

# MTH 4441 Test #1

FALL 2024

Pat Rossi

Name \_\_\_\_\_

## 1. Define: Group

A non-empty 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  $a \equiv b \pmod{n}$ , exactly when  $a - b = kn$ , for some integer  $k$ . (i.e.,  $a \equiv b \pmod{n}$  exactly when  $a - b$  is a multiple of  $n$ .) Otherwise,  $a$  and  $b$  are **incongruent modulo  $n$** , denoted  $a \not\equiv b \pmod{n}$ .

## 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  $a \equiv b \pmod{n}$ , exactly when  $a$  and  $b$  have the same “proper remainder” (i.e.,  $r \in \{0, 1, 2, \dots, n - 1\}$ ) when divided by  $n$ . Otherwise,  $a$  and  $b$  are **incongruent modulo  $n$** , denoted  $a \not\equiv b \pmod{n}$ .

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

Let  $n \geq 2$  and let  $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$ . 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  $U_n = \{1, 2, \dots, n-1\}$ . 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:

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

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

$$\text{Hence, } (b^{-1} * a^{-1}) = (a * b)^{-1} \quad \blacksquare$$

8. **Define:** The **order of an element  $x$**  of a group  $(G, *)$  (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 identity element  $e$  in a group  $(G, *)$  is unique.

**Remark:** We will show that the identity element is unique by assuming that there are (at least) two identity elements in the group and showing that these must be the same element.

**pf/** Suppose that there are two identity elements,  $e$  and  $e_1$  in  $G$ .

**Observe:**  $e = e * e_1$  (because  $e_1$  is an identity)

**Also:**  $e * e_1 = e_1$  (because  $e$  is an identity)

$$\Rightarrow e = e * e_1 = e_1$$

i.e.,  $e = e_1$   $\blacksquare$

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

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

$$U_7 = \{1, 2, 3, 4, 5, 6\}$$

$\odot$	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 2

The operator in the group is multiplicative.

Therefore,  $o(2)$  is the least natural number  $n$  such that  $2^n \equiv 1 \pmod{7}$

(i.e., the least natural number  $n$  such that  $2^n$  is congruent to the identity)

$$2^1 = 2 \equiv 2 \pmod{7}$$

$$2^2 = 4 \equiv 4 \pmod{7}$$

$$2^3 = 8 \equiv 1 \pmod{7}$$

$o(2) = 3$
------------

12. Construct the group table for  $(\mathbb{Z}_6, \oplus)$

In  $(\mathbb{Z}_6, \oplus)$ , the operation  $\oplus$  is addition modulo 6

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

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  $n4 \equiv 0 \pmod{6}$

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

$$1 \cdot 4 = 4 \equiv 4 \pmod{6}$$

$$2 \cdot 4 = 8 \equiv 2 \pmod{6}$$

$$3 \cdot 4 = 12 \equiv 0 \pmod{6}$$

$o(4) = 3$
------------

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

A binary operation  $*$  on a non-empty set  $S$  is a binary operation that has the property that  $\forall a, b, c \in S$ ,

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

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

**Observe:**  $*$ , as defined above, IS a binary operation on  $\mathbb{R}$ . For all  $a, b \in \mathbb{R}$ ,  $a * b = ab + b \in \mathbb{R}$  also.

(i.e.,  $\forall a, b \in \mathbb{R}$ ,  $*$  assigns the real number  $ab + b$  to the ordered pair  $(a, b)$ .)

Is  $*$  an **associative** binary operation on  $\mathbb{R}$ ?

**Observe:**  $(a * b) * c = (a * b)c + c = (ab + b)c + c = abc + bc + c$

**Also:**  $a * (b * c) = a(b * c) + (b * c) = a(bc + c) + (bc + c) = abc + ac + bc + c$

It appears that  $(a * b) * c = abc + bc + c \neq abc + ac + bc + c = a * (b * c)$

To prove this conclusively, we exhibit a counter-example:

Consider  $a = 1, b = 1, c = 2$

$$(a * b) * c = abc + bc + c = 1 \cdot 1 \cdot 2 + 1 \cdot 2 + 2 = 6$$

$$a * (b * c) = abc + ac + bc + c = 1 \cdot 1 \cdot 2 + 1 \cdot 2 + 1 \cdot 2 + 2 = 8$$

Thus, for  $a = 1, b = 1, c = 2$ ,  $(a * b) * c \neq a * (b * c)$

Thus,  $*$  is NOT associative.

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

**Remark:** We will show that the inverse of the element  $x$  in the group  $(G, *)$  is unique by assuming that there are two inverses of  $x$  and then showing that they must be one, and the same, element.

**pf/** Let  $y$  and  $z$  be inverses of  $x$ .

Then  $x * y = e = y * x$  (because  $y$  is an inverse of  $x$ ).

Also:  $x * z = e = z * x$  (because  $z$  is an inverse of  $x$ ).

**Observe:**  $y = y * e = y * (x * z) = (y * x) * z = e * z = z$

i.e.,  $y = z$

Hence, the inverse of an element  $x$  is unique. ■