

Oxford A0 - Linear Algebra

Dan Davison

November 9, 2017

Sheet 1

1. (a) Prove that $\mathbb{F}_p = \{0, 1, \dots, p-1\}$, the set of equivalence classes of integers modulo a prime p , satisfies the axioms of a field. How many elements are there in a vector space of dimension n over the field \mathbb{F}_p ?

Let¹ $a, b, c \in \mathbb{Z}$ with $0 \leq a < p$, $0 \leq b < p$, $0 \leq c < p$.

Let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{F}$ be equivalence classes of integers modulo p .

The field axioms are listed below, together with proof that they hold for \mathbb{F}_p .

1. **\mathbb{F}_p is an abelian group under addition**

Define $\bar{a} + \bar{b} := \overline{a + b}$, then:

(a) *Existence of identity:* $\bar{0}$ is the identity since $\bar{a} + \bar{0} = \overline{a + 0} = \bar{a}$ for all $\bar{a} \in \mathbb{F}_p$.

(b) *Existence of inverses:* $(\bar{a})^{-1} = \overline{-a}$ since $\bar{a} + \overline{-a} = \overline{a + -a} = \bar{0}$ for all $a \in \mathbb{F}_p$.

(c) *Commutativity:* $\bar{a} + \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} + \bar{a}$ for all $a, b \in \mathbb{F}_p$.

(d) *Associativity:* $\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{b + c} = \overline{a + b + c} = \overline{a + b} + \bar{c} = (\bar{a} + \bar{b}) + \bar{c}$.

2. **$\mathbb{F}_p \setminus \{\bar{0}\}$ is an abelian group under multiplication**

Define $\bar{a} \bar{b} := \overline{ab}$, then:

(a) *Existence of identity:* $\bar{1}$ is the identity since $\bar{a} \bar{1} = \overline{a \cdot 1} = \bar{a}$ for all $\bar{a} \in \mathbb{F}_p$.

<https://courses.maths.ox.ac.uk/node/5353>

¹Unlike the question, I am trying to use notation that distinguishes between integers and their equivalence classes.

(b) *Existence of inverses for everything except additive identity:*

The claim is that for all $\bar{a} \in \mathbb{F}_p \setminus \{\bar{0}\}$ there exists $\bar{b} \in \mathbb{F}_p$ such that $\bar{a} \bar{b} = \bar{1}$.

Fix an arbitrary $a \in \{1, \dots, p-1\}$.

The claim is equivalent to the following: there exists $b \in \{0, 1, \dots, p\}$ such that for all $i, j \in \mathbb{Z}$ there exists $k \in \mathbb{Z}$ such that $(ip + a)(jp + b) = kp + 1$.

But note that $(ip + a)(jp + b) = p(ijp + aj + bi) + ab$ and therefore

$$\begin{aligned} (ip + a)(jp + b) &= kp + 1 \\ \iff ab &= p(k - ijp - aj - bi) + 1. \end{aligned}$$

Since k can be chosen freely, the condition is simply that for all $i, j \in \mathbb{Z}$ there exists $k \in \mathbb{Z}$ such that $ab = kp + 1$.

Note² that a and p are coprime (gcd is 1). By Bezout's identity, there exists $b, -k \in \mathbb{Z}$ such that

$$ba + (-k)p = 1 \iff ab = kp + 1. \quad \square$$

(c) *Commutativity:* $\bar{a} \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \bar{a}$ for all $a, b \in \mathbb{F}_p$.

(d) *Associativity:* $\bar{a}(\bar{b}\bar{c}) = \bar{a} + \overline{bc} = \overline{abc} = \overline{ab} \bar{c} = (\bar{a} \bar{b})\bar{c}$.

3. Distributive axiom

(a) *Multiplication distributes over addition:* $\bar{a}(\bar{b} + \bar{c}) = \bar{a}(\overline{b+c}) = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \bar{a} \bar{b} + \bar{a} \bar{c}$

There are p^n elements in a vector space of dimension n over the field \mathbb{F}_p .

²I eventually allowed myself to google for a hint here which brought up people pointing to Bezout's identity.

(b) Determine all subspaces of $(\mathbb{F}_2)^3$.

Remark: This is like the 8 vectors that form the unit cube in \mathbb{R}^3 , except that when extended beyond the cube by vector addition or scalar multiplication they “wrap around”.

Note that

$$\begin{aligned}
 (\mathbb{F}_2)^3 &= \{\bar{0}, \bar{1}\}^3 \\
 &= \{(\bar{0}, \bar{0}, \bar{0}), \\
 &\quad (\bar{0}, \bar{0}, \bar{1}), \\
 &\quad (\bar{0}, \bar{1}, \bar{0}), \\
 &\quad (\bar{0}, \bar{1}, \bar{1}), \\
 &\quad (\bar{1}, \bar{0}, \bar{0}), \\
 &\quad (\bar{1}, \bar{0}, \bar{1}), \\
 &\quad (\bar{1}, \bar{1}, \bar{0}), \\
 &\quad (\bar{1}, \bar{1}, \bar{1})\}.
 \end{aligned}$$

