# MTH 4441 Test #1 - Solutions

Fall 2023

Pat Rossi Name ______________________

1. **Define: Group**

   A nonempty set $G$ together with a binary operation $*$ on $G$ form a **group**, denoted $(G, *)$, exactly when the following four "group axioms" hold:

- $G$ is "closed under $*$."
- $*$ is associative
- $\exists\ e \in G$ such that $e * x = x = x * e$, $\forall x \in G$

  We call $e$ the **identity element**
- $\forall x \in G$, $\exists\ y \in G$ such that $x * y = e$ and $y * x = e$

  We call $y$ the **inverse** of $x$

2. **Define: Binary operation**

   Given a non-empty set $S$, a **binary operation** $*$ on the set $S$ is a rule that assigns an element $x_3$ to each ordered pair $(x_1, x_2)$ of elements in $S$ .The assignment is made in this manner:

   $$x_1 * x_2 = x_3$$

3. **Define:** Integers $a$ and $b$ **congruent modulo** $n$.

   Let $n \geq 2$ be a natural number. Then integers $a$ and $b$ are **congruent modulo** $n$, denoted $a \equiv b \,(\mathrm{mod}\, n)$, exactly when $a - b = kn$, for some integer $k$. (i.e., $a \equiv b \,(\mathrm{mod}\, n)$ exactly when $a - b$ is a multiple of $n$.) Otherwise, $a$ and $b$ are **incongruent modulo** $n$, denoted $a \not\equiv b \ (\mathrm{mod}\, n)$.

4. Give an alternate characterization of **congruence modulo** $n$.

   Let $n \geq 2$ be a natural number. Then integers $a$ and $b$ are **congruent modulo** $n$, denoted $a \equiv b \,(\mathrm{mod}\, n)$, exactly when $a$ and $b$ have the same "proper remainder" (i.e., $r \in \{0, 1, 2, \ldots, n-1\}$) when divided by $n$. Otherwise, $a$ and $b$ are **incongruent modulo** $n$, denoted $a \not\equiv b \ (\mathrm{mod}\, n)$.

5. **Define:** $(\mathbb{Z}_n, \oplus)$ (the **additive group of integers modulo** $n$)

   Let $n \geq 2$ and let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. The **additive group of integers modulo** $n$, is the group $(\mathbb{Z}_n, \oplus)$ in which $\oplus$ is addition modulo $n$.

6. **Define:** $(U_n, \odot)$ (the **multiplicative group of integers modulo** $n$)

   Let $n$ be a prime natural number and let $U_n = \{1, 2, \ldots, n-1\}$. The **multiplicative group of integers modulo** $n$ is the group $(U_n, \odot)$ in which $\odot$ is multiplication modulo $n$.

7. **Prove:** If $(G, *)$ is a group, and $a, b$ are any elements of $G$, then $(a * b)^{-1} = b^{-1} * a^{-1}$

   **pf/** Observe that:

   $(a * b) * (b^{-1} * a^{-1}) = a * (b * (b^{-1} * a^{-1})) = a * ((b * b^{-1}) * a^{-1}) = a * (e * a^{-1}) = a * a^{-1} = e$

   i.e., $(a * b) * (b^{-1} * a^{-1}) = e$,

   Hence, $(b^{-1} * a^{-1}) = (a * b)^{-1}$ ■

8. **Define:** The **order of an element** $x$ of a group $(G, *)$ (In your definition, specify either **additive** or **multiplicative** notation.)

   Given a group $(G, *)$, and an element $x \in G$, the **order** of the element $x$, denoted $o(x)$, is the least $n \in \mathbb{N}$ such that $nx = 0$. (Additive notation) If no such $n$ exists, then $o(x) = \infty$.

   Given a group $(G, *)$, and an element $x \in G$, the **order** of the element $x$, denoted $o(x)$, is the least $n \in \mathbb{N}$ such that $x^n = 1$. (Multiplicative notation) If no such $n$ exists, then $o(x) = \infty$.

9. **Prove:** The inverse of an element $x$ in a group $(G, *)$ is unique.

   **Remark:** We will show that an element $x$ has a unique inverse by assuming that $x$ has (at least) two inverses elements in the group and showing that they must be one, and the same element.

