MATH 540 HONORS LINEAR ALGEBRA SUMMER 2021, Melody Chan
PROBLEM SET B

Due Monday May 24 at 11:59pm Eastern

Submit all of the following on Gradescope, and don't forget to tag each answer to its page. We have implemented a course policy whereby failing to tag results in half credit. I put a copy of this problem set in the Overleaf folder too.

1. (2 points) Read the Introductions in the Discussions page on Canvas. Leave some responses.
2. (2 points) Fill in the following table of powers of 2 in $\mathbb{F}_{13}$. I've started it for you.[1]

n	0	1	2	3	4	5	6	7	8	9	10	11
2^n	1	2	4									

3. (6 points) In this problem, you'll fill out a proof from Review Sheet B. Let $f\colon \mathbb{R}^2 \to \mathbb{R}^3$ be defined by
$$(x, y) \mapsto (x, x + y, y).$$
   (a) Write down, from the definition of injectivity and preferably using universal quantifiers, the statement that f is injective.[2] Write down, preferably using universal quantifiers, the statement that f is *not* injective. Now prove the correct statement (the first one).[3]
   (b) Write down, using universal quantifiers, the statement that f is surjective. Write down, using universal quantifiers, the statement that f is *not* surjective. Now prove the correct statement (the second one).

Continued on the next page

[1] Notice how the nonzero elements of $\mathbb{F}_{13}$ appear, once each, all scrambled up in the bottom row of the table. In this situation, 2 is called a *primitive element* of $\mathbb{F}_{13}$. The problem of "unscrambling" the bottom row is known as the *discrete logarithm problem* and is understood to be computationally hard. The hardness of this unscrambling problem forms the basis for some public-key cryptography schemes, e.g., *Diffie-Hellman key exchange*, in which two people can establish a shared secret while communicating entirely in public. You can look all of this up online. It is amazing!

[2] Hint: it could begin with *For all…*

[3] A possibly silly-sounding but useful observation: given $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{R}$, when is it the case that
$$(a_1, \dots, a_n) = (b_1, \dots, b_n)?$$
The answer is: exactly when $a_1 = b_1, \dots, a_n = b_n$. In other words, two ordered n-tuples are equal exactly when they are equal coordinatewise.

4. (2 points, an interesting example to hopefully stretch your mind) Let X be any set.

   Let V be the set of all subsets of X. Sometimes V is also called the *power set* of X.[4]

   Define an addition operation on V by defining the sum of two subsets to be their *symmetric difference*:

$$A + B = A \triangle B \qquad \text{for subsets } A, B \subseteq X.$$

   Define a scalar multiplication operation on V, with scalars $\mathbb{F}_2 = \{0, 1\}$, by defining

$$0 \cdot A = \emptyset, \qquad 1 \cdot A = A$$

   for any subset A of X.

   Check that V is a vector space over $\mathbb{F}_2$. That is, check that the six properties of a vector space listed on p. 12 of Axler's textbook hold.

[4] For example, if $X = \{1, 2, 3\}$, then V has eight elements:

$$V = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$