Cooper Johnston

# Linear Algebra

November 2024

# Contents

# 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. This intuitive treatment of sets will suffice for the purposes of this course. A more rigorous approach, axiomatic set theory, is outside the scope of this course.

**Definition 0.1.1.** 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 $S$.

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 $S$.

The set that does not contain any elements is called the empty set, denoted $\varnothing$.

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, denoted by

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

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 $n = 1, 2, 3, 4$, denoted by

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

The latter notation is often called set-builder notation.

We will denote certain special sets of numbers as follows:

$\mathbb{Z}$ is the set of integers;
$\mathbb{Z}^+$ is the set of positive 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.

**Example 0.1.2.** The set of even numbers is the set of all numbers $2n$ where $n$ is an integer, i.e. $\{2n \mid n \in \mathbb{Z}\}$.

**Example 0.1.3.** The set of **ratio**nal 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. $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$.

**Definition 0.1.4.** 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. for every $b \in B$, we have $b \in A$.

$B$ is called a proper subset of $A$, denoted $B \subset A$, if $B \subseteq A$ and $B \neq A$.

**Definition 0.1.5.** Let $A_1, A_2, \ldots, A_n$ be non-empty sets. The set

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

is called the Cartesian product of $A_1, A_2, \ldots, A_n$.

The Cartesian product of a set with itself can be denoted by

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

For example, $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, the set of ordered pairs of real numbers.

**Example 0.1.6.** Let $A = \{1, 2\}$ and $B = \{1, 2, 3\}$. Then,

$$\begin{aligned} A \times B &= \{(a, b) \mid a \in A, b \in B\} \\ &= \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}. \end{aligned}$$

## 0.2 Mappings

**Definition 0.2.1.** Let $A$ and $B$ be two non-empty sets, and let $\mathcal{R} \subseteq A \times B$. The set $\mathcal{R}$ is called a relation between $A$ and $B$. For an ordered pair $(a, b) \in \mathcal{R}$, we say that $\mathcal{R}$ relates $a$ to $b$.

**Definition 0.2.2.** Let $A$ and $B$ be two non-empty sets. A relation $f$ between $A$ and $B$ is called a mapping or a function if for every $a \in A$, there exists exactly one $b \in B$ such that $f$ relates $a$ to $b$. The set $A$ is called the domain of $f$, and $B$ is called the codomain of $f$.

We write $f : A \to B$ to denote that $f$ is a mapping with domain $A$ and codomain $B$; that is, $f$ is a mapping from $A$ to $B$.

We write $f(a) = b$ or $a \mapsto b$ to denote that $f$ relates $a$ to $b$; that is, $f$ maps $a$ to $b$.

**Definition 0.2.3.** Let $A$ and $B$ be two sets and let $\odot : B \times A \to A$. The mapping $\odot$ is called a binary operation. If $A = B$, i.e. we have $\odot : A \times A \to A$, we say $\odot$ is a binary operation on $A$.

We write $x \odot y = z$ to denote that $\odot$ maps $(x, y)$ to $z$.

## 0.3 Propositional logic

## 0.4 Proofs

# Chapter 1

# Vectors

## 1.1 Vector spaces

**Definition 1.1.1.** Let $F$ be a set and let $+$ and $\cdot$ be two binary operations on $F$. $F$, together with the operations $+$ and $\cdot$, is called a field if all of the following axioms are satisfied:

1. $+$ and $\cdot$ are associative, i.e. 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. $+$ and $\cdot$ are commutative, i.e. for all $a, b \in F$, we have

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

3. 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. 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. 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. 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. $\cdot$ is distributive over $+$, i.e. for all $a, b, c \in F$, we have

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

The operation $+$ is called addition, and the operation $\cdot$ is called multiplication. For multiplication, we will often use the notation $a \cdot b = ab$.

Let us examine some examples of what is and isn't a field.

**Example 1.1.2.** Show that the set of real numbers $\mathbb{R}$, together with standard addition and multiplication, is a field.

*Solution.* We will prove this result by examining each of the axioms one-by-one:

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

Hence, $\mathbb{R}$ is a field. $\square$

**Example 1.1.3.** Show that the set of integers $\mathbb{Z}$, together with standard addition and multiplication, is not a field.

*Solution.* 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. $\square$

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

**Definition 1.1.4.** Let $F$ be a field and $V$ be a set, and let $\odot : F \times V \to V$ and $\oplus : V \times V \to V$ 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. $\oplus$ is associative, i.e. 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. $\oplus$ is commutative, i.e. for all $\mathbf{u}, \mathbf{v} \in V$, we have
$$\mathbf{u} \oplus \mathbf{v} = \mathbf{v} \oplus \mathbf{u}.$$

3. 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. 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. For all $a, b \in F$ and $\mathbf{v} \in V$, we have
$$a \odot (b \odot \mathbf{v}) = (ab) \odot \mathbf{v}.$$

6. 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. $\odot$ is distributive over $\oplus$, i.e. 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. For all $a, b \in F$ and $\mathbf{v} \in V$, we have
$$(a + b) \odot \mathbf{v} = (a \odot \mathbf{v}) \oplus (b \odot \mathbf{v}).$$

The elements of $F$ are called scalars and the elements of $V$ are called vectors. The operation $\odot$ is called scalar multiplication and the operation $\oplus$ is called vector addition.

Note that the zero vector is the same as the additive identity under vector addition.

Let us now examine some examples of what is and isn't a vector space.

**Example 1.1.5.** Show that $\mathbb{R}^2$, together with

- vector addition $\oplus$ defined such that for all $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, we have $(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$; and
- scalar multiplication $\odot$ defined such that for all $c \in \mathbb{R}$ and $(x, y) \in \mathbb{R}^2$, we have $c \odot (x, y) = (cx, cy)$,

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 $a, b \in \mathbb{R}$. We will prove this result by examining each of the axioms one-by-one:

1. We have

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

so $\oplus$ is associative.

2. We have

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

so $\oplus$ is commutative.

3. Let $\mathbf{0} = (0, 0)$. Then,

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

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

4. Let $-(x, y) = (-x, -y)$. Then,

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

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

5. We have

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

6. Recall that the number 1 is the multiplicative identity of $\mathbb{R}$. We have

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

7. We have

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

so $\odot$ is distributive over $\oplus$.

8. We have

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

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

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.

## Exercises

**Exercise 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.

## Appendix A

# Solutions to Exercises

## Chapter 1

*Solution 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:

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

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

2. Commutativity:

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

$$\begin{aligned}(a+bi)\cdot(c+di) &= (ac-bd)+(ad+bc)i = (ca-db)+(da+cb)i \\ &= (c+di)\cdot(a+bi).\end{aligned}$$

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 $a+bi \in \mathbb{C}$, 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 $a+bi \neq 0$. Then, we have three possible cases:
   (a) $a, b \neq 0$.
   (b) $a = 0$, $b \neq 0$.
   (c) $a \neq 0$, $b = 0$.
7. Distributivity:

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

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