Math 24, Winter 2020, Pset 1

This problem set is due at the start of lecture on Wednesday January 15.

1. In this exercise, F is a field and V is a vector space over F. Prove the following statements. Justify each step in your proof.

   (a) $(a+b)(x+y) = ax+ay+bx+by$ for all $a, b \in F, x, y \in V$.

   (b) If $cx = \mathbf{0}$ for some scalar $c \in F$ and vector $x \in V$, then either $c = 0$ or $x = \mathbf{0}$. (The zero vector is denoted $\mathbf{0} \in V$, while the zero scalar is $0 \in F$.)

   (c) Assume that F is one of the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Then $v + v = 2v$.

2. (a) Let V be the set

   $$V = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{C} \text{ for } i = 1, 2 \ldots, n\}$$

   By example 1 in section 1.2, V is a vector space over $\mathbb{C}$. Is V a vector space over $\mathbb{R}$ with operations of coordinatewise addition and multiplication?

   (b) Let V be the set

   $$V = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{R} \text{ for } i = 1, 2 \ldots, n\}$$

   By example 1 in section 1.2, V is a vector space over $\mathbb{R}$. Is V a vector space over $\mathbb{C}$ with operations of coordinatewise addition and multiplication?

3. If m, n, p are integers we say that m is congruent to n modulo p (denoted $m \equiv n \bmod p$) if the difference $m - n$ is divisible by p.

   Suppose $p \geq 2$ and consider the set

   $$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$$

   Elements of $\mathbb{F}_p$ can be added as follows: The sum of two elements $a, b \in \mathbb{F}_p$ is defined to be the unique element $c \in \mathbb{F}_p$ such that $a + b \equiv c \bmod p$. Subtraction and multiplication of elements in $\mathbb{F}_p$ (but not division!) are defined similarly.

   For example, in $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ we have

   - $3+2 = 2+3 = 5$, $2 \times 3 = 3 \times 2 = 6$, $3-2 = 1$, $2-3 = 6$;
   - $4+6 = 6+4 = 3$, $4 \times 6 = 6 \times 4 = 3$, $4-6 = 5$, $6-4 = 2$, .

   It is easy to check that addition and multiplication in $\mathbb{F}_p$ are commutative, associative, and distributive. We have $a + 0 = a$ and $1 \times a = a$ in $\mathbb{F}_p$. It turns out that if p is a *prime number* then $\mathbb{F}_p$ is a *field*. To see this we need to verify that we can *divide* by any element other than zero.

   Proposition 1 *For all $a, b \in \mathbb{F}_p$, if $a \neq 0$ there exists a unique $c \in \mathbb{F}_p$ such that $ac = b$ in $\mathbb{F}_p$.*

(a) For all $a, b, c \in \mathbb{F}_p$ with $a \neq 0$, prove that if $ab = ac$ in $\mathbb{F}_p$ then $b = c$.

Hint. Recall that positive integers have a unique prime factorization. In particular, if xy is divisible by p then either x is divisible by p or y is divisible by p.

(b) If $a \neq 0$ in $\mathbb{F}_p$, explain why no two elements in the set

$$\{a \times 0, a \times 1, \cdots, a \times (p-1)\}$$

are congruent modulo p.

(c) Prove the existence of the element $c \in \mathbb{F}_p$ in Proposition 1.

(d) Prove the uniqueness of the element $c \in \mathbb{F}_p$ in Proposition 1.

4. Give an example of two elements $a, b \in \mathbb{F}_4$ with $a \neq 0$ such that there does not exist c with $ac = b$ in $\mathbb{F}_4$. (In other words, $\mathbb{F}_4$ is *not* a field.)

5. Let $V = F^3$ be the vector space of example 1 in section 1.2 for the finite field $F = \mathbb{F}_5$. In this vector space, calculate:

   (a) With $c = 3 \in \mathbb{F}_5$ and $x = (1, 3, 2) \in V$, what is cx?

   (b) With $x = (1, 3, 2) \in V$ and $y = (0, 4, 3) \in V$, what is $x + y$?

   (c) What is the additive inverse of the vector $x = (0, 1, 3)$ (as in axiom VS4)?

6. Give an example of a subspace $W \subset V$ of the vector space $V = F^2$ over the field $F = \mathbb{F}_7$ that is not $W = \{0\}$ or $W = V$. How many vectors are there in W?