

# MTH 4441 Homework #4 - Solutions

DUE: MONDAY, SEPTEMBER 20, 2021

Pat Rossi

Name \_\_\_\_\_

## 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  $n \geq 2$ ,  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ , and the group  $(\mathbb{Z}_n, \oplus)$  is called the **additive group of integers modulo n**. ( $\oplus$  is addition modulo n.)

$\oplus$	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

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

$\oplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

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  $n \geq 2$ ,  $U_n = \{1, \dots, n-1\}$ , 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

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

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

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

$\odot$	1	2
1	1	2
2	2	1

5. 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

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

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

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

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

$(U_6, \odot)$  is NOT a group

There are a few things that disqualify  $(U_6, \odot)$  from being a group

1.  $U_6$  is not closed under  $\odot$ . For example:  $2 \odot 3 = 0$
2. None of the elements of  $U_6$  appear at least once in every row and in every column. For example, 1 does not appear in the row headed by 2
3. The elements 2, 3, 4 appear more than once in some rows and columns. For example, 3 appears three times in the row and the column headed by 3.
4. The elements 2, 3, 4 do not have an inverse. This can be seen by the fact that the identity 1 does not appear in the rows and the columns that are headed by 2, 3, and 4.

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

The equation  $2x = 3$  does NOT have a solution in  $(U_6, \odot)$ . This is shown by the fact that the element 3 does not appear in the row headed by the element 2.

This is symptomatic of the fact that 2 does not have an inverse in  $U_6$  and that  $U_6$  is not closed under  $\odot$ .

If 2 DID have an inverse (let's denote it as  $2^{-1}$ ), then we could multiply both sides of the equation  $2 \odot x = 3$  by  $2^{-1}$ .

$$\text{This would yield: } 2^{-1} \odot (2 \odot x) = 2^{-1} \odot 3 \Rightarrow (2^{-1} \odot 2) \odot x = 2^{-1} \odot 3$$

$$\Rightarrow 1 \odot x = 2^{-1} \odot 3 \Rightarrow x = 2^{-1} \odot 3.$$

Provided that  $U_6$  is closed under  $\odot$ ,  $x = 2^{-1} \odot 3$  would be an element of  $U_6$

Thus,  $x = 2^{-1} \odot 3$  would be the solution to the equation  $2 \odot x = 3$

To verify that  $x = 2^{-1} \odot 3$  is the solution of the equation  $2 \odot x = 3$ , observe:

$$2 \odot x = 2 \odot (2^{-1} \odot 3) = (2 \odot 2^{-1}) \odot 3 = 1 \odot 3 = 3$$

i.e.,  $2 \odot x = 3$

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

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

$\odot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

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

$(U_4, \odot)$  is NOT a group

There are a few things that disqualify  $(U_4, \odot)$  from being a group

1.  $U_4$  is not closed under  $\odot$ . For example:  $2 \odot 2 = 0$
2. The elements 1 and 3 of  $U_4$  do NOT appear at least once in every row and in every column. The elements 1 and 3 do not appear in the row or the column headed by 2.
3. The elements 2 appears more than once in the row and column headed by 2.
4. The elements 2 does not have an inverse. This can be seen by the fact that the identity 1 does not appear in the row and the column that are headed by 2.

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

The  $2x = 3$  does NOT have a solution in  $(U_4, \odot)$ , as is seen from the fact that 3 does not appear in the row headed by 2.

Again, this is symptomatic of the fact that 2 does not have an inverse in  $U_4$  and that  $U_4$  is not closed under  $\odot$ .

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

From the examples that we've seen, it would be reasonable to hypothesize that  $(U_n, \odot)$  is a group exactly when  $n$  is prime.

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

Since the elements  $b$  and  $c$  each appear more than once in a column, the table does NOT define a group

Clearly,  $a$  is the identity. Therefore, there should not exist another element  $x$  such that  $x * c = c$ . And yet,  $b * c = c$

Similarly, the element  $c$  is such that  $c * b = b$

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

This table does NOT define  $(G, *)$  as a group.

1. The elements  $b$  and  $c$  appear more than once in the rows and columns headed by  $b$  and  $c$ .
2. The identity 1 does not appear in any row or column headed by  $b$  or  $c$ , which indicates that neither  $b$  nor  $c$  has an inverse.