The set of subspaces of $(\mathbb{F}_2)^3$ is

$$\begin{aligned}
 &\{(\bar{0}, \bar{0}, \bar{0})\} && \cup \\
 &\{(\bar{0}, \bar{0}, \bar{0}), x \mid x \in (\mathbb{F}_2)^3\} && \cup \\
 &\{(\bar{0}, a, b) \mid a, b \in \mathbb{F}_2\} && \cup \\
 &\{(a, \bar{0}, b) \mid a, b \in \mathbb{F}_2\} && \cup \\
 &\{(a, b, \bar{0}) \mid a, b \in \mathbb{F}_2\} && \cup \\
 &\{(\mathbb{F}_2)^3\}.
 \end{aligned}$$

2. Show that the vector space of polynomials $\mathbb{R}[x]$ is isomorphic to a proper subspace of itself.

We need to:

1. **Exhibit a proper subspace $S[x] \subset \mathbb{R}[x]$ and a bijection $f : \mathbb{R}[x] \rightarrow S[x]$**

Let $a_i \in \mathbb{R}$ for $i = 0, 1, 2, \dots$ so that $\mathbb{R}[x] = \{a_0 + a_1x^1 + a_2x^2 + \dots\}$.

Define $S[x] = \{0 + a_1x^1 + a_2x^2 + a_3x^3 + \dots\}$, i.e. the restriction of $\mathbb{R}[x]$ to those polynomials that have constant term zero.

$S[x]$ is a proper subspace of $\mathbb{R}[x]$ since it contains the zero polynomial, and is closed under addition and scalar multiplication.

Define $f : \mathbb{R}[x] \rightarrow S[x]$ where $f(a_0 + a_1x^1 + a_2x^2 + \dots) = 0 + a_0x^1 + a_1x^2 + a_2x^3 + \dots$

f is clearly injective, since if $f(r(x)) = f(r'(x))$ then their coefficients a_0, a_1, \dots are the same and hence $r(x) = r'(x)$.

Also, f is clearly surjective since if $s(x) = a_1x^1 + a_2x^2 + a_3x^3 + \dots$ then $s(x) = f(a_0 + a_1x^1 + a_2x^2 + \dots)$.

2. **Prove that f preserves addition**

Let $a_i, b_i \in \mathbb{R}$ for $i = 0, 1, 2, \dots$

Let $r(x) = a_0 + a_1x^1 + a_2x^2 + \dots$ and $r'(x) = b_0 + b_1x^1 + b_2x^2 + \dots$

Then

$$\begin{aligned} f(r(x) + r'(x)) &= f((a_0 + b_0) + (a_1 + b_1)x^1 + (a_2 + b_2)x^2 + \dots) \\ &= 0 + (a_0 + b_0)x^1 + (a_1 + b_1)x^2 + (a_2 + b_2)x^3 + \dots \\ &= (0 + a_0x^1 + a_1x^2 + a_2x^3 + \dots) \\ &\quad + (0 + b_0x^1 + b_1x^2 + b_2x^3 + \dots) \\ &= f(r(x)) + f(r'(x)). \end{aligned}$$

3. Prove that f preserves scalar multiplication

$$\begin{aligned} f\left(\lambda r(x)\right) &= f\left(\lambda a_0 + \lambda a_1 x^1 + \lambda a_2 x^2 + \dots\right) \\ &= 0 + \lambda a_0 x^1 + \lambda a_1 x^2 + \lambda a_2 x^3 + \dots \\ &= \lambda(0 + a_0 x^1 + a_1 x^2 + a_2 x^3 + \dots) \\ &= \lambda f\left(r(x)\right) \end{aligned}$$

3. Show that the space of functions $f : \mathbb{N} \rightarrow \mathbb{R}$ does not have a countable basis.

Note:

1. The space of functions $f : \mathbb{N} \rightarrow \mathbb{R}$ is the space of real-valued infinite sequences.
2. A basis is countable iff a bijection exists between the basis and \mathbb{N} .

I haven't managed to do this. What follows is what I was thinking, but must be wrong since it contradicts the question.

Let $x_i \in \mathbb{R}$ for $i \in \mathbb{N}$ and define the following:

- $F_n := \{(x_1, x_2, \dots, x_n) \mid x_1, x_2, \dots, x_n \in \mathbb{R}\}$ is the space of functions $f : \{1, 2, \dots, n\} \rightarrow \mathbb{R}$
- $F_\infty := \{(x_1, x_2, \dots) \mid x_1, x_2, \dots \in \mathbb{R}\}$ is the space of functions $f : \mathbb{N} \rightarrow \mathbb{R}$.

Note that $F_1 = \{x_1 \mid x_1 \in \mathbb{R}\} = \mathbb{R}$. Therefore every basis for F_1 has cardinality 1 (every basis is a set containing a single non-zero real number).

Similarly, $F_2 = \mathbb{R}^2$, and every basis of F_2 has cardinality 2.

Basically it seems like the following is a basis of this space of functions, but it is countable:

$$\begin{aligned} &(1, 0, 0, \dots), \\ &(0, 1, 0, \dots), \\ &(0, 0, 1, \dots), \\ &\dots \end{aligned}$$