MAT 108 PS05

Melissa Zhang

Due Monday, May 4, 2026 at 9:00 pm on Gradescope

Instructions

There are three goals for this problem set:

- Maintain good mathematical writing form in your justifications even when you aren't explicitly asked to prove a given statement.
- Practice working with equivalence relations and equivalence classes.
- Gain familiarity with common examples of equivalence classes that inherit algebraic structure ("quotient rings"), such as $\mathbb{Z}/n\mathbb{Z}$.
- Understand better when and how to check "well-definedness".

Here are some reminders about best practices:

- You absolutely must write in full, connected English sentences. Whenever possible, do not start a sentence with mathematical symbols. Do not use symbols like $\Rightarrow$, $\forall$, $\exists$, $\therefore$, etc. (except when explicitly discussing statements about logic).
- Your solution must be *neat*. You **will** be graded on style, which includes mathematical style and professionalism.
- It is your responsibility to mark where your solutions for each problem begins on Gradescope so that the TA and reader can properly grade your solutions.

Exercise 1

(Not graded) Do you know the difference between the symbols $\in$ and $\subseteq$? Explain to yourself what the follow statements mean:

- $a \in P \in S$
- $a \in P \subset S$
- $A \subset P \in S$

Exercise 2

For each of the following relations, determine whether it is an equivalence relation. If it is, determine the equivalence classes.

(a) On $\mathbb{Z}$, $x \sim y$ if $xy > 0$.

(b) On $\mathbb{Z} - \{0\}$, $x \sim y$ if $x|y$ or $y|x$.

(c) On $\mathbb{Z}$, $x \sim y$ if $x = y$ or $x = -y$.

Exercise 3

For a moment, pretend we have already introduced the real numbers $\mathbb{R}$ that we work with all the time in calculus. Prove that the following are equivalence relations, and describe the equivalence classes geometrically.

(a) On the plane $\mathbb{R} \times \mathbb{R}$, define $(x, y) \sim (v, w)$ if $x^2 + y^2 = v^2 + w^2$.

(b) On the *punctured* plane $\mathbb{R} \times \mathbb{R} - \{0, 0\}$, define $(x, y) \sim (v, w)$ if there exists a nonzero $r \in \mathbb{R}$ such that $(v, w) = (rx, ry)$.

Exercise 4

Prove that the multiplication operation

$$\begin{aligned} \cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ ([a], [b]) &\mapsto [a \cdot b] \end{aligned}$$

on $\mathbb{Z}/n\mathbb{Z}$ is well-defined.

Exercise 5

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

$$\begin{aligned} \text{division} : \mathbb{Z}/7\mathbb{Z} \times (\mathbb{Z}/7\mathbb{Z} - \{[0]\}) &\to \mathbb{Z}/7\mathbb{Z} \\ (x, y) &\mapsto x \cdot y^{-1} \end{aligned}$$

which you will be able to define 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 (multiplicative) 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.)

This is an exploration problem. You don't need to write any proofs; just work out the calculations and fill in the tables like the ones below:

(a)

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

(b)

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

(c)

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

(d)

Squares:	
Non-squares:	

Exercise 6

Recall that $\mathbb{Z}[x]$ denotes the set of polynomials in the indeterminate variable x with coefficients in the integers. (Also recall from precalculus that polynomial addition and multiplication are both commutative and associative, and satisfy the distributive property. There's no need to mention these terms in your solution to this exercise.)

We define divisibility of polynomials similarly to how we defined it for integers:

Definition. For polynomials $f(x), p(x) \in \mathbb{Z}[x]$, we say $p(x)$ divides $f(x)$, and write $p(x) \mid f(x)$, if there exists some $q(x) \in \mathbb{Z}[x]$ such that $f(x) = p(x)q(x)$.

We wish to define an algebraic object called $\mathbb{Z}[x]/(p(x))$ as the equivalence classes of the following equivalence relation:

$$f(x) \sim g(x) \qquad \text{if} \qquad p(x) \mid (f(x) - g(x)).$$

(a) Prove that $\sim$ is an equivalence relation.

(b) For $p(x) = x^2$, determine the set of equivalence classes. Use set notation to explicitly write down each equivalence class.

(c) There are *induced* addition and multiplication operations on $\mathbb{Z}[x]/(p(x))$; this means that the definition is inherited from addition in $\mathbb{Z}[x]$. Write down these two binary operations (as in Exercise 4). (No proof needed here.)

(d) Prove that addition and multiplication are both well-defined.