

Cooper Johnston

# Linear Algebra

Early Draft  
December 2024



# Contents

<b>0</b>	<b>Sets and Proofs</b>	<b>1</b>
0.1	Sets . . . . .	1
0.2	Mathematical logic . . . . .	4
0.3	Mappings . . . . .	4
<b>1</b>	<b>Vectors</b>	<b>7</b>
1.1	Fields . . . . .	7
1.2	Vector spaces . . . . .	9
1.3	Subspaces . . . . .	16
1.4	Linear combinations . . . . .	17
1.5	Basis and dimension . . . . .	19
<b>A</b>	<b>Solutions to Exercises</b>	<b>21</b>



# Chapter 0

## Sets and Proofs

### 0.1 Sets

We will begin by exploring the concept of a set through what is sometimes called intuitive or naive set theory. There exist more rigorous approaches, axiomatic set theories, but we will not be looking at these; our intuitive treatment of sets will suffice for the purposes of this course.

#### Definition 0.1.1.

1. A *set* is a well-defined collection of objects. By “well-defined” we mean that for any set  $S$ , any object is either definitely in  $S$  or definitely not in  $S$ .
2. An object that is in a set is called an *element* of that set. We write  $x \in S$  to denote that  $x$  is an element of the set  $S$ .
3. The set that does not contain any elements is called the *empty set*, denoted  $\emptyset$ .
4. The number of elements in a set is called the *cardinality* of that set. We write  $|S|$  to denote the cardinality of the set  $S$ .

One way to describe a set is by listing its elements. For example, we can define  $A$  to be the set containing the numbers 3, 6, 9, and 12, which we write as

$$A = \{3, 6, 9, 12\}.$$

Another way is to give a defining property of its elements. For example,  $A$  is the set of the first four positive multiples of three, or more mathematically,  $A$  is the set of all elements  $3n$  such that  $n = 1, 2, 3, 4$ , which we write as

$$A = \{3n \mid n = 1, 2, 3, 4\}.$$

The latter notation is often called set-builder notation.

We will denote certain special sets of numbers as follows:

- $\mathbb{N}$  is the set of natural numbers, which we will take to start at 1;
- $\mathbb{Z}$  is the set of integers;
- $\mathbb{Q}$  is the set of rational numbers;
- $\mathbb{Q}^+$  is the set of positive rational numbers;
- $\mathbb{R}$  is the set of real numbers;
- $\mathbb{R}^+$  is the set of positive real numbers; and
- $\mathbb{C}$  is the set of complex numbers.

It is possible to construct some of these using elements of the others. For example, the set of *rational* numbers  $\mathbb{Q}$  is the set of all numbers that can be expressed as a *ratio*  $p/q$  where  $p$  and  $q$  are integers and  $q \neq 0$ , i.e.

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}.$$

We can also use them to define other sets of numbers, such as the set of even numbers, which is the set of all numbers  $2n$  where  $n$  is an integer, i.e.  $\{2n \mid n \in \mathbb{Z}\}$ .

**Definition 0.1.2.** Let  $A$  and  $B$  be two sets.  $B$  is called a *subset* of  $A$ , denoted  $B \subseteq A$ , if every element in  $B$  is also an element in  $A$ , i.e. if  $b \in B$ , then  $b \in A$ .  $B$  is called a *proper subset* of  $A$ , denoted  $B \subset A$ , if  $B \subseteq A$  and  $B \neq A$ . The sets  $B = \emptyset$  and  $B = A$  are called the *trivial subsets* of  $A$ .

We can see from this definition that

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Continuous subsets of the real numbers can be expressed as *intervals*:

$$\begin{aligned} (a, b) &= \{x \in \mathbb{R} \mid a < x < b\} && \text{(open interval),} \\ [a, b] &= \{x \in \mathbb{R} \mid a \leq x \leq b\} && \text{(closed interval),} \\ [a, b) &= \{x \in \mathbb{R} \mid a \leq x < b\}, \\ (a, b] &= \{x \in \mathbb{R} \mid a < x \leq b\}. \end{aligned}$$

**Definition 0.1.3.** Let  $A_1, A_2, \dots, A_n$  be non-empty sets. The set

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}$$

is called the *Cartesian product* of  $A_1, A_2, \dots, A_n$ . If  $A_1 = A_2 = \cdots = A_n = A$ , then we can write

$$\underbrace{A \times A \times \cdots \times A}_{n \text{ times}} = A^n.$$

A common example of a Cartesian product is the set of ordered pairs of real numbers, which can be expressed as

$$\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}.$$

Note that the notation for an ordered pair  $(x, y) \in \mathbb{R}^2$  is the same as the notation for an open interval  $(x, y) \subseteq \mathbb{R}$ . This motivates an important rule in mathematics: We must be careful to specify what we mean with our notation if it is not clear from the context!

**Definition 0.1.4.** Let  $A$  and  $B$  be two sets. The set

$$A \cup B = \{c \mid c \in A \text{ or } c \in B\},$$

i.e. the set containing all elements of  $A$  as well as all the elements of  $B$ , is called the *union* of  $A$  and  $B$ . The set

$$A \cap B = \{c \mid c \in A \text{ and } c \in B\},$$

i.e. the set containing all the elements that are in both  $A$  and  $B$  at the same time, is called the *intersection* of  $A$  and  $B$ .

**Example 0.1.5.** Let  $A = \{1, 2\}$  and  $B = \{2, 4, 6\}$ . Express  $A \times B$ ,  $A \cup B$ , and  $A \cap B$  by listing their elements.

*Solution.*

1.  $A \times B$  is the set of all ordered pairs where the first element is in  $A$  and the second is in  $B$ :

$$A \times B = \{(1, 2), (1, 4), (1, 6), (2, 2), (2, 4), (2, 6)\}.$$

2.  $A \cup B$  is the set of all elements that are in either  $A$  or  $B$  (or both):

$$A \cup B = \{1, 2, 4, 6\}.$$

3.  $A \cap B$  is the set of all elements that are in both  $A$  and  $B$ :

$$A \cap B = \{2\}.$$

□

## Exercises

**Problem 0.1.** For each of the following, find  $A \cup B$ ,  $A \cap B$ ,  $A \times B$ , and  $B \times A$ .

(a)  $A = \{-1, 1\}$ ,  $B = \{1, 2, 3\}$ .

(b)  $A = \{0, 1\}$ ,  $B = \{3, 9, 27\}$ .

(c)  $A = [-1, 1]$ ,  $B = (0, \infty)$ .

**Problem 0.2.** Express the set of integers  $\mathbb{Z}$  in terms of the set of natural numbers  $\mathbb{N}$  and the set  $\{0\}$ .

**Problem 0.3.** Express the set of complex numbers  $\mathbb{C}$  in terms of the set of real numbers  $\mathbb{R}$  and the imaginary number  $i$ .

