MTH 4441 Homework #4

Due: Monday, September 20, 2021

Pat Rossi Name ____________________

Synopsis of Groups and Modulo Arithmetic

Def - The non empty set G together with a binary operation * form a **group**, denoted $(G, *)$, exactly when the following four "group axioms" hold:

- G is "closed under * " (Actually, this *must* be true in order for * to be a binary operation).

- * is associative

- $\exists\ e \in S$ such that $e * x = x = x * e$, $\forall x \in G$

  We call e the **identity element**

- $\forall x \in G$, $\exists\ y \in S$ such that $x * y = e$ and $y * x = e$

  We call y the inverse of x

Def - Groups in which * is commutative are called **Abelian Groups.**

Thm - The identity element of a group is unique

Thm - Given $x \in (G, *)$, The inverse of x is unique

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

Thm - If $(G, *)$ is a group, then the table that defines the group is such that every element of G appears exactly once in each row and in each column of the table

Def - The Left Cancellation Law: $a * b = a * c \Rightarrow b = c$

The Right Cancellation Law: $b * a = c * a \Rightarrow b = c$

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

Thm - If $(G, *)$ is a group, and a, b are any elements of G, then the linear equations $a * x = b$ and $y * a = b$ have unique solutions in G.

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

Thm - (The Division Algorithm) Given a natural number $n \geq 2$, and an integer a, the division algorithm gives us:

$$a = qn + r \qquad \text{where } 0 \leq r < n$$

The possible values for r are: $0, 1, 2, 3, \ldots, n-1$. These values of r are called the **remainders of a modulo n.**

Def - Let $n \geq 2$ be a natural number. Two integers a and b are congruent modulo n, denoted $a \equiv b \pmod{n}$, exactly when $a - b = kn$, for some integer, k. Otherwise, a is incongruent to b modulo n, denoted $a \not\equiv b \pmod{n}$.

Alternative Definition - Let $n \geq 2$ be a natural number. For arbitrary integers a and b, $a \equiv b \pmod{n}$ iff a and b have the same remainder (by division algorithm) when divided by n.

Theorem 1 *Let $n \geq 2$ be fixed. Then for arbitrary integers:*

- $a \equiv a \pmod{n}$
- *If* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$
- *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$
- *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$
- *If* $a \equiv b \pmod{n}$ *then* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$
- *If* $a \equiv b \pmod{n}$ *then* $a^k \equiv b^k \pmod{n}$

Def - Given $a, b \in \mathbb{Z}$, 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.

Def - Given $a, b \in \mathbb{Z}$, a and b are said to be **relatively prime** exactly when $\gcd(a, b) = 1$

Thm - If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$. (i.e., If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then the cancellation laws hold.)

Homework Exercises

1. Let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, and let $(\mathbb{Z}_6, \oplus)$ be a group, where $\oplus$ is addition modulo 6. Construct the group table.

   Remark: The group $(\mathbb{Z}_6, \oplus)$ is called the **additive group of integers modulo 6.**

   Remark: In general, given $n \geq 2$, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, and the group $(\mathbb{Z}_n, \oplus)$ is called the **additive group of integers modulo n.** **(**$\oplus$ is addition modulo n.)

2. Construct the group table for $(\mathbb{Z}_7, \oplus)$.

3. Let $U_5 = \{1, 2, 3, 4\}$, and let $(U_5, \odot)$ be a group, where $\odot$ is multiplication modulo 5. Construct the group table.

   Remark: The group $(U_5, \odot)$ is called the **multiplicative group of integers modulo 5.**

   Remark: In general, given $n \geq 2$, $U_n = \{1, \ldots, n-1\}$, and the group $(U_n, \odot)$ is called the **multiplicative group of integers modulo n.** **(**$\odot$ is multiplication modulo n.)

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

4. Construct the group table for $(U_3, \odot)$.

   In $(U_3, \odot)$, the operation $\odot$ is multiplication modulo 3

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

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

6. Construct the group table for $(U_6, \odot)$.

   In $(U_6, \odot)$, the operation $\odot$ is multiplication modulo 6

   (a) Is $(U_6, \odot)$ actually a group? Why or why not?

   (b) Does the equation $2x = 3$ have a solution in $(U_6, \odot)$? If not, what do you perceive the problem to be?

7. Construct the group table for $(U_4, \odot)$.

   In $(U_4, \odot)$, the operation $\odot$ is multiplication modulo 4

   (a) Is $(U_4, \odot)$ actually a group? Why or why not?

   (b) Does the equation $2x = 3$ have a solution in $(U_4, \odot)$? If not, what do you perceive the problem to be?

   (c) Under what conditions is $(U_n, \odot)$ a group? (Formulate a hypothesis.)

8. Determine whether the table below defines a group for $G = \{a, b, c\}$. (State why or why not.)

*	a	b	c
a	a	b	c
b	b	a	c
c	c	b	a

9. Determine whether the table below defines a group for $G = \{a, b, c\}$. (State why or why not.)

*	a	b	c
a	a	b	c
b	b	b	c
c	c	c	c