Homework Assignment 1
Assigned Fri 1/16. Due Fri 1/23.

On Style: Homework solutions must be written in complete sentences, legibly with adequate spacing and margins, or will be returned without further evaluation. Mathematical writing should respect all the rules of grammatical English. As with riding a bicycle, ballroom dancing, or any sport, say, your skill in communicating your ideas improves only with practice and discipline.

1. Suppose $F$ (with binary operations $+$, ·) is some field, and assume all quantities referenced in this problem are elements of $F$. Do this problem using only the basic field axioms.
   (a) Show that the multiplicative identity 1 (i.e., $1_F$) is unique. [To help get started, your solution could start “Suppose some element $\hat{1} \in F$ is a multiplicative identity. This means that $\hat{1} \alpha = \alpha$ for all $\alpha \in F$.” Then prove $\hat{1} = 1$.]
   (b) (cf. Curtis (2.13)) Prove: Whenever $\alpha, \beta \in F$ and $\alpha \neq 0$, the equation $\alpha x = \beta$ has a unique solution $x \in F$. [Note there are two things to prove: (i) some solution exists, and (ii) there is only one.]
   (c) Show that $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$, provided $b, d \neq 0$. [We define $\frac{a}{b} = a \cdot b^{-1}$, where $b^{-1}$ is the (unique) multiplicative inverse of $b$.]

2. Let $p$ be prime, and $F = \{0, 1, \ldots, p - 1\}$. Define + and · to be addition and multiplication (respectively) modulo $p$. (E.g., if the ordinary product $\alpha \beta = k p + \gamma$ where $k \in \mathbb{Z}$ and $\gamma \in F$, then $\alpha \cdot \beta$ is defined as $\gamma$.) Prove that whenever $\beta \in F$ is nonzero, the map $\alpha \mapsto \alpha \beta$ is injective (one-to-one). Using this result, deduce that each nonzero element of $F$ has a multiplicative inverse. (This is field axiom 7. Axioms 1–6 are easy to verify. Hence $F$ is a field, usually denoted $\mathbb{Z}_p$.)

3. Let $F$ be a field, and let $F^2$ be the set of all ordered pairs $(\alpha, \beta)$ of elements of $F$.
   (a) If $F = \mathbb{Z}_3$ and addition and multiplication are defined by
   $$(\alpha, \beta) + (\gamma, \delta) = (\alpha + \gamma, \beta + \delta), \quad (\alpha, \beta)(\gamma, \delta) = (\alpha \gamma - \beta \delta, \alpha \delta + \beta \gamma),$$
   prove $F^2$ is a field. $\square$
   (b) In the previous part, if $\mathbb{Z}_3$ is replaced by $\mathbb{Z}_5$, show that the given addition and multiplication rules do not make $F^2$ a field.

4. For this question, $F = \mathbb{R}$, $V \subseteq \mathbb{R}^2$ is the specified subset, and addition and scalar multiplication are defined as the respective operation for $\mathbb{R}^2$.
   (a) Let $V = \{(x_2^2) \mid x_1, x_2 \in \mathbb{R}, x_2 = x_1^2\}$. Is $V$ a vector space? Justify.
   (b) Let $f : \mathbb{R} \to \mathbb{R}$ be a function. $V = \{(x_1^2) \mid x_1, x_2 \in \mathbb{R}, x_2 = f(x_1)\}$. Show that $V$ is a vector space, if and only if $\exists \alpha \in \mathbb{R}$, such that $f(x) = \alpha x$ for all $x \in \mathbb{R}$.

Continued on next page

---

1I’ll grant you the axioms of commutativity and associativity. But prove the other 5!
5. Let $F$ be a field. Define $P(F)$ to be the set of all polynomials over $F$. That is, $P(F)$ is the set of all functions $f : F \to F$ such that there exist $n \in \mathbb{N}_0 = \{0, 1, \ldots\}$ and $a_0, \ldots, a_n \in F$ for which

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \quad \text{for all } x \in F. \quad (*)$$

Define vector addition, and scalar multiplication as we did for functions; e.g., $f + g$ is the function such that for all $x \in F$, $(f + g)(x) = f(x) + g(x)$.

(a) Show that $P(F)$ is a vector space.

(b) For this part, suppose $F = \mathbb{R}$ or $F = \mathbb{C}$. Show that if $f \in P(F)$ and $f \neq 0$, then $f$ has a unique representation as in $(*)$ with $a_n \neq 0$. In this case $n$ is called the degree of the polynomial $f$. [Note: What you have to prove here is to suppose $f(x) = \sum_{i=0}^{m} a_i x^i = \sum_{i=0}^{n} b_i x^i$, with $a_m, b_n \neq 0$, and show that this necessarily implies $m = n$, and $a_i = b_i$ for all $i$.]

(c) Show that the uniqueness in the previous part may be false if we don’t assume $F = \mathbb{R}$ or $F = \mathbb{C}$.

(d) Let $F = \mathbb{R}$ or $F = \mathbb{C}$. Given $n \in \mathbb{N}$, let $U_n$ be all elements of $P(F)$ with degree exactly $n$. With addition and scalar multiplication defined as in $P(F)$, is $U_n$ a vector space? Provide a proof, or counter example.

(e) Let $F = \mathbb{R}$ or $F = \mathbb{C}$, and let $P_n(F)$ be all elements of $P(F)$ with degree less than or equal to $n$. Is $P_n(F)$ a vector space? Provide a proof, or counter example.

Writing mathematics well:

- Make your response self-contained. State assumptions, explain notation, describe the goal, and indicate the strategy — whether the proof uses induction, contradiction, or contraposition, say. Note that written mathematics consists of complete sentences conforming to English grammar!

- Identify your audience. Effective communication is aimed at a target audience. You want to include enough detail to convince the instructor that you understand the material, but not bore with trivial detail (unless it’s essential for the point of the problem, ugh). It’s tricky to find the right balance. One way to target your writing is to aim at a student in class a week ago, say, who hasn’t seen this problem.

- Aim at clarity — don’t turn in a first draft. Mathematics is difficult enough. Reduce the burden on your reader by reading your first draft critically and revising it. My method of writing research papers is: 1. Write. 2. Read. 3. Tear up. 4. Repeat until clear (usually at least 5 times, unfortunately).