

Vector spaces

1.1 Definitions

Vector spaces are sets equipped with number systems called fields. We recall the concept of a field first, before we revisit the definition and properties of a vector space.

1.1.1 Fields

Fields are algebraic structures devised to generalise familiar number systems such as the set of real numbers equipped with the standard operations of addition and multiplication, which in turn satisfy certain properties. The following definition of a field outlines the required properties in a formal way.

Definition 1.1 A **field** is a set \mathbb{F} equipped with binary operations $+$ and \cdot , which satisfies the following axioms, for all $a, b, c \in \mathbb{F}$:

FA0 Closure under addition: $a + b \in \mathbb{F}$.

FA1 Associativity of addition: $a + (b + c) = (a + b) + c$.

FA2 Existence of additive identity: there exists $o \in \mathbb{F}$ such that for all $a \in \mathbb{F}$, $a + o = a$.

FA3 Existence of additive inverses: for each $a \in \mathbb{F}$, there exists $a^- \in \mathbb{F}$ such that $a + a^- = o$.

FA4 Commutativity of addition: $a + b = b + a$.

FM0 Closure under multiplication: $a \cdot b \in \mathbb{F}$.

FM1 Associativity of multiplication: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

FM2 Existence of multiplicative identity: there exists $e \in \mathbb{F}$ such that, for all $a \in \mathbb{F}$, $a \cdot e = a$.

FM3 Existence of multiplicative inverses: for each $a \in \mathbb{F}$, $a \neq o$, there exists $a^* \in \mathbb{F}$ such that $a \cdot a^* = e$.

FM4 Commutativity of multiplication: $a \cdot b = b \cdot a$.

FD Distributivity law: $a \cdot (b + c) = a \cdot b + a \cdot c$.

We denote a generic field by $(\mathbb{F}, +, \cdot)$. We will refer to the elements of a field \mathbb{F} as **scalars**; they will be denoted by italic lower-case letters. The corresponding binary operations will be referred to as **scalar addition** and **scalar multiplication**.



Axioms FA0–FA4 indicate that $(\mathbb{F}, +)$ is an Abelian group when equipped with the addition operation, while axioms FM0–FM4 indicate that $(\mathbb{F} \setminus \{o\}, \cdot)$ is an Abelian group when equipped with the multiplication operation.



In order to verify that $(\mathbb{F}, +, \cdot)$ is a field, we need to verify the above axioms, which implies establishing the existence of additive and multiplicative identities o and e , as well as that of the additive and multiplicative inverses a^- and a^* .

Example 1.1 The fields $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$, where $+$, \cdot denote the standard addition and multiplication operations have $o = 0, e = 1$. Moreover, given $a \neq 0$, we identify $a^- = -a$ and $a^* = a^{-1}$. Finally, note that $e^- = -1$ and $e^* = 1^{-1} = 1$.

Exercise 1.1 Let $(\mathbb{F}, +, \cdot)$ be a field. Using the notation introduced in the above definition, show that

1. $a^- + a = o$;
2. $e \cdot a = a$;
3. $a^* \cdot a = e$;
4. $(a + b) \cdot c = a \cdot c + b \cdot c$.

While the most common fields employed in this course are $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$, both of which are infinite, one can also work with finite fields.

Example 1.2 Let p denote a prime number and let \mathbb{Z}_p denote the set of congruence classes modulo p . There are finitely-many elements of \mathbb{Z}_p , namely the integers $\{0, 1, \dots, p-1\}$. Let \oplus, \odot denote addition and multiplication modulo p , i.e.,

$$a \oplus b := (a + b) \bmod p, \quad a \odot b := ab \bmod p.$$

Then $(\mathbb{Z}_p, \oplus, \odot)$ is a (finite) field.

Exercise 1.2 Fill in the following modular arithmetic tables:

\oplus	0	1	2	3	4
0					
1					
2					
3					
4					

\odot	0	1	2	3	4
0					
1					
2					
3					
4					

Hence, check that $(\mathbb{Z}_5, \oplus, \odot)$ is a field.

Exercise 1.3 The algebraic structure $(\mathbb{Z}_4, \oplus, \odot)$ is not a field. Which field axiom does it fail to satisfy?

