MTH 4441 – Definitions, Theorems, and Proofs to Know for Test #1

Fall 2023

Pat Rossi Name ______________________________

Part #1 Definitions and Theorems

1. 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:

   $$x_1 * x_2 = x_3$$

2. Define what it means for a binary operation to be **closed** on a set S.

   A binary operation $*$ on the set S is said to be **closed** on S exactly when $*$ assigns an element $x_3 \in S$ to each ordered pair (x_1, x_2) of elements in S . (i.e., the element x_3, assigned to each ordered pair (x_1, x_2) of elements in S, is also an element of S.)

3. Define what it means for a binary operation to be **commutative.**

   A binary operation $*$ on S is said to be **commutative** exactly when $x_1 * x_2 = x_2 * x_1$ $\forall x_1, x_2 \in S$

   elements in S, is also an element of S.)

4. 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 $x_1 * (x_2 * x_3) = (x_1 * x_2) * x_3$ $\forall x_1, x_2, x_3 \in S$

5. 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

6. Define **abelian group**

   A group in which $*$ is commutative is called an **abelian groups.**

7. **Thm -** The identity element e in a group $(G, *)$ is unique.

8. **Thm -** The inverse of an element x in a group $(G, *)$ is unique.

9. **Thm -** The group $(G, *)$ is commutative exactly when the group table is symmetric about the main diagonal.

10. **Thm -** Given a group $(G, *)$, the the group table for $(G, *)$ is such that every element of G appears exactly once in each row and in each column of the table

11. **Thm -** If $(G, *)$ is a group, then the left and right cancellation laws hold.

    i.e., if $a, b, c \in G$, then:

    $a * b = a * c \Rightarrow b = c$ (left cancellation law)

    and

    $b * a = c * a \Rightarrow b = c$ (right cancellation law)

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

13. Define **congruent (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 $a - b = kn$, 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 $a \not\equiv b \pmod{n}$.

14. **(Alternative Definition)** Define **congruent (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 $a \not\equiv b \pmod{n}$.

15. Define **greatest common divisor**

    Given integers a and b, not both equal to zero, the **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is the largest natural number that is a factor of both a and b.

16. Define **zero divisor**

    Suppose that $a, b \in \mathbb{Z}$ with $a \not\equiv 0 \pmod{n}$ and $b \not\equiv 0 \pmod{n}$. Suppose further, that $a * b \equiv 0 \pmod{n}$.Then a and b are said to be **zero divisors** modulo n.

17. Define 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.

18. **Thm -** For $n \in \mathbb{N}$, where n is NOT prime, $(U_n, \odot) = (\{1, 2, \ldots, n-1\}, \odot)$ is NOT a group. The elements of $\{1, 2, \ldots, n-1\}$ that are zero divisors modulo n are exactly those elements of U_n that are not relatively prime with respect to n .

19. Define 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.

20. Define the **order of a group** $(G, *)$

    The **order** of a group $(G, *)$, denoted $|G|$, is the number of elements in the group. If $(G, *)$ is infinite, then $|G| = \infty$.

21. Define the **order of an element** of a group $(G, *)$

    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 $o(x) = \infty$.

Part #2 - Proofs to Know

22. **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., $e = e_1$ ■

23. **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., $y = z$ ■

24. **Prove:** If $(G, *)$ is a group, then the left and right cancellation laws hold.

i.e., if $a, b, c \in G$, then:

$a * b = a * c \Rightarrow b = c$ (left cancellation law)

and

$b * a = c * a \Rightarrow b = c$ (right cancellation law)

pf/ Suppose that $(G, *)$ is a group, and that $a, b, c \in G$.

Then a has an inverse, a^{-1}

Thus, given $a * b = a * c$, we have:

$a^{-1} * (a * b) = a^{-1} * (a * c) \Rightarrow \left(a^{-1} * a\right) * b = \left(a^{-1} * a\right) * c \Rightarrow e * b = e * c \Rightarrow b = c$

i.e., $a * b = a * c \Rightarrow b = c$

Similarly, given $b * a = c * a$, we have:

$(b * a) * a^{-1} = (c * a) * a^{-1} \Rightarrow b * \left(a * a^{-1}\right) = c * \left(a * a^{-1}\right) \Rightarrow b * e = c * e \Rightarrow b = c$

i.e., $b * a = c * a \Rightarrow b = c$ ■

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

(i.e., the inverse of a product is the product of the inverses **- in reverse order!**)

pf/ Observe that:

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

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

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