MAT 108: Problem Set 5

Solutions

Due 2/14/23 at 11:59 pm on Canvas

Reminders:

- **No Monday 1-2 office hours with Dr. Zhang on 2/13.** TA office hours on 2/13 and Thursday, 2/16 office hours are as usual.
- Your homework submission must be typed up in full sentences, with proper mathematical formatting. Handwritten homework submissions will receive a score of 0. Solutions containing incomplete sentences or poor formatting will lose points.
- You will receive feedback on PS4 by next Tuesday, 2/14. PS4 revisions are due Friday, 2/17 at 11:59 pm. Underneath your old solution, type

  ```
  \revisedsolution
  ```

  and then type your revised solution.

Exercise 1

Consider the set $\mathbb{Z}/7\mathbb{Z}$, equipped with the operations addition $(+)$ and multiplication $(\cdot)$. We also have division, defined as a function

$$\text{division} : \mathbb{Z}/7\mathbb{Z} \times (\mathbb{Z}/7\mathbb{Z} - \{[0]\}) \to \mathbb{Z}/7\mathbb{Z},$$

which you will be able to define by $(x, y) \mapsto xy^{-1}$ after you've completed part (a) below.

Remark. For readability reasons, we will stop using the notation $[x]$ to represent the equivalence class of $x \in \mathbb{Z}$ under the "mod 7" relation. In real life, mathematicians just write "2" for $[2] \in \mathbb{Z}/7\mathbb{Z}$ if the context is clear.

(a) For each of the elements of $\mathbb{Z}/7\mathbb{Z} - \{0\}$, determine its inverse. (Fill in the table provided.)

(b) Fill in the addition table provided below.

(c) Fill in the multiplication table provided below.

(d) An element $m \in \mathbb{Z}$ is called a *square* if there exists some $n \in \mathbb{Z}$ such that $n \cdot n = m$. We can make the same definition in $\mathbb{Z}/7\mathbb{Z}$. Which elements of $\mathbb{Z}/7\mathbb{Z} - \{0\}$ are *squares*? (Fill in the chart below.)

(0 is indeed a square, but it's extra special, so we consider it separately.)

Remark. Just to be clear, this is an exploration problem. You don't need to write any proofs; just work out the calculations and fill in the tables below!

SOLUTION.

(a)

Element of $\mathbb{Z}/7\mathbb{Z} - \{0\}$	Inverse element
1	1
2	4
3	5
4	2
5	3
6	6

(b)

	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

(c)

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(d)

Squares:	1,2,4
Non-squares:	3,5,6

Exercise 2

Let $x, y \in \mathbb{R}_{>0}$. Show that if $x < y$, then $0 < \frac{1}{y} < \frac{1}{x}$.

Remark. Remember that you have many properties and axioms to use from Sections 8.1 and 8.2. We didn't explicitly cover them in class if they come from axioms that $\mathbb{Z}$ also satisfied; in that case, the proofs for $\mathbb{Z}$ and for $\mathbb{R}$ are identical.

SOLUTION.

Let $x, y \in \mathbb{R}_{>0}$ and suppose that $x < y$. First, note that

$$x \cdot \frac{1}{x} = 1 = y \cdot \frac{1}{y}$$

by the definition of multiplicative inverses. Since $y > x$, we then have

$$y \cdot \frac{1}{x} > x \cdot \frac{1}{x} = y \cdot \frac{1}{y},$$

i.e.

$$y \cdot \frac{1}{x} > y \cdot \frac{1}{y}.$$

By Proposition 8.37.(ii), since $y > 0$, we now have

$$\frac{1}{x} > \frac{1}{y}.$$

It remains to show that $\frac{1}{y} > 0$. To show this, we will use Proposition 8.36, which states:

If $a, c \in \mathbb{R}_{>0}$ and $b \in \mathbb{R}$, then if $ab = c$, then $b \in \mathbb{R}_{>0}$.

Let $a = y, b = \frac{1}{y}$, and $c = 1$. Since $y, 1 \in \mathbb{R}_{>0}$, we have that $\frac{1}{y} \in \mathbb{R}_{>0}$ as well.

Putting the two inequalities together, we arrive at

$$\frac{1}{x} > \frac{1}{y} > 0.$$

Exercise 3

In class, we talked about upper bounds (Section 8.4). In this problem, you will prove some analogous facts for lower bounds.

(a) Let $B \subseteq \mathbb{R}$ be a nonempty subset. Give a precise definition for the *infimum* $\inf(B)$ of B, i.e. the *greatest lower bound* for B.

(b) Give a definition for $\min(B)$, the *smallest element* of B. (Note that in class we only defined this function for subsets of $\mathbb{Z}$; your definition should be very similar.) Then, prove the following analogue to Proposition 8.49:

Proposition. Let $A \subseteq \mathbb{R}$ be nonempty. If $\inf(A) \in A$, then $\inf(A) = \min(A)$. Conversely, if A has a smallest element, then $\min(A) = \inf(A)$ and $\inf(A) \in A$.

Solution.

Remark. Note that in this solution, I use the the term *the infimum*, implying that it is unique. We will see / have seen in class that suprema are unique; the proof of uniqueness is similar for infima.

(a)

Definition. Let $B \subseteq \mathbb{R}$ be a nonempty subset. If there exists an $a \in \mathbb{R}$ such that for all lower bounds a' for B, $a \geq a'$, then we call a the *infimum* of B, denoted $\inf(B)$.

(b)

Definition. Let B be a nonempty subset of $\mathbb{R}$. If there exists $a \in$ such that for all $b \in B$, $a \leq b$, then $a = \min(B)$.

We now prove the proposition. Let $A \subseteq \mathbb{R}$ be a nonempty subset.

First, suppose $\inf(A)$ exists and is an element of A. By definition, $\inf(A)$ is the greatest lower bound for A. In particular, $\inf(A)$ is *a lower bound* for A, i.e. for all $a \in A$, $\inf(A) \leq a$. Since $\inf(A) \in A$ also, by our definition of $\min(A)$ above, $\inf(A) = \min(A)$.

Now we show the converse. Suppose A has a smallest element called $\min(A) \in A$. It suffices to show that $\min(A)$ is also $\inf(A)$, since this implies that $\inf(A) = \min(A) \in A$. To show this, we need to show that, for any lower bound b of A, $b \leq \min(A)$, as this is our definition of the infimum. But since for all $a \in A$, $b \leq a$, in particular $\min(A) \in A$, so $b \leq a$ indeed. Therefore $\min(A) = \inf(A) \in A$.