1.1.2 Vector spaces

Just as fields are generalisations of standard number systems, vector spaces are generalisations of concepts and properties associated with the complex numbers and their geometric interpretation. In particular, Hamilton's attempts to generalise the complex number system with its evident two-dimensional interpretation to a number system in/for three-dimensions (an impossible task), resulted in the invention of quaternions, which can be seen as modeling four-dimensional space. Later, Gibbs and Heaviside extracted from Hamilton's model the three-dimensional description of vectors that we are familiar with, namely objects with magnitude and direction, geometrically represented by arrows. They also defined operations, such as addition, multiplication by a real number and dot and cross products. The modern definition of vector spaces is based on these latter concepts. Thus, we equip an abstract set V with two operations:

- an additive operation involving two vectors (and returning a vector);
- a multiplicative operation involving a scalar and a vector (and returning a vector).

These operations will also need to exhibit certain properties: commutativity, associativity, distributivity. The definition will also require a choice of scalars (i.e., a choice of field). Henceforth, generic vectors will be denoted by bold lower-case letters, unless otherwise indicated.

Definition 1.2 Let $(\mathbb{F}, +, \cdot)$ be a field and let e denote its multiplicative identity. A **vector space** over \mathbb{F} is a set V equipped with the operations of vector addition $+$ and scalar-vector multiplication \bullet , satisfying the following axioms for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, $a, b \in \mathbb{F}$:

VA0 Closure under addition: $\mathbf{u} + \mathbf{v} \in V$.

VA1 Associativity of vector addition: $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$.

VA2 Existence of vector additive identity: there exists $\mathbf{z} \in V$ such that for all $\mathbf{v} \in V$, $\mathbf{v} + \mathbf{z} = \mathbf{v}$.

VA3 Existence of vector additive inverses: for all $\mathbf{v} \in V$, there exists $\mathbf{v}^- \in V$ such that $\mathbf{v} + \mathbf{v}^- = \mathbf{z}$.

VA4 Commutativity of vector addition: $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$.

VM0 Closure under scalar-vector multiplication: $a \bullet \mathbf{v} \in V$.


VM1 Associativity of scalar-vector multiplication: $a \bullet (b \bullet \mathbf{v}) = (a \cdot b) \bullet \mathbf{v}$.


VM2 Distributive property of scalar-vector multiplication: $a \bullet (\mathbf{u} + \mathbf{v}) = (a \bullet \mathbf{u}) + (a \bullet \mathbf{v})$.

VM3 Distributive property of scalar addition: $(a + b) \bullet \mathbf{v} = (a \bullet \mathbf{v}) + (b \bullet \mathbf{v})$.

VM4 Multiplicative identity property: $e \bullet \mathbf{v} = \mathbf{v}$, where e is the scalar multiplicative identity in \mathbb{F} .

We denote a generic vector space by $(V, +, \bullet, \mathbb{F})$, although often we use the simplified notation $V(\mathbb{F})$, or just V and only specify the field \mathbb{F} (see examples later).

 If axioms VA0–VA4 are satisfied, then $(V, +)$ is an Abelian group. The remaining axioms add to this group structure properties which hold for Euclidean vectors (see Appendix B).

 It is important to note that there are **four operations** involved in the above set of axioms: the two field operations $+$, \cdot and the two operations returning vectors $+$, \bullet . It is evident that these operations only make sense in the given context; however, one tends to be sloppy and use the same symbols for the latter two operations as for the first two. We illustrate this later for the case of a real vector space, which is the most common structure used in this course.

We now turn to some basic properties of vector spaces.

1.2 Basic properties.

The vector space axioms are sufficient to ensure that basic, intuitive properties of vector spaces hold. These are listed in the following two propositions, together with selected proofs.

Proposition 1.1 — Elementary properties I. Let $V(\mathbb{F})$ be a vector space. Then the following hold:

1. (Cancellation in sums) For any $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, if $\mathbf{u} + \mathbf{v} = \mathbf{u} + \mathbf{w}$ then $\mathbf{v} = \mathbf{w}$.
2. For all $\mathbf{v} \in V$, $o \bullet \mathbf{v} = \mathbf{z}$.
3. For all $\mathbf{v} \in V$, $e^- \bullet \mathbf{v} = \mathbf{v}^-$.
4. For all $a \in \mathbb{F}$, $a \bullet \mathbf{z} = \mathbf{z}$.

Proof. To show 1, we use the axioms VA1–VA4:

$$\mathbf{u} + \mathbf{v} = \mathbf{u} + \mathbf{w} \implies \mathbf{u}^- + (\mathbf{u} + \mathbf{v}) = \mathbf{u}^- + (\mathbf{u} + \mathbf{w}) \implies (\mathbf{u}^- + \mathbf{u}) + \mathbf{v} = (\mathbf{u}^- + \mathbf{u}) + \mathbf{w} \implies \mathbf{z} + \mathbf{v} = \mathbf{z} + \mathbf{w} \implies \mathbf{v} = \mathbf{w}.$$

To show 2, we use axioms VA2, VM4, FA2, VM3 and VM4, in that order:

$$\mathbf{v} + \mathbf{z} = \mathbf{v} = e \bullet \mathbf{v} = (e + o) \bullet \mathbf{v} = e \bullet \mathbf{v} + o \bullet \mathbf{v} = \mathbf{v} + o \bullet \mathbf{v}.$$

Hence, by cancellation in sums, $\mathbf{z} = o \bullet \mathbf{v}$. The third and fourth claims are left as exercises. ■

Note that, by commutativity, if $\mathbf{v} + \mathbf{u} = \mathbf{w} + \mathbf{u}$ then $\mathbf{v} = \mathbf{w}$.

Proposition 1.2 — Elementary properties II. Let $V(\mathbb{F})$ be a vector space. Then:

1. (Cancellation in products)
 - (a) Let $o \neq a \in \mathbb{F}$ and $\mathbf{u}, \mathbf{v} \in V$. If $a \bullet \mathbf{u} = a \bullet \mathbf{v}$, then $\mathbf{u} = \mathbf{v}$.
 - (b) Let $a, b \in \mathbb{F}$ and $\mathbf{z} \neq \mathbf{u} \in V$. If $a \bullet \mathbf{u} = b \bullet \mathbf{u}$, then $a = b$.
2. Let $a \in \mathbb{F}$ and $\mathbf{u} \in V$. If $a \bullet \mathbf{u} = \mathbf{z}$, then either $a = o$ or $\mathbf{u} = \mathbf{z}$.

Proof. To prove statement 1 we note the following

- Let $a \bullet \mathbf{u} = a \bullet \mathbf{v}$ and $a \neq o$. Since $a \neq o$, by FM3, there exists a^* such that $a^* \cdot a = e$. Multiplying both sides with a^* on the left, we get, using VM1, FM3 and VM4, respectively,

$$a^* \cdot (a \bullet \mathbf{u}) = a^* \cdot (a \bullet \mathbf{v}) \implies (a^* \cdot a) \bullet \mathbf{u} = (a^* \cdot a) \bullet \mathbf{v} \implies e \bullet \mathbf{u} = e \bullet \mathbf{v} \implies \mathbf{u} = \mathbf{v}.$$

- Assume now that $\mathbf{u} \neq \mathbf{z}$. We show the statement by contradiction: assume that $a \neq b$. Then

$$a \bullet \mathbf{u} = b \bullet \mathbf{u} \implies a \bullet \mathbf{u} + b^- \bullet \mathbf{u} = b \bullet \mathbf{u} + b^- \bullet \mathbf{u} \implies (a + b^-) \bullet \mathbf{u} = o \bullet \mathbf{u} \implies (a + b^-) \bullet \mathbf{u} = \mathbf{z}.$$

Now $a + b^- \neq b + b^- = o$. Hence, there exists $(a + b^-)^*$; multiplying the last identity from the left by this scalar we get $\mathbf{u} = (a + b^-)^* \bullet \mathbf{z} = \mathbf{z}$, which is a contradiction. Hence, we must have $a = b$.

To prove statement 2, we note the following.

- By item 4 in Proposition 1.1 we can write $a \bullet \mathbf{u} = \mathbf{z} = a \bullet \mathbf{z}$; if $a \neq o$, we can use cancellation in products (part (a)) to find $\mathbf{u} = \mathbf{z}$.
- By item 2 in Proposition 1.1 we can write $a \bullet \mathbf{u} = \mathbf{z} = o \bullet \mathbf{u}$; if $\mathbf{u} \neq \mathbf{z}$, we can use cancellation in products (part (b)) to find $a = o$.

Hence, if $a \bullet \mathbf{u} = \mathbf{z}$, then either $a = o$ or $\mathbf{u} = \mathbf{z}$. ■

Exercise 1.4 Show that axioms VA0 and VM0 can be replaced with the requirement that $a \bullet \mathbf{u} + b \bullet \mathbf{v} \in V$ for all $\mathbf{u}, \mathbf{v} \in V$ and for all $a, b \in \mathbb{F}$.

1.3 Examples

We end this topic with examples of vector spaces, some involving familiar mathematical objects, such as column vectors, polynomials and continuous functions.

1.3.1 Euclidean vectors

These are the familiar ‘arrows’ in 3D, which form a vector space when equipped with standard (geometric) operations of vector addition and scalar-vector multiplication. We denote this vector space by $(\mathbb{E}^3, +, \cdot, \mathbb{R})$ or simply by \mathbb{E}^3 . An extensive discussion of Euclidean vectors is included in Appendix B.

1.3.2 Column vectors

We define (real) column vectors to be vertical arrays of (real) numbers. A generic column vector of size $n \in \mathbb{N}$ has the form

$$\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix},$$

where $v_i \in \mathbb{R}$ ($i = 1, \dots, n$). We denote the i th component of \mathbf{v} by $[\mathbf{v}]_i := v_i$; we also write $[v_i]_{1 \leq i \leq n} = \mathbf{v}$ or simply $[v_i] = \mathbf{v}$. We denote the set of real column vectors of size n by \mathbb{R}^n . On this set, we can define the following operations, inspired by the corresponding coordinate operations for 3D vectors:

$$\mathbf{u} + \mathbf{v} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} := \begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{bmatrix}, \quad a \bullet \mathbf{v} := \begin{bmatrix} av_1 \\ av_2 \\ \vdots \\ av_n \end{bmatrix} \quad (a \in \mathbb{R}).$$

These operations can be used to generate a vector space structure for \mathbb{R}^n , as the following result shows.

Proposition 1.3 Let the set \mathbb{R}^n be equipped with the following operations, for any $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n, a \in \mathbb{R}$:

- i. vector addition: $\mathbf{u} + \mathbf{v} := [u_i + v_i]$;
- ii. scalar-vector multiplication: $a \bullet \mathbf{v} := [a \cdot v_i]$.

Then $(\mathbb{R}^n, +, \bullet, \mathbb{R})$ is a vector space.

Proof. The proof is left as an exercise. ■

As part of the above proof, one should identify the zero vector and the additive inverse:

$$\mathbf{z} := \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \mathbf{v}^- := \begin{bmatrix} -v_1 \\ -v_2 \\ \vdots \\ -v_n \end{bmatrix} =: -\mathbf{v}.$$

The space \mathbb{R}^n is sometimes referred to as Euclidean space, as it can be seen as a generalisation of the sets of Euclidean coordinates in 3D. Note that the convention in this course is to use column vectors as members of \mathbb{R}^n , although some references prefer to use row vectors.

1.3.3 Polynomials

Let \mathcal{P}_n denote the set of polynomials of degree at most n with real coefficients:

$$\mathcal{P}_n = \{p(x) = a_0 + a_1x + \cdots + a_nx^n : a_i \in \mathbb{R}, i = 0, 1, \dots, n\}.$$

The sum of two polynomials of degree at most n , say p and q , is a polynomial of degree at most n , say r . We write formally

$$r(x) := (p + q)(x) := p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n,$$

given $p(x) = a_0 + a_1x + \cdots + a_nx^n$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$. The scalar multiple of a polynomial of degree at most n is also a polynomial of degree at most n . Formally,

$$(a \bullet p)(x) := a \cdot p(x) = a(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = aa_0 + aa_1x + \cdots + aa_nx^n.$$

These operations can be used to give \mathcal{P}_n a vector space structure.

Proposition 1.4 Let \mathcal{P}_n be equipped with the following operations, for any $p, q \in \mathcal{P}_n, a \in \mathbb{R}$:

- i. Vector addition: $(p + q)(x) := p(x) + q(x)$;
- ii. Scalar-vector multiplication: $(a \bullet p)(x) := a \cdot p(x)$.

Then $(\mathcal{P}_n, +, \bullet, \mathbb{R})$ is a vector space.

Proof. The proof is left as an exercise. ■

As part of the above proof, one should identify the 'zero vector' and the additive inverse:

$$\mathbf{z} := 0 + 0x + \cdots + 0x^n, \quad p^-(x) = -a_0 - a_1x - \cdots - a_nx^n.$$

In other words, the zero polynomial is the polynomial with zero coefficients.

1.3.4 Continuous functions

Let $\Omega \subset \mathbb{R}$ and consider the set

$$C(\Omega) = \{f : \Omega \rightarrow \mathbb{R} \mid f \text{ is continuous}\}.$$

This set is sometimes denoted by $C^0(\Omega)$ (see below for generalisations). We define, as in the case of polynomials,

$$(f + g)(x) := f(x) + g(x), \quad (a \bullet f)(x) = a \cdot f(x).$$

We note that $f + g$ and $a \bullet f$ are also continuous functions.