## 0.2 Mathematical logic

### 0.3 Mappings

**Definition 0.3.1.** Let  $A$  and  $B$  be two non-empty sets. A subset  $f \subseteq A \times B$  is called a *mapping* or a *function* from  $A$  to  $B$  if for all  $a \in A$ , there exists exactly one  $b \in B$  such that  $(a, b) \in f$  (when we say that a mapping is *well-defined*, we are referring to this property).

The set  $A$  is called the *domain* of  $f$  and the set  $B$  is called the *codomain*. For any pair  $(a, b) \in f$ , we write  $f(a) = b$  or  $a \mapsto b$  and say  $f$  maps  $a$  to  $b$ . We write

$$f : A \rightarrow B, \quad a \mapsto b \\ \text{(or } f(a) = b \text{)}$$

to denote that  $f$  is a mapping from  $A$  to  $B$  that maps elements  $a \in A$  to corresponding elements  $b \in B$ .

**Definition 0.3.2.** Let  $f : A \rightarrow B$  be a mapping. The set  $\{f(a) \mid a \in A\}$  is called the *range* of  $f$ , denoted  $\text{range}(f)$ .

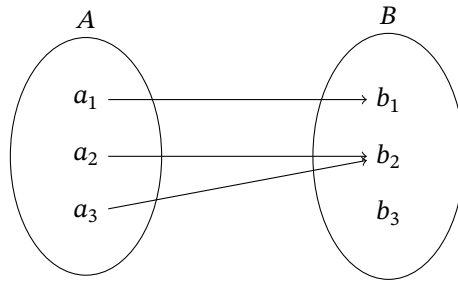


Figure 1: An example of a mapping from  $A = \{a_1, a_2, a_3\}$  to  $B = \{b_1, b_2, b_3\}$

If we have a mapping with a finite domain and codomain, we can represent it with a diagram like in Figure 1. We see that the range of the mapping shown in this diagram is  $\{b_1, b_2\}$  since these are the elements in  $B$  that are mapped to.

**Definition 0.3.3.** A mapping  $f : A \rightarrow B$  is called *injective* if for all  $a, \tilde{a} \in A$ , if  $f(a) = f(\tilde{a})$ , then  $a = \tilde{a}$ ; in other words, no two different elements in  $A$  map to the same element in  $B$ .  $f$  is called *surjective* if for all  $b \in B$ , there exists an  $a \in A$  such that  $f(a) = b$ . A mapping that is both injective and surjective is called *bijective*.



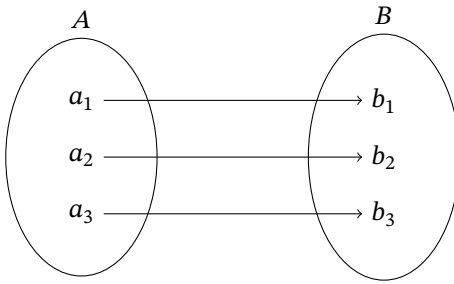


Figure 2: An example of a bijective mapping from  $A = \{a_1, a_2, a_3\}$  to  $B = \{b_1, b_2, b_3\}$

**Theorem 0.3.4.** A mapping  $f : A \rightarrow B$  is surjective if and only if  $\text{range}(f) = B$ .

*Proof.* Exercise 0.4

**Definition 0.3.5.** Let  $f : A \rightarrow B$  be a bijective mapping. The mapping  $f^{-1} : B \rightarrow A$ ,  $f^{-1}(f(a)) = a$  is called the *inverse mapping* of  $f$ .

## Exercises

**Problem 0.4.** Prove Theorem 0.3.4.



# Chapter 1

## Vectors

### 1.1 Fields

**Definition 1.1.1.** Let  $A$  and  $B$  be two non-empty sets. A mapping of the form

$$\odot : B \times A \rightarrow A, \quad (b, a) \mapsto b \odot a$$

is called a *binary operation*. Since the result  $b \odot a$  must be an element of  $A$ , we say that the set  $A$  is *closed* under such a binary operation.

**Definition 1.1.2.** Let  $F$  be a set and let

$$\begin{aligned} + : F \times F &\rightarrow F & (\text{addition}), \\ \cdot : F \times F &\rightarrow F & (\text{multiplication}) \end{aligned}$$

be two binary operations.  $F$ , together with these operations, is called a *field* if all of the following axioms are satisfied:

1. ASSOCIATIVITY: For all  $a, b, c \in F$ , we have

$$(a + b) + c = a + (b + c) \quad \text{and} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

2. COMMUTATIVITY: For all  $a, b \in F$ , we have

$$a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a.$$

3. EXISTENCE OF ADDITIVE IDENTITY: There exists an element  $0_F \in F$ , called the *additive identity*, such that for all  $a \in F$ , we have

$$a + 0_F = a.$$

4. EXISTENCE OF MULTIPLICATIVE IDENTITY: There exists an element  $1_F \in F$ , called the *multiplicative identity*, such that for all  $a \in F$ , we have

$$a \cdot 1_F = a.$$

5. **EXISTENCE OF ADDITIVE INVERSE:** For every  $a \in F$ , there exists an element  $-a \in F$ , called the *additive inverse* of  $a$ , such that

$$a + (-a) = 0_F.$$

6. **EXISTENCE OF MULTIPLICATIVE INVERSE:** For every  $a \in F$  other than  $0_F$ , there exists an element  $a^{-1} \in F$ , called the *multiplicative inverse* of  $a$ , such that

$$a \cdot a^{-1} = 1_F.$$

7. **DISTRIBUTIVITY OF  $\cdot$  OVER  $+$ :** For all  $a, b, c \in F$ , we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

A field is therefore a structure that consists of a set and two binary operations on that set. When evaluating whether a given structure is a field, we must take care to ensure that the given operations are valid, that is, that both operations are indeed well-defined mappings and that the set is closed under them. Then we can investigate the properties of the operations to check for consistency with the field axioms. Let us examine some examples.

**Example 1.1.3.** Show that the set of real numbers  $\mathbb{R}$ , together with standard addition and multiplication, is a field.

*Solution.* Much of this proof will involve results that we already know and don't need to show in detail. First, note that since the sum and product of two real numbers is always a real number,  $\mathbb{R}$  is closed under standard addition and multiplication. Now we can check the field axioms:

1. We already know that standard addition and multiplication are associative.
2. **Commutativity:** We also know that standard addition and multiplication are commutative.
3. **Existence of additive identity:** The additive identity is the number 0.
4. **Existence of multiplicative identity:** The multiplicative identity is the number 1.
5. **Existence of additive inverse:** For any  $x \in \mathbb{R}$ , the additive inverse is the number  $-x$ .
6. **Existence of multiplicative inverse:** For any  $x \in \mathbb{R}$  other than 0, the multiplicative inverse is the number  $1/x$ .
7. **Distributivity:** We already know that standard multiplication is distributive over standard addition.

Hence,  $\mathbb{R}$  with standard addition and multiplication is a field. □

**Example 1.1.4.** Show that the set of integers  $\mathbb{Z}$ , together with standard addition and multiplication, is not a field.

*Solution.* We need only find one axiom that does not hold. The multiplicative identity is the number 1. Consider the number  $2 \in \mathbb{Z}$ . There does not exist a number  $n \in \mathbb{Z}$  such that  $2n = 1$ ; that is, 2 does not have a multiplicative inverse in  $\mathbb{Z}$ . Hence,  $\mathbb{Z}$  is not a field.  $\square$

We will typically denote a field simply by its set, and when working with fields of numbers, we will from now on assume standard addition and multiplication unless otherwise specified. For example, the field “ $\mathbb{R}$ ” is assumed to mean  $\mathbb{R}$  together with standard addition and multiplication.

## Exercises

**Problem 1.1.** Consider the set of complex numbers  $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$  where  $i$  is the imaginary number, defined such that  $i^2 = -1$ . We naturally have the operations  $+$  and  $\cdot$  defined such that for all  $(a + bi), (c + di) \in \mathbb{C}$ , we have

$$(a + bi) + (c + di) = a + c + bi + di = (a + c) + (b + d)i$$

and

$$\begin{aligned} (a + bi) \cdot (c + di) &= ac + a(di) + (bi)c + (bi)(di) = ac + adi + bci + bdi^2 \\ &= ac + adi + bci - bd = (ac - bd) + (ad + bc)i. \end{aligned}$$

Show that  $\mathbb{C}$  with these operations is a field.

## 1.2 Vector spaces

**Definition 1.2.1.** Let  $F$  be a field whose elements we will call *scalars*, let  $V$  be a set whose elements we will call *vectors*, and let

$$\begin{aligned} \odot : F \times V &\rightarrow V && (\text{scalar multiplication}), \\ \oplus : V \times V &\rightarrow V && (\text{vector addition}) \end{aligned}$$

be two binary operations.  $V$ , together with these operations, is called a *vector space* over  $F$  if all of the following axioms are satisfied:

1. ASSOCIATIVITY OF  $\oplus$ : For all  $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ , we have

$$(\mathbf{u} \oplus \mathbf{v}) \oplus \mathbf{w} = \mathbf{u} \oplus (\mathbf{v} \oplus \mathbf{w}).$$

2. COMMUTATIVITY OF  $\oplus$ : For all  $\mathbf{u}, \mathbf{v} \in V$ , we have

$$\mathbf{u} \oplus \mathbf{v} = \mathbf{v} \oplus \mathbf{u}.$$

3. **EXISTENCE OF ZERO VECTOR:** There exists an element  $\mathbf{0} \in V$ , called the *zero vector*, such that for all  $\mathbf{v} \in V$ , we have

$$\mathbf{v} \oplus \mathbf{0} = \mathbf{v}.$$

4. **EXISTENCE OF ADDITIVE INVERSE:** For every  $\mathbf{v} \in V$ , there exists an element  $-\mathbf{v} \in V$ , called the additive inverse of  $\mathbf{v}$ , such that

$$\mathbf{v} \oplus (-\mathbf{v}) = \mathbf{0}.$$

5. **COMPATIBILITY OF  $\odot$  WITH FIELD MULTIPLICATION:** For all  $a, b \in F$  and  $\mathbf{v} \in V$ , we have

$$a \odot (b \odot \mathbf{v}) = (ab) \odot \mathbf{v}.$$

6. **SCALAR MULTIPLICATIVE IDENTITY:** For every  $\mathbf{v} \in V$ , we have

$$1_F \odot \mathbf{v} = \mathbf{v}$$

where  $1_F$  is the multiplicative identity of  $F$ .

7. **DISTRIBUTIVITY OF  $\odot$  OVER  $\oplus$ :** For all  $a \in F$  and  $\mathbf{u}, \mathbf{v} \in V$ , we have

$$a \odot (\mathbf{u} \oplus \mathbf{v}) = (a \odot \mathbf{u}) \oplus (a \odot \mathbf{v}).$$

8. **DISTRIBUTIVITY OF  $\odot$  OVER FIELD ADDITION:** For all  $a, b \in F$  and  $\mathbf{v} \in V$ , we have

$$(a + b) \odot \mathbf{v} = (a \odot \mathbf{v}) \oplus (b \odot \mathbf{v}).$$

A vector space is therefore a structure that consists of a field of scalars, a set of vectors, and two binary operations—one that takes a scalar and a vector and one that takes two vectors—that both yield a vector result. Note that the zero vector is the same as the additive identity under vector addition. To distinguish between scalars and vectors, we will typically write vectors in **bold**.

Just like with fields, when evaluating whether a given structure is a vector space, we must verify that the given operations are well-defined and that the set of vectors is closed under them. If it is not already clear, we must also verify that the given field of scalars is indeed a field. Let us examine some examples.

**Example 1.2.2.** Show that  $\mathbb{R}^2$ , together with the operations  $\oplus$  and  $\odot$  defined such that for all  $c \in \mathbb{R}$  and  $(x, y), (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ , we have

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \quad \text{and} \quad c \odot (x, y) = (cx, cy),$$

is a vector space over  $\mathbb{R}$ .

*Solution.* Let  $(x, y), (x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$  and let  $a, b \in \mathbb{R}$ . First we must verify that  $\mathbb{R}^2$  is closed under the given operations. Since  $(x_1 + x_2), (y_1 + y_2) \in \mathbb{R}$ , we see that

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \in \mathbb{R}^2,$$

and similarly, since  $cx, cy \in \mathbb{R}$ , we also see that

$$c \odot (x, y) = (cx, cy) \in \mathbb{R}^2.$$

Thus,  $\mathbb{R}^2$  is closed under  $\oplus$  and  $\odot$ . Now we can check the vector space axioms:

1. ASSOCIATIVITY OF  $\oplus$ :

$$\begin{aligned} ((x_1, y_1) \oplus (x_2, y_2)) \oplus (x_3, y_3) &= (x_1 + x_2, y_1 + y_2) \oplus (x_3, y_3) \\ &= (x_1 + x_2 + x_3, y_1 + y_2 + y_3) \\ &= (x_1, y_1) \oplus (x_2 + x_3, y_2 + y_3) \\ &= (x_1, y_1) \oplus ((x_2, y_2) \oplus (x_3, y_3)). \end{aligned}$$

2. COMMUTATIVITY OF  $\oplus$ :

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2) = (x_2 + x_1, y_2 + y_1) = (x_2, y_2) \oplus (x_1, y_1).$$

3. EXISTENCE OF ZERO VECTOR: Consider  $\mathbf{0} = (0, 0)$ . We see

$$(x, y) \oplus \mathbf{0} = (x, y) \oplus (0, 0) = (x + 0, y + 0) = (x, y),$$

so  $\mathbf{0}$ , as we have defined it, is the zero vector.

4. EXISTENCE OF ADDITIVE INVERSE: Consider  $-(x, y) = (-x, -y)$ . We see

$$(x, y) \oplus (-(x, y)) = (x, y) \oplus (-x, -y) = (x - x, y - y) = (0, 0) = \mathbf{0},$$

so  $-(x, y)$ , as we have defined it, is the additive inverse of  $(x, y)$ .

5. COMPATIBILITY OF  $\odot$  WITH FIELD MULTIPLICATION:

$$a \odot (b \odot (x, y)) = a \odot (bx, by) = (abx, aby) = (ab) \odot (x, y).$$

6. SCALAR MULTIPLICATIVE IDENTITY: Recall that the number 1 is the multiplicative identity of  $\mathbb{R}$ . We see

$$1 \odot (x, y) = (1x, 1y) = (x, y).$$

7. DISTRIBUTIVITY OF  $\odot$  OVER  $\oplus$ :

$$\begin{aligned} a \odot ((x_1, y_1) \oplus (x_2, y_2)) &= a \odot (x_1 + x_2, y_1 + y_2) = (a(x_1 + x_2), a(y_1 + y_2)) \\ &= (ax_1 + ax_2, ay_1 + ay_2) = (ax_1, ay_1) \oplus (ax_2, ay_2) \\ &= (a \odot (x_1, y_1)) \oplus (a \odot (x_2, y_2)). \end{aligned}$$

8. DISTRIBUTIVITY OF  $\odot$  OVER FIELD ADDITION:

$$\begin{aligned}(a + b) \odot (x, y) &= ((a + b)x, (a + b)y) = (ax + bx, ay + by) \\ &= (ax, ay) \oplus (bx, by) = (a \odot (x, y)) \oplus (b \odot (x, y)).\end{aligned}$$

Hence,  $\mathbb{R}^2$  with these operations is a vector space over  $\mathbb{R}$ .  $\square$

**Example 1.2.3.** Let  $P_2(\mathbb{R})$  be the set of all polynomials of degree  $\leq 2$  over the real numbers, i.e.

$$P_2(\mathbb{R}) = \{p : \mathbb{R} \rightarrow \mathbb{R}, p(x) = a_0 + a_1x + a_2x^2 \mid a_0, a_1, a_2 \in \mathbb{R}\}.$$

Show that  $P_2(\mathbb{R})$ , together with the operations  $\oplus$  and  $\odot$  defined such that for all  $c \in \mathbb{R}$  and  $p(x) = a_0 + a_1x + a_2x^2, q(x) = b_0 + b_1x + b_2x^2 \in P_2(\mathbb{R})$ , we have

$$p(x) \oplus q(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2$$

and

$$c \odot p(x) = ca_0 + ca_1x + ca_2x^2,$$

is a vector space over  $\mathbb{R}$ .

*Solution.* Since the coefficients of  $p(x) \oplus q(x)$  and  $c \odot p(x)$  are in  $\mathbb{R}$ , we see that  $p(x) \oplus q(x)$  and  $c \odot p(x)$  are in  $P_2(\mathbb{R})$ . Thus,  $P_2(\mathbb{R})$  is closed under addition and scalar multiplication. Now we can check the vector space axioms:

1. ASSOCIATIVITY OF  $\oplus$ : Let  $r(x) = c_0 + c_1x + c_2x^2 \in P_2(\mathbb{R})$ . Then,

$$\begin{aligned}(p(x) \oplus q(x)) \oplus r(x) &= ((a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2) \oplus r(x) \\ &= (a_0 + b_0 + c_0) + (a_1 + b_1 + c_1)x + (a_2 + b_2 + c_2)x^2 \\ &= p(x) \oplus ((b_0 + c_0) + (b_1 + c_1)x + (b_2 + c_2)x^2) \\ &= p(x) \oplus (q(x) \oplus r(x)).\end{aligned}$$

2. COMMUTATIVITY OF  $\oplus$ :

$$\begin{aligned}p(x) \oplus q(x) &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 \\ &= (b_0 + a_0) + (b_1 + a_1)x + (b_2 + a_2)x^2 = q(x) \oplus p(x).\end{aligned}$$

3. EXISTENCE OF ZERO VECTOR: Consider  $o(x) = 0 + 0x + 0x^2$ . We see

$$p(x) \oplus o(x) = (a_0 + 0) + (a_1 + 0)x + (a_2 + 0)x^2 = a_0 + a_1x + a_2x^2 = p(x),$$

so  $o(x)$  is the zero vector.

4. EXISTENCE OF ADDITIVE INVERSE: Consider  $-p(x) = -a_0 + (-a_1)x + (-a_2)x^2$ . We see

$$\begin{aligned}p(x) \oplus (-p(x)) &= (a_0 + (-a_0)) + (a_1 + (-a_1))x + (a_2 + (-a_2))x^2 \\ &= 0 + 0x + 0x^2 = o(x),\end{aligned}$$

so  $-p(x)$ , as we have defined it, is the additive inverse of  $p(x)$ .



5. COMPATIBILITY OF  $\odot$  WITH FIELD MULTIPLICATION: Let  $d \in F$ . Then,

$$\begin{aligned} c \odot (d \odot p(x)) &= c \odot (da_0 + da_1x + da_2x^2) = cda_0 + cda_1x + cda_2x^2 \\ &= (cd) \odot p(x). \end{aligned}$$

6. SCALAR MULTIPLICATIVE IDENTITY:

$$1 \odot p(x) = 1a_0 + 1a_1x + 1a_2x^2 = a_0 + a_1x + a_2x^2 = p(x).$$

7. DISTRIBUTIVITY OF  $\odot$  OVER  $\oplus$ :

$$\begin{aligned} c \odot (p(x) \oplus q(x)) &= c \odot ((a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2) \\ &= c(a_0 + b_0) + c(a_1 + b_1)x + c(a_2 + b_2)x^2 \\ &= (ca_0 + cb_0) + (ca_1 + cb_1)x + (ca_2 + cb_2)x^2 \\ &= (c \odot p(x)) \oplus (c \odot q(x)). \end{aligned}$$

8. DISTRIBUTIVITY OF  $\odot$  OVER FIELD ADDITION:

$$\begin{aligned} (c + d) \odot p(x) &= (c + d)a_0 + (c + d)a_1x + (c + d)a_2x^2 \\ &= (ca_0 + da_0) + (ca_1 + da_1)x + (ca_2 + da_2)x^2 \\ &= (c \odot p(x)) \oplus (d \odot p(x)). \end{aligned}$$

Hence,  $P_2(\mathbb{R})$  with these operations is a vector space over  $\mathbb{R}$ . □

**Example 1.2.4.** Show that  $\mathbb{R}^3$ , together with the operations  $\oplus$  and  $\odot$  defined such that for all  $c \in \mathbb{R}$  and  $(x, y, z), (\tilde{x}, \tilde{y}, \tilde{z}) \in \mathbb{R}^3$ , we have

$$(x, y, z) \oplus (\tilde{x}, \tilde{y}, \tilde{z}) = (x + \tilde{x}, y + \tilde{y}, 0) \quad \text{and} \quad c \odot (x, y, z) = (cx, cy, cz),$$

is not a vector space over  $\mathbb{R}$ .

*Solution.* We need only find one vector space axiom that does not hold. Consider  $(1, 1, 1) \in \mathbb{R}^3$ . We see

$$(1, 1, 1) \oplus (x, y, z) = (x, y, 0) \neq (1, 1, 1)$$

for any  $(x, y, z) \in \mathbb{R}^3$ , so there is no additive identity in  $\mathbb{R}^3$  under  $\oplus$ . Hence,  $\mathbb{R}^3$  with these operations is not a vector space. □

In these examples and in the definition, we used the symbols  $\odot$  and  $\oplus$  for scalar multiplication and vector addition, respectively, in order to help distinguish these operations from addition and multiplication on the field. From now on, we will use additive notation

$$\mathbf{u} \oplus \mathbf{v} = \mathbf{u} + \mathbf{v}$$

for vector addition and multiplicative notation

$$c \odot \mathbf{v} = c\mathbf{v}$$

for scalar multiplication, but it is still important to remember the distinction between these operations with vectors and the analogous operations on the field. We will also write expressions with vectors assuming that scalar multiplication takes precedence over vector addition, akin to the standard order of operations.

**Theorem 1.2.5.** *Let  $V$  be a vector space over a field  $F$ . For all  $\mathbf{v} \in V$  and  $a \in F$ , the following hold:*

1.  $0_F \mathbf{v} = \mathbf{0}$ .
2.  $a\mathbf{0} = \mathbf{0}$ .
3. If  $a\mathbf{v} = \mathbf{0}$ , then  $a = 0_F$  or  $\mathbf{v} = \mathbf{0}$ .
4.  $(-1_F)\mathbf{v} = -\mathbf{v}$ .

*Proof.*

1. Since  $0_F$  is the additive identity on the field, we know  $c + 0_F = c$ . In particular,  $0_F + 0_F = 0_F$ . Thus,

$$\begin{aligned}
 0_F \mathbf{v} &= (0_F + 0_F) \mathbf{v} \\
 0_F \mathbf{v} &= 0_F \mathbf{v} + 0_F \mathbf{v} && \text{distributive property} \\
 0_F \mathbf{v} + (-(0_F \mathbf{v})) &= 0_F \mathbf{v} + 0_F \mathbf{v} + (-(0_F \mathbf{v})) \\
 \mathbf{0} &= 0_F \mathbf{v} + 0_F \mathbf{v} + (-(0_F \mathbf{v})) && \text{vector additive inverse} \\
 \mathbf{0} &= 0_F \mathbf{v} + (0_F \mathbf{v} + (-(0_F \mathbf{v}))) && \text{associative property} \\
 \mathbf{0} &= 0_F \mathbf{v} + \mathbf{0} && \text{vector additive inverse} \\
 \mathbf{0} &= 0_F \mathbf{v}. && \text{vector additive identity}
 \end{aligned}$$

2. Since the zero vector  $\mathbf{0}$  is the additive identity under vector addition, we know  $\mathbf{v} + \mathbf{0} = \mathbf{v}$ . In particular,  $\mathbf{0} + \mathbf{0} = \mathbf{0}$ . Thus,

$$\begin{aligned}
 a\mathbf{0} &= a(\mathbf{0} + \mathbf{0}) \\
 a\mathbf{0} &= a\mathbf{0} + a\mathbf{0} && \text{distributive property} \\
 a\mathbf{0} + (-(a\mathbf{0})) &= a\mathbf{0} + a\mathbf{0} + (-(a\mathbf{0})) \\
 \mathbf{0} &= a\mathbf{0} + a\mathbf{0} + (-(a\mathbf{0})) && \text{vector additive inverse} \\
 \mathbf{0} &= a\mathbf{0} + (a\mathbf{0} + (-(a\mathbf{0}))) && \text{associative property} \\
 \mathbf{0} &= a\mathbf{0} + \mathbf{0} && \text{vector additive inverse} \\
 \mathbf{0} &= a\mathbf{0}. && \text{vector additive identity}
 \end{aligned}$$

3. Suppose  $a\mathbf{v} = \mathbf{0}$ . We have two possible cases for  $a$ . If  $a = 0_F$ , then we are already finished with the proof. Otherwise, if  $a \neq 0_F$ , we can multiply both sides with the multiplicative inverse (on the field) of  $a$ :

$$\begin{aligned}
 a\mathbf{v} &= \mathbf{0} \\
 a^{-1}(a\mathbf{v}) &= a^{-1}\mathbf{0} \\
 (a^{-1}a)\mathbf{v} &= a^{-1}\mathbf{0} && \text{vector space axiom 5} \\
 1_F\mathbf{v} &= a^{-1}\mathbf{0} && \text{field multiplicative inverse} \\
 \mathbf{v} &= a^{-1}\mathbf{0} && \text{scalar multiplicative identity} \\
 \mathbf{v} &= \mathbf{0}. && \text{part 2 of this theorem}
 \end{aligned}$$

4. We will start by using the zero vector:

$$\begin{aligned}
 -\mathbf{v} &= -\mathbf{v} + \mathbf{0} \\
 &= -\mathbf{v} + 0_F\mathbf{v} && \text{part 1 of this theorem} \\
 &= -\mathbf{v} + (1_F + (-1_F))\mathbf{v} && \text{field additive inverse} \\
 &= -\mathbf{v} + (1_F\mathbf{v} + (-1_F)\mathbf{v}) && \text{distributive property} \\
 &= -\mathbf{v} + (\mathbf{v} + (-1_F)\mathbf{v}) && \text{scalar multiplicative identity} \\
 &= (-\mathbf{v} + \mathbf{v}) + (-1_F\mathbf{v}) && \text{associative property} \\
 &= \mathbf{0} + (-1_F)\mathbf{v} && \text{vector additive inverse} \\
 &= (-1_F)\mathbf{v}. && \text{vector additive identity} \quad \blacksquare
 \end{aligned}$$

Note that in the above proof, the distributive property used in parts 1 and 2 comes from vector space axiom 7, while the distributive property used in part 4 comes from axiom 8.

## Exercises

**Problem 1.2.** Let  $P_n(\mathbb{C})$  be the set of all polynomials of degree  $\leq n$  over  $\mathbb{C}$ , i.e.

$$P_n(\mathbb{C}) = \left\{ p : \mathbb{C} \rightarrow \mathbb{C}, p(z) = \sum_{k=0}^n a_k z^k \mid a_0, a_1, \dots, a_n \in \mathbb{C} \right\}.$$

Show that  $P_n(\mathbb{C})$ , together with addition and scalar multiplication defined such that for all  $c \in \mathbb{C}$  and  $p(z) = \sum_{k=0}^n a_k z^k, q(z) = \sum_{k=0}^n b_k z^k \in P_n(\mathbb{C})$ , we have

$$p(z) + q(z) = \sum_{k=0}^n (a_k + b_k) z^k \quad \text{and} \quad cp(z) = \sum_{k=0}^n ca_k z^k,$$

is a vector space over  $\mathbb{C}$ .

**Problem 1.3.** Show that the zero vector of a vector space is unique, i.e. show that if  $\mathbf{0}$  and  $\tilde{\mathbf{0}}$  are two zero vectors in the same vector space, then  $\mathbf{0} = \tilde{\mathbf{0}}$ .

**Problem 1.4.** Show that for every vector  $\mathbf{v}$  in a vector space  $V$ , the additive inverse  $-\mathbf{v}$  is unique.

**Problem 1.5.** Show that for all vectors  $\mathbf{u}, \mathbf{v}$  in a vector space  $V$ , there exists a unique vector  $\mathbf{x} \in V$  such that  $\mathbf{u} + \mathbf{x} = \mathbf{v}$ . Show that the solution must be  $\mathbf{x} = -\mathbf{u} + \mathbf{v}$ .

### 1.3 Subspaces

**Definition 1.3.1.** Let  $V$  be a vector space over a field  $F$  and let  $W$  be a non-empty subset of  $V$ . The set  $W$ , together with vector addition and scalar multiplication as defined on  $V$ , is called a *subspace* of  $V$  if  $W$  with these operations is a vector space over  $F$ . The subspaces  $W = \{\mathbf{0}_V\}$  and  $W = V$  are called the *trivial subspaces* of  $V$ .

**Theorem 1.3.2.** Let  $V$  be a vector space over a field  $F$  and let  $W$  be a non-empty subset of  $V$ . Then,  $W$  is a subspace of  $V$  if and only if for all  $\mathbf{u}, \mathbf{v} \in W$  and  $a \in F$ , we have the closure conditions

$$\mathbf{u} + \mathbf{v} \in W \quad \text{and} \quad a\mathbf{u} \in W.$$

*Proof.*

$\Rightarrow$  Suppose  $W$  is a subspace of  $V$ . Then,  $W$  is a vector space, so  $W$  must be closed under vector addition and scalar multiplication.

$\Leftarrow$  Suppose that the closure conditions hold. Since the operations for vector addition and scalar multiplication are inherited from the vector space  $V$ , we know vector space axioms 1 and 2 (commutativity and associativity), 5 and 6 (properties of scalar multiplication), and 7 and 8 (distributivity) are satisfied. Therefore, we need only show:

3. Existence of zero vector: Since  $a\mathbf{u} \in W$  for all  $a \in F$ , choose  $a = 0_F$ . Then, by part 1 of Theorem 1.2.5, we have  $0_F\mathbf{u} = \mathbf{0} \in W$ .
4. Existence of additive inverse: Now choose  $a = -1_F$ . Then, by part 4 of Theorem 1.2.5, we have  $(-1_F)\mathbf{u} = -\mathbf{u} \in W$ .

Hence,  $W$  is a vector space. ■

**Lemma 1.3.3.** If  $W$  is a subspace of a vector space  $V$ , then  $\mathbf{0}_V \in W$  and  $\mathbf{0}_W = \mathbf{0}_V$ .

*Proof.* Exercise 1.6

**Theorem 1.3.4.** Let  $U$  be a vector space. If  $V$  and  $W$  are subspaces of  $U$ , then  $V \cap W$  is also a subspace of  $U$ .

*Proof.* Suppose  $V$  and  $W$  are subspaces of  $U$ . Then, by Lemma 1.3.3,  $\mathbf{0}_U \in V$  and

$\mathbf{0}_U \in W$ , so  $\mathbf{0}_U \in V \cap W$ . This means that  $V \cap W \neq \emptyset$ , and clearly  $V \cap W \subseteq U$ . We will now use Theorem 1.3.2.

Let  $\mathbf{u}_1, \mathbf{u}_2 \in V \cap W$ . Then  $\mathbf{u}_1, \mathbf{u}_2 \in V$  and  $\mathbf{u}_1, \mathbf{u}_2 \in W$ , so since  $V$  and  $W$  are vector spaces,  $\mathbf{u}_1 + \mathbf{u}_2 \in V$  and  $\mathbf{u}_1 + \mathbf{u}_2 \in W$ . Thus,

$$\mathbf{u}_1 + \mathbf{u}_2 \in V \cap W.$$

Let  $\mathbf{u} \in V \cap W$  and let  $a$  be a scalar. Then,  $a\mathbf{u} \in V$  and  $a\mathbf{u} \in W$ , so

$$a\mathbf{u} \in V \cap W.$$

Hence,  $V \cap W$  is a subspace of  $U$ . ■

**Corollary 1.3.5.** *Let  $V$  be a vector space and let  $W_1, W_2, \dots, W_n$ ,  $n \geq 2$  be subspaces of  $V$ . Then,  $\cap_{k=1}^n W_k$  is also a subspace of  $V$ .*

*Proof.* Exercise 1.7

## Exercises

**Problem 1.6.** Prove Lemma 1.3.3.

**Problem 1.7.** Prove Corollary 1.3.5.

## 1.4 Linear combinations

**Definition 1.4.1.** Let  $V$  be a vector space over a field  $F$  and let  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in V$  and  $a_1, a_2, \dots, a_n \in F$ . A vector of the form

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_n\mathbf{v}_n = \sum_{k=1}^n a_k\mathbf{v}_k$$

is called a *linear combination* of  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ .

**Definition 1.4.2.** Let  $V$  be a vector space over a field  $F$  and let  $S = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} \subseteq V$ . The set of all linear combinations of  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ , i.e.

$$\{a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_n\mathbf{v}_n \mid a_1, a_2, \dots, a_n \in F\},$$

is called the *span* of  $S$ , denoted  $\text{span}(S)$ .

If  $\text{span}(S) = V$ , we say that the set  $S$  spans  $V$ .

**Theorem 1.4.3.** *Let  $V$  be a vector space and let  $S = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} \subseteq V$ . Then,*

1.  $\text{span}(S)$  is a subspace of  $V$ ; and

2. If  $W$  is a subspace of  $V$  and  $S \subseteq W$ , then  $\text{span}(S) \subseteq W$ . In other words,  $\text{span}(S)$  is the smallest subspace of  $V$  that contains all the vectors in  $S$ .

*Proof.*

1. By assumption,  $\text{span}(S) \neq \emptyset$ , and since  $V$  is closed under addition and scalar multiplication,  $\text{span}(S) \subseteq V$ . Now we will show that  $\text{span}(S)$  is closed under addition and scalar multiplication. Let  $\mathbf{u}, \mathbf{v} \in \text{span}(S)$ . Then,

$$\mathbf{u} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n \quad \text{and} \quad \mathbf{v} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_n\mathbf{v}_n$$

for some scalars  $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ . Thus,

$$\begin{aligned} \mathbf{u} + \mathbf{v} &= a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n + b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_n\mathbf{v}_n \\ &= a_1\mathbf{v}_1 + b_1\mathbf{v}_1 + a_2\mathbf{v}_2 + b_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n + b_n\mathbf{v}_n \\ &= (a_1 + b_1)\mathbf{v}_1 + (a_2 + b_2)\mathbf{v}_2 + \cdots + (a_n + b_n)\mathbf{v}_n \in \text{span}(S). \end{aligned}$$

Similarly, letting  $c$  be an arbitrary scalar, we see

$$c\mathbf{u} = c(a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n) = ca_1\mathbf{v}_1 + ca_2\mathbf{v}_2 + \cdots + ca_n\mathbf{v}_n \in \text{span}(S).$$

Hence, by Theorem 1.3.2,  $\text{span}(S)$  is a subspace of  $V$ .

2. Let  $W$  be a subspace of  $V$  such that  $S \subseteq W$ . Then,  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in W$ . Since  $W$  is a vector space,  $W$  is closed under addition and scalar multiplication, so any linear combination of vectors in  $W$  is also in  $W$ . In particular, any linear combination of  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$  is in  $W$ . Hence,  $\text{span}(S) \subseteq W$ . ■

**Definition 1.4.4.** Let  $V$  be a vector space over a field  $F$  and let  $S = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} \subseteq V$  and  $a_1, a_2, \dots, a_n \in F$ . The set  $S$  is called *linearly independent* if

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$$

only if  $a_1 = a_2 = \cdots = a_n = 0_F$ . Otherwise, if there exists such a linear combination where at least one of the coefficients  $a_1, a_2, \dots, a_n$  is non-zero, we say  $S$  is *linearly dependent*.

**Theorem 1.4.5.** Let  $V$  be a vector space and let  $S = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} \subseteq V$  where  $n \geq 2$ . The set  $S$  is linearly dependent if and only if at least one of the vectors in  $S$  can be expressed as a linear combination of the others.

*Proof.*

- ⇒ Suppose  $S$  is linearly dependent. Then, there exist scalars  $a_1, a_2, \dots, a_n$ , not all zero, such that  $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$ . Say  $a_k \neq 0$  for some  $k \in \{1, 2, \dots, n\}$ .

Then,

$$\begin{aligned} \mathbf{0} &= a_1 \mathbf{v}_1 + \cdots + a_{k-1} \mathbf{v}_{k-1} + a_k \mathbf{v}_k + a_{k+1} \mathbf{v}_{k+1} + \cdots + a_n \mathbf{v}_n \\ -a_k \mathbf{v}_k &= a_1 \mathbf{v}_1 + \cdots + a_{k-1} \mathbf{v}_{k-1} + a_{k+1} \mathbf{v}_{k+1} + \cdots + a_n \mathbf{v}_n \\ \mathbf{v}_k &= -a_k^{-1} a_1 \mathbf{v}_1 + \cdots + (-a_k^{-1}) a_{k-1} \mathbf{v}_{k-1} + (-a_k^{-1}) a_{k+1} \mathbf{v}_{k+1} + \\ &\quad \cdots + (-a_k^{-1}) a_n \mathbf{v}_n. \end{aligned}$$

Hence,  $\mathbf{v}_k$  can be expressed as a linear combination of the other vectors.

$\Leftarrow$  Let  $F$  denote the field of scalars. Suppose that for some  $\mathbf{v}_k \in S$ , there exist scalars  $b_1, \dots, b_{k-1}, b_{k+1}, \dots, b_n$  such that  $\mathbf{v}_k = b_1 \mathbf{v}_1 + \cdots + b_{k-1} \mathbf{v}_{k-1} + b_{k+1} \mathbf{v}_{k+1} + \cdots + b_n \mathbf{v}_n$ . Then,

$$\begin{aligned} \mathbf{0} &= b_1 \mathbf{v}_1 + \cdots + b_{k-1} \mathbf{v}_{k-1} + (-\mathbf{v}_k) + b_{k+1} \mathbf{v}_{k+1} + \cdots + b_n \mathbf{v}_n \\ \mathbf{0} &= b_1 \mathbf{v}_1 + \cdots + b_{k-1} \mathbf{v}_{k-1} + (-1_F) \mathbf{v}_k + b_{k+1} \mathbf{v}_{k+1} + \cdots + b_n \mathbf{v}_n, \end{aligned}$$

where we see there is at least one coefficient,  $-1_F$ , that is definitely non-zero. Hence,  $S$  is linearly dependent.  $\blacksquare$

## 1.5 Basis and dimension

**Definition 1.5.1.** A set  $S = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$  of vectors in a vector space  $V$  is called a *basis* of  $V$  if  $S$  is linearly independent and  $\text{span}(S) = V$ . The vectors in  $S$  are called *basis vectors*.

**Theorem 1.5.2.** Let  $S = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$  be a basis of a vector space  $V$ . Then, every  $\mathbf{v} \in V$  can be expressed as a unique linear combination of the vectors in  $S$ .

*Proof.* By definition,  $\text{span}(S) = V$ , so any vector in  $V$  can be expressed as a linear combination of the vectors in  $S$ . To show uniqueness, suppose  $\mathbf{v} \in V$  can be expressed as two linear combinations

$$\mathbf{v} = a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \cdots + a_n \mathbf{v}_n \quad \text{and} \quad \mathbf{v} = b_1 \mathbf{v}_1 + b_2 \mathbf{v}_2 + \cdots + b_n \mathbf{v}_n.$$

Then,

$$\begin{aligned} \mathbf{v} + (-\mathbf{v}) &= a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \cdots + a_n \mathbf{v}_n + (-(b_1 \mathbf{v}_1 + b_2 \mathbf{v}_2 + \cdots + b_n \mathbf{v}_n)) \\ \mathbf{0} &= (a_1 - b_1) \mathbf{v}_1 + (a_2 - b_2) \mathbf{v}_2 + \cdots + (a_n - b_n) \mathbf{v}_n. \end{aligned}$$

Since  $S$  is linearly independent, this means that  $a_1 - b_1 = a_2 - b_2 = \cdots = a_n - b_n = 0_F$  (where  $F$  is the field of scalars), so  $a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$ . Hence, the representation of  $\mathbf{v}$  as a linear combination of the vectors in  $S$  is unique.  $\blacksquare$

**Theorem 1.5.3.** Let  $V$  be a vector space. If there exists a basis of  $V$  with  $n$  vectors, then every subset of  $V$  with more than  $n$  vectors is linearly dependent.

**Corollary 1.5.4.** *Let  $V$  be a vector space. If there exists a basis of  $V$  with  $n$  vectors, then every basis of  $V$  has  $n$  vectors.*

**Definition 1.5.5.** Let  $V$  be a vector space that has a basis with  $n$  vectors. The number  $n$  is called the *dimension* of  $V$ , denoted  $\dim(V)$ . If  $V = \{\mathbf{0}\}$ , then  $\dim(V) = 0$ .

**Theorem 1.5.6.** *Let  $V$  be a vector space and let  $\dim(V) = n$ . Then,*

1. *If a subset  $S \subseteq V$  with  $n$  vectors is linearly independent, then  $S$  is a basis of  $V$ ; and*
2. *If a subset  $S \subseteq V$  with  $n$  vectors spans  $V$ , then  $S$  is a basis of  $V$ .*



# Appendix A

## Solutions to Exercises

### Chapter 0

- 0.1 (a)  $A \cup B = \{-1, 1, 2, 3\}$ ,  
 $A \cap B = \{1\}$ ,  
 $A \times B = \{(-1, 1), (-1, 2), (-1, 3), (1, 1), (1, 2), (1, 3)\}$ ,  
 $B \times A = \{(1, -1), (1, 1), (2, -1), (2, 1), (3, -1), (3, 1)\}$ .
- (b)  $A \cup B = \{0, 1, 3, 9, 27\}$ ,  
 $A \cap B = \emptyset$ ,  
 $A \times B = \{(0, 3), (0, 9), (0, 27), (1, 3), (1, 9), (1, 27)\}$ ,  
 $B \times A = \{(3, 0), (3, 1), (9, 0), (9, 1), (27, 0), (27, 1)\}$ .
- (c)  $A \cup B = [-1, \infty)$ ,  
 $A \cap B = (0, 1]$ ,  
 $A \times B = \{(a, b) \mid a \in [-1, 1], b \in (0, \infty)\}$ ,  
 $B \times A = \{(b, a) \mid b \in (0, \infty), a \in [-1, 1]\}$ .
- 0.2  $\mathbb{Z} = \{\pm n \mid n \in \mathbb{N}\} \cup \{0\}$ .
- 0.3  $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ .

### Chapter 1

- 1.1 Let  $a, b, c, d, e, f \in \mathbb{R}$ . First we must verify that  $\mathbb{C}$  is indeed closed under the given operations. Since  $(a + c), (b + d) \in \mathbb{R}$ , we see that

$$(a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{C},$$

and similarly, since  $(ac - bd), (ad + bc) \in \mathbb{R}$ , we also see that

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i \in \mathbb{C}.$$

Thus,  $\mathbb{C}$  is closed under  $+$  and  $\cdot$ . Now we can check the field axioms:

1. Associativity:

$$\begin{aligned} ((a + bi) + (c + di)) + (e + fi) &= (a + c + (b + d)i) + (e + fi) \\ &= a + c + e + (b + d + f)i \\ &= a + bi + (c + e) + (d + f)i \\ &= (a + bi) + ((c + di) + (e + fi)). \end{aligned}$$

$$\begin{aligned}
 ((a + bi) \cdot (c + di)) \cdot (e + fi) &= (ac - bd + (ad + bc)i) \cdot (e + fi) \\
 &= (ac - bd)e - (ad + bc)f + ((ac - bd)f + (ad + bc)e)i \\
 &= ace - bde - adf - bcf + (acf - bdf + ade + bce)i \\
 &= a(ce - df) - b(cf + de) + (a(cf + de) + b(ce - df))i \\
 &= (a + bi) \cdot (ce - df + (cf + de)i) \\
 &= (a + bi) \cdot ((c + di) \cdot (e + fi)).
 \end{aligned}$$

2. Commutativity:

$$(a + bi) + (c + di) = (a + b) + (c + d)i = (b + a) + (d + c)i = (c + di) + (a + bi).$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i = (ca - db) + (da + cb)i = (c + di) \cdot (a + bi).$$

3. Existence of additive identity: Consider  $0 = 0 + 0i \in \mathbb{C}$ . We see

$$(a + bi) + (0 + 0i) = (a + 0) + (b + 0)i = a + bi.$$

4. Existence of multiplicative identity: Consider  $1 = 1 + 0i \in \mathbb{C}$ . We see

$$(a + bi) \cdot (1 + 0i) = (1a - 0b) + (0a + 1b)i = a + bi.$$

5. Existence of additive inverse: For  $a + bi$ , consider  $-a - bi \in \mathbb{C}$ . We see

$$(a + bi) + (-a - bi) = (a - a) + (b - b)i = 0 + 0i = 0.$$

6. Existence of multiplicative inverse: Suppose  $a + bi \neq 0$ . Consider<sup>1</sup>

$$\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \in \mathbb{C}.$$

We see

$$\begin{aligned}
 (a + bi) \cdot \left( \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \right) &= \frac{a^2}{a^2 + b^2} + \frac{b^2}{a^2 + b^2} + \left( \frac{ab}{a^2 + b^2} - \frac{ba}{a^2 + b^2} \right)i \\
 &= \frac{a^2 + b^2}{a^2 + b^2} + 0i = 1.
 \end{aligned}$$

7. Distributivity:

$$\begin{aligned}
 (a + bi) \cdot ((c + di) + (e + fi)) &= (a + bi) \cdot (c + e + (d + f)i) \\
 &= a(c + e) - b(d + f) + (a(d + f) + b(c + e))i \\
 &= ac + ae - bd - bf + (ad + af + bc + be)i \\
 &= ac - bd + (ad + bc)i + ae - bf + (af + be)i \\
 &= ((a + bi) \cdot (c + di)) + ((a + bi) \cdot (e + fi)).
 \end{aligned}$$

Hence,  $\mathbb{C}$  with these operations is a field.

**1.3** By the definition of the zero vector, for any vector  $\mathbf{v}$ , we have  $\mathbf{v} + \mathbf{0} = \mathbf{v}$  and  $\mathbf{v} + \tilde{\mathbf{0}} = \mathbf{v}$ . In particular,  $\mathbf{0} = \mathbf{0} + \tilde{\mathbf{0}} = \tilde{\mathbf{0}} + \mathbf{0} = \tilde{\mathbf{0}}$ .

**1.6 (Proof of Lemma 1.3.3)** Since  $W$  is a vector space, there must exist a zero vector  $\mathbf{0}_W \in W$ , and since  $W \subseteq V$ , we have  $\mathbf{0}_W \in V$ . By uniqueness of the zero vector (see Exercise 1.3),  $\mathbf{0}_W = \mathbf{0}_V$ .

**1.7 (Proof of Corollary 1.3.5)** We can prove this result by induction. The base case (where  $n = 2$ ) is Theorem 1.3.4. For our inductive hypothesis, suppose  $U = \cap_{k=1}^m W_k$  is a subspace of  $V$ . By Theorem 1.3.4, if  $W_{m+1}$  is a subspace of  $V$ , then  $U \cap W_{m+1} = \cap_{k=1}^{m+1} W_k$  is also a subspace of  $V$ . Hence,  $\cap_{k=1}^n W_k$  is a subspace of  $V$  for all  $n \geq 2$ .

<sup>1</sup>This can be found by setting  $(a + bi) \cdot (x + yi) = 1$  and solving for  $x$  and  $y$ .