   **pf/** Suppose that $x$ has (at least) two inverses, $y$ and $z$ in $G$.

   Then $xy = e$ and $yx = e$ (because $y$ is an inverse of x)

   Also: $xz = e$ and $zx = e$ (because $z$ is an inverse of x)

   **Observe:** $y = ye = y(xz) = (yx)z = ez = z$

   i.e., $y = z$ ■

10. Construct the group table for $(U_7, \odot)$

In $(U_7, \odot)$, the operation $\odot$ is multiplication modulo 7

| $\odot$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

11. In the previous exercise, determine the order of the element 3

With **multiplicative** notation, the order of an element $g \in G$ is the least natural number $n$ such that $g^n = e$ (the identity).

In the context of the group $(U_7, \odot)$, the order of an element $g \in U_7$ is the least natural number $n$ such that $g^n = 1$ (the identity).

**Observe:**

$3^1 = 3 \quad$ i.e., $3^1 = 3$

$3^2 = 9 \equiv 2 \pmod 7 \quad$ i.e., $3^2 = 2$

$3^3 = 3 \cdot 3^2 \equiv 3 \cdot 2 \pmod 7 \equiv 6 \pmod 7 \quad$ i.e., $3^3 = 6$

$3^4 = 3 \cdot 3^3 \equiv 3 \cdot 6 \pmod 7 \equiv 4 \pmod 7 \quad$ i.e., $3^4 = 4$

$3^5 = 3 \cdot 3^4 \equiv 3 \cdot 4 \pmod 7 \equiv 12 \pmod 7 \equiv 5 \pmod 7 \quad$ i.e., $3^5 = 5$

$3^6 = 3 \cdot 3^5 \equiv 3 \cdot 5 \pmod 7 \equiv 15 \pmod 7 \equiv 1 \pmod 7 \quad$ i.e., $3^6 = 1$

The least natural number $n$ such that $3^n = 1$ is 6.

Thus, $o(3) = 6$

12. Construct the group table for $(\mathbb{Z}_5, \oplus)$

In $(\mathbb{Z}_5, \oplus)$, the operation $\oplus$ is addition modulo 5

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

| $\oplus$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

13. In the previous exercise, determine the order of the element 4

The operator in the group is additive.

Therefore, $o(4)$ is the least natural number $n$ such that $n4 \equiv 0 \,(\text{mod})\, 5$

(i.e., the least natural number $n$ such that $n4$ is congruent to the identity)

$1 \cdot 4 = 4 \equiv 4 \,(\text{mod})\, 5$

$2 \cdot 4 = 8 \equiv 3 \,(\text{mod})\, 5$

$3 \cdot 4 = 12 \equiv 2 \,(\text{mod})\, 5$

$4 \cdot 4 = 16 \equiv 1 \,(\text{mod})\, 5$

$5 \cdot 4 = 20 \equiv 0 \,(\text{mod})\, 5$

$\boxed{o(4) = 5}$

14. Define what it means for a binary operation $*$ to be associative.

A binary operation $*$ on a set $S$ is said to be **associative** exactly when $x_1 * (x_2 * x_3) = (x_1 * x_2) * x_3$, $\forall x_1, x_2, x_3 \in S$

15. Determine whether the operation $*$, given by $a * b = ab + ba$ is an associative binary operation on the set $\mathbb{R}$.

**Observe:**

$$(a * b) * c = (a * b)\,c + c\,(a * b) = (ab + ba)\,c + c\,(ab + ba)$$

$$= \underbrace{abc + bac + cab + cba = abc + abc + abc + abc}_{\text{Because Multiplication of Real Numbers is commutative}} = 4abc$$

**Also:**

$$a * (b * c) = a\,(b * c) + (b * c)\,a = a\,(bc + cb) + (bc + cb)\,a$$

$$= \underbrace{abc + acb + bca + cba = abc + abc + abc + abc}_{\text{Because Multiplication of Real Numbers is commutative}} = 4abc$$

$(a * b) * c = 4abc = a * (b * c)$

i.e., $(a * b) * c = a * (b * c)$.

Hence, $*$ is associative on $\mathbb{R}$.

16. Fill out the group table below:

| * | e | a | b | c |
|---|---|---|---|---|
| e | | | | |
| a | | | | |
| b | | | | |
| c | | | | |

There are a number of possibilities. Here are a few:

| * | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | c | e | a |
| c | c | e | a | b |

| * | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | c | e | b |
| b | b | e | c | a |
| c | c | b | a | e |

| * | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | a | e |
| c | c | b | e | a |

| * | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | c | e | a |
| c | c | e | a | b |

| * | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |