a}^m \rangle \cap \langle \mathbf{a}^n \rangle$ is equal to $\langle \mathbf{a}^{\text{lcm}(m, n)} \rangle$. □

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

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

$$\langle \mathbf{a} \rangle = \{\mathbf{e}, \mathbf{a}^1, \dots, \mathbf{a}^{\mathbf{m}-1}\} \quad \langle \mathbf{b} \rangle = \{\mathbf{e}, \mathbf{b}^1, \dots, \mathbf{a}^{\mathbf{n}-1}\}$$

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

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

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