Oxford A0 - Linear Algebra

Dan Davison

December 3, 2017

Sheet 1

1. (a) Prove that $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, 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 $\mathbb{F}_p$?

Let[1] $a, b, c \in \mathbb{Z}$ with $0 \leq a < p, \quad 0 \leq b < p, \quad 0 \leq c < p$.

Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{F}$ 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 $\overline{a} + \overline{b} := \overline{a + b}$, then:
   (a) *Existence of identity*: $\overline{0}$ is the identity since $\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}$ for all $\overline{a} \in \mathbb{F}_p$.
   (b) *Existence of inverses*: $(\overline{a})^{-1} = \overline{-a}$ since $\overline{a} + \overline{-a} = \overline{a + -a} = \overline{0}$ for all $a \in \mathbb{F}_p$.
   (c) *Commutativity*: $\overline{a} + \overline{b} = \overline{a + b} = \overline{b} + \overline{a}$ for all $a, b \in \mathbb{F}_p$.
   (d) *Associativity*: $\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b + c} = \overline{a + b + c} = \overline{a + b} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}$.
2. **$\mathbb{F}_p \setminus \{\overline{0}\}$ is an abelian group under multiplication**
   Define $\overline{a}\ \overline{b} := \overline{ab}$, then:
   (a) *Existence of identity*: $\overline{1}$ is the identity since $\overline{a}\overline{1} = \overline{a \cdot 1} = \overline{a}$ for all $\overline{a} \in \mathbb{F}_p$.

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

[1] Unlike 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 $\overline{a} \in \mathbb{F}_p \setminus \{\overline{0}\}$ there exists $\overline{b} \in \mathbb{F}_p$ such that $\overline{a}\ \overline{b} = \overline{1}$.

Proof 1
We show that elements cannot repeat in a row/column of the group operation table, therefore something muct be the inverse.

$$\begin{aligned} a \cdot b = a \cdot c &\mod p \\ a(b-c) = 0 &\mod p \\ a = 0 \text{ or } \ b = c &\mod p \end{aligned}$$

Proof 2
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 $ab = kp + 1$.

Note[2] 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*: $\overline{a}\ \overline{b} = \overline{ab} = \overline{b}\ \overline{a}$ for all $a, b \in \mathbb{F}_p$.

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

3. **Distributive axiom**

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

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

[2] I 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

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

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

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

Per AC this is missing, at least, a subspace of size 4. Also see Sylov theorems.

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 $f : \mathbb{R}[x] \to S[x]$**

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

   Define $S[x] = \{0 + a_1x^1 + a_2x^2 + a_3x^3 + \ldots\}$, 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 $f : \mathbb{R}[x] \to S[x]$ where $f(a_0 + a_1x^1 + a_2x^2 + \ldots) = 0 + a_0x^1 + a_1x^2 + a_2x^3 + \ldots$.

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

   Also, f is clearly surjective since if $s(x) = a_1x^1 + a_2x^2 + a_3x^3 + \ldots$ then $s(x) = f(a_1 + a_2x^1 + a_3x^2 + \ldots)$.

2. **Prove that f preserves addition**

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

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

   Then

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

3. **Prove that f preserves scalar multiplication**

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

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

Note:

1. The space of functions $f : \mathbb{N} \to \mathbb{R}$ 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:

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

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:

$$\begin{array}{l}(1, 0, 0, \ldots),\\ (0, 1, 0, \ldots),\\ (0, 0, 1, \ldots),\\ \ldots\end{array}$$

I think the answer here is that E is a basis for F_∞ iff every element of F_∞ can be expressed as a linear combination of a *finite* number of elements from E. But this is untrue, at least for the basis I have suggested, since for example the constant function $f(i) = 1\ \forall i$ fails.

4. Let $\mathbb{F}$ be a field and $f(x)$ be an irreducible polynomial in $\mathbb{F}[x]$. Show that the set of polynomials modulo $f(x)$ form a field.

Let P be the set of polynomials modulo $f(x)$.

The field axioms are listed below, together with proof that they hold for P.

1. **P is an abelian group under addition**

   Define $\overline{g(x)} + \overline{h(x)} := \overline{g(x) + h(x)}$, then:

   (a) *Existence of identity*:
   The additive identity is $\overline{0} = \Big\{ f(x)g(x) \mid g(x) \in \mathbb{F}[x] \Big\}$.

   (b) *Existence of inverses*:
   $\overline{g(x)}^{\,-1} = \overline{-g(x)}$ for all $g(x) \in P$.

   (c) *Commutativity and Associativity*:
   Proofs of these are essentially the same as for $\mathbb{F}_p$ (question 1).

2. **$P \setminus \{\overline{0}\}$ is an abelian group under multiplication**

   Define $\overline{g(x)} \cdot \overline{h(x)} := \overline{g(x) \cdot h(x)}$, then:

   (a) *Existence of identity*:
   The multiplicative identity is $\overline{1} = \Big\{ f(x)g(x) + 1 \mid g(x) \in \mathbb{F}[x] \Big\}$.

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

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

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

   The claim is equivalent to the following: there exists $b \in \{0, 1, \ldots, p\}$ 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 $ab = kp + 1$.

Note[3] 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*: $\overline{a}\ \overline{b} = \overline{ab} = \overline{b}\ \overline{a}$ for all $a, b \in \mathbb{F}_p$.

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

3. **Distributive axiom**

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

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

5. (a) A non-empty subset I of a ring R is an ideal if for all $s, t \in I$ and all $r \in R$ we have

$$s - t \in I \text{ and } rt, tr \in I.$$

List all the ideals of a field $\mathbb{F}$ and of the ring $\mathbb{Z}$. Show that the kernel of any ring homomorphism is an ideal.

(b) Show that $(r+I)(r'+I) := rr' + I$ gives a well defined multiplication on the set of cosets R/I making it into a ring.

(c) Formulate the first isomorphism theorem for rings.

6. (a) Show that the set $M_n(R)$ of $(n \times n)$-matrices with entries in a ring R is a ring with the usual matrix addition and multiplication.

(b) Show that the canonical surjection $R \to R/I$ induces a surjective ring homomorphism $M_n(R) \to M_n(R/I)$. What is the kernel? Consider the example when $R = \mathbb{Z}$ and $I = 3\mathbb{Z}$.

(c) Describe the ideals of $M_n(R)$ for a ring R with multiplicative unit 1.

7. Prove that a linear transformation $P : V \to V$ of a finite dimensional vector space satisfies $P^2 = P$ if and only if there exists a basis such that the matrix of P with respect to that basis is a block matrix

$$\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

Hence determine the minimal and characteristic polynomials of P.

8. Let $T : V \to V$ be a linear transformation of a finite dimensional vector space over a field $\mathbb{F}$ to itself. Prove that T is invertible if and only if x does not divide the minimal polynomial $m_T(x)$.

9. Let $T : V \to V$ be a linear transformation of a finite dimensional vector space over a field $\mathbb{F}$ to itself. Assume that $\{v, Tv, T^2v, \dots\}$ span V for some $v \in V$. Show that

(i) there exists a k such that $v, Tv, \dots, T^{k-1}v$ are linearly independent and for some $\alpha_i \in \mathbb{F}$

$$T^k v = \alpha_0 v + \alpha_1 Tv + \cdots + \alpha_{k-1} T^{k-1} v;$$

(ii) the set $\{v, Tv, \dots, T^{k-1}v\}$ forms a basis for V;

(iii) its minimal polynomial is given by $m_T(x) = x^k - \alpha_{k-1}x^{k-1} - \cdots - \alpha_0$.

What is the characteristic polynomial $\chi_T(x)$?