MTH 4441 Test #1

FALL 2022

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., $r \in \{0, 1, 2, \ldots, n-1\}$) 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 $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. 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 $(G, *)$ (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., $e = e_1$ ■

10. Construct the group table for $(U_5, \odot)$

In $(U_5, \odot)$, the operation $\odot$ is multiplication modulo 5

$U_5 = \{1, 2, 3, 4\}$

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

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

The operator in the group is multiplicative.

Therefore, $o(3)$ is the least natural number n such that $3^n \equiv 1 \pmod 5$

(i.e., the least natural number n such that 3^n is congruent to the identity)

$3^1 = 3 \equiv 3 \pmod 5$

$3^2 = 9 \equiv 4 \pmod 5$

$3^3 = 27 \equiv 2 \pmod 5$

$3^4 = 81 \equiv 1 \pmod 5$

$$\boxed{o(3) = 4}$$

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)

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

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

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

    $\boxed{o(4) = 3}$

14. Determine whether the operation $*$, given by $a * b = ab^2$ is an associative binary operation on the set $\mathbb{R}$.

    Observe: $*$, as defined above, IS a binary operation on $\mathbb{R}$. For all $a, b \in \mathbb{R}$, $ab^2 \in \mathbb{R}$ also.

    (i.e., $\forall\, a, b \in \mathbb{R}$, $*$ assigns the real number ab^2 to the ordered pair (a, b).)

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

    Observe: $(a * b) * c = (ab^2) * c = ab^2c^2$

    Also: $a * (b * c) = a * (bc^2) = a\left(bc^2\right)^2 = ab^2c^4$

    It appears that $(a * b) * c = ab^2c^2 \neq ab^2c^4 = a * (b * c)$

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

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

    $(a * b) * c = ab^2c^2 = 1 \cdot 1^2 \cdot 2^2 = 4$

    $a * (b * c) = ab^2c^4 = 1 \cdot 1^2 \cdot 2^4 = 16$

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

    Thus, $*$ is NOT associative.

15. 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