Proposition 1.5 Let $C(\Omega)$ be equipped with the following operations, for any $f, g \in C(\Omega), a \in \mathbb{R}$:

- i. Vector addition: $(f \oplus g)(x) := f(x) + g(x)$;
- ii. Scalar-vector multiplication: $(a \bullet f)(x) = a \cdot f(x)$.

Then $(C(\Omega), \oplus, \bullet, \mathbb{R})$ is a vector space.

Proof. The proof is left as an exercise. ■

As part of the proof, we identify the 'zero vector' as the zero function; the additive inverse of f is $-f$. For smoother functions, one can define the sets $C^k(\Omega)$, where $k \in \mathbb{N}$:

$$C^k(\Omega) = \left\{ f : \Omega \rightarrow \mathbb{R} : \frac{d^j f}{dx^j} \text{ is continuous, } 0 \leq j \leq k \right\}.$$

In other words, $C^k(\Omega)$ are the sets of functions that are k times differentiable on Ω for some $k \in \mathbb{N}$. One can similarly check that these are also vector spaces over \mathbb{R} , when equipped with the same operations.

1.3.5 Vector spaces over finite fields

Let $(\mathbb{F}_q, \oplus, \odot)$ denote a finite field with q elements, where q is a prime. Consider the set

$$\mathbb{F}_q^n := \{\mathbf{v} = (v_1, v_2, \dots, v_n) : v_i \in \mathbb{F}_q\}.$$

Then \mathbb{F}_q^n is a vector space over \mathbb{F}_q when equipped with the vector operations

$$\mathbf{u} \oplus \mathbf{v} := (u_1 \oplus v_1, u_2 \oplus v_2, \dots, u_n \oplus v_n), \quad a \bullet \mathbf{v} = (a \odot v_1, a \odot v_2, \dots, a \odot v_n),$$

where $a \in \mathbb{F}_q$. Unlike the previous examples, the set $V = \mathbb{F}_q^n$ has a finite number of elements, its cardinality being $|\mathbb{F}_q^n| = q^n$. A common choice is $\mathbb{F}_q = \mathbb{Z}_q$, with \oplus, \odot denoting addition and multiplication modulo q . These vector spaces are studied in Number Theory and Representation Theory.

1.4 Notation

For the remainder of this course, we will simplify the notation as follows:

- We will use the notation for sets to indicate also the corresponding structures, i.e., fields or vector spaces, e.g., we will write \mathbb{R} to indicate the field $(\mathbb{R}, +, \cdot)$, or \mathbb{R}^n to indicate the vector space $(\mathbb{R}^n, \oplus, \bullet, \mathbb{R})$.
- We will denote all the additive operations by $+$ and all multiplicative operations by \cdot (sometimes even dropping this symbol), e.g., we will write $a \cdot \mathbf{u}$ or $a\mathbf{u}$ instead of $a \bullet \mathbf{u}$.
- We will change notation as follows: $0 = o, 1 = e, -1 = e^-$ and $\mathbf{0} = \mathbf{z}$.

With these simplifications, the definition of a real vector space reads as follows.

Definition 1.3 A **real vector space** is a set V equipped with two operations, $+$ and \cdot , satisfying the following axioms, for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V, a, b \in \mathbb{R}$:

- VA0 Closure under vector addition: $\mathbf{u} + \mathbf{v} \in V$.
- VA1 Associativity of vector addition: $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$.
- VA2 Existence of zero vector: there exists $\mathbf{0} \in V$ such that for all $\mathbf{v} \in V, \mathbf{v} + \mathbf{0} = \mathbf{v}$.
- VA3 Existence of vector additive inverses: for all $\mathbf{v} \in V$, there exists $\mathbf{v}^- \in V$ such that $\mathbf{v} + \mathbf{v}^- = \mathbf{0}$.
- VA4 Commutativity of vector addition: $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$.
- VM0 Closure under scalar-vector multiplication: $a\mathbf{v} \in V$.
- VM1 Associativity of scalar-vector multiplication: $a(b\mathbf{v}) = (ab)\mathbf{v}$.
- VM2 Distributive property of scalar-vector multiplication: $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$.
- VM3 Distributive property of scalar addition: $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$.
- VM4 Multiplicative identity property: $1\mathbf{v} = \mathbf{v}$.



The definition of a **complex vector space** is similar, with the scalars a, b drawn from the field \mathbb{C} . We will mostly work with real vector spaces, although complex vector spaces will also be considered occasionally.