ALGEBRA

MATHS 120

Department of Mathematics
The University of Auckland, New Zealand

February 2025

Contents

Set Theory

In this chapter we will learn the basics of mathematical reasoning and some widely used proof techniques.

1.1 Introduction to logic

Mathematics mainly asks questions about whether a given claim (a statement) is true or false. To answer such questions, it is important to agree on aspects of the "language of the mathematics".

A **statement** (or **proposition**) is a sentence that is either always true (which we abbreviate as **T**) or always false (abbreviated as **F**). For example:

- $2+2=4$. (this statement is **T**)
- $2+3=7$. (this statement is **F**)

are all statements. The following are *not* statements:

- What time is it? (this is a question)
- He is 1.9 metres tall.
- $n+3=2$.

The last two examples fail to be statements because we need to specify who "He" is and what value n takes: for some choices for a number n, the statement will be true, and for some other choices the statement will be false. Here "He" and n are **free variables** (we are 'free' to replace them with any value we like); a sentence containing free variables is called a **predicate**.

1.1.1 Implications

Let A and B be statements. An **implication** is a statement in the form "If A then B" or "A implies B". A is called the **hypothesis** and B is called the **conclusion**. (Note that we use the word ‘hypothesis’ differently to how it is used in some other subjects.) We write the implication symbolically as $A \implies B$.

Informally, we want the implication $A \implies B$ to mean “if A is true then B is true”. These sort of notions are made precise by a system of logic called propositional calculus. We can write a table with all the possible truth values for A and B on the left and the resulting value for $A \implies B$ on the right; this table (called a **truth table**) will then become the definition of the symbol $A \implies B$ — whenever we have two statements, we can check their truth value and look up the relevant line in the table to check the truth value of $A \implies B$. The table is as follows:

A	B	$A \implies B$
T	T	**T**
T	F	**F**
F	T	**T**
F	F	**T**

Note that the truth value of $A \implies B$ does not depend upon the actual statements A or B, but only on their truth values. By definition, the only time $A \implies B$ is false is when A is true and B is false.

1.1.2 Compound statements

One of the properties of the symbol “ $\implies$ ” is that it takes two propositions and returns one (more complicated) proposition. A symbol like this is called a **connective**, because they are often used to connect different propositions together.

The basic connectives are

- “not”, denoted by $\neg$
- “and”, denoted by $\wedge$,
- “or”, denoted by $\vee$,
- “equivalent (if and only if)”, denoted by $\iff$,
- “implies”, denoted by $\implies$.

Statements built up using these connectives are **compound statements**. For statements A and B, we have

- $\neg A$ is **T** if A is **F** and vise-versa. (Note that $\neg(\neg A) \iff A$: if A is **T** then $\neg A$ is **F** and so $\neg(\neg A)$ is **T**).
- $A \wedge B$ is **T** only if both A and B are **T**.

- $A \vee B$ is **T** if either of A or B is **T**.
- $A \iff B$ is **T** only if A and B have the same truth values.

As earlier, we can also collect these definitions in a truth table:

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \iff B$
T	T	**F**	**T**	**T**	**T**
T	F	**F**	**F**	**T**	**F**
F	T	**T**	**F**	**T**	**F**
F	F	**T**	**F**	**F**	**T**

1.1.3 Properties

These connectives have many properties, here are some examples.

Proposition 1.1.1: Properties of logical connectives

Let A, B and C be statements. The following holds:

1. $\neg(\neg A) \iff A$ *(Double negation)*
2. $\neg(A \wedge B) \iff ((\neg A) \vee (\neg B))$ *(De Morgan's Laws)*
3. $\neg(A \vee B) \iff ((\neg A) \wedge (\neg B))$ *(De Morgan's Laws)*
4. $(A \wedge (B \vee C)) \iff ((A \wedge B) \vee (A \wedge C))$ *(Distributivity)*
5. $(A \vee (B \wedge C)) \iff ((A \vee B) \wedge (A \vee C))$ *(Distributivity)*

Proof. All of these can be proved using truth tables. For example, we can build the following truth table to prove (2):

A	B	$A \wedge B$	$\neg(A \wedge B)$	$\neg A$	$\neg B$	$(\neg A) \vee (\neg B)$
T	T	**T**	**F**	**F**	**F**	**F**
T	F	**F**	**T**	**F**	**T**	**T**
F	T	**F**	**T**	**T**	**F**	**T**
F	F	**F**	**T**	**T**	**T**	**T**

We now compare the truth values in the two highlighted columns:

A	B	$\neg(A \wedge B) \iff ((\neg A) \vee (\neg B))$
T	T	**T**
T	F	**T**
F	T	**T**
F	F	**T**

Therefore, $\neg(A \wedge B)$ and $(\neg A) \vee (\neg B)$ are equivalent. □

Exercise 1.1.2: More properties of logical connectives

Using truth tables, show that if A, B, and C are statements then the following holds.

1. $(A \wedge B) \iff (B \wedge A)$ *(Commutativity of logical and)*
2. $(A \vee B) \iff (B \vee A)$ *(Commutativity of logical or)*
3. $((A \wedge B) \wedge C) \iff (A \wedge (B \wedge C))$ *(Associativity of logical and)*
4. $((A \vee B) \vee C) \iff (A \vee (B \vee C))$ *(Associativity of logical or)*
5. $(A \wedge (A \implies B)) \implies B$ *(Modus ponens)*
6. $((A \implies B) \wedge (B \implies C)) \implies (A \implies C)$ *(Transitivity of logical implication)*
7. $((A \iff B) \wedge (B \iff C)) \implies (A \iff C)$ *(Transitivity of logical equivalence)*
8. $A \implies (A \vee B)$
9. $(A \wedge B) \implies A$

Remark 1.1.3

We can conclude from part 3 and 4 of Exercise 1.1.2 that there is no need to use brackets and we can just write

$$A \wedge B \wedge C$$

and

$$A \vee B \vee C$$

Be warned that brackets are needed when there is a mix of "logical and" and "logical or"! For example, one can check (using a truth table, for example) that the two statements

$$(A \wedge B) \vee C$$

and

$$A \wedge (B \vee C)$$

are not equivalent, so that

$$A \wedge B \vee C$$

is not well defined!

1.1.4 Converse and contrapositive statements

Let A and B be statements. The **converse** of the implication $A \implies B$ is the implication $B \implies A$. The **contrapositive** of the implication $A \implies B$ is the implication $\neg B \implies \neg A$.

Example 1.1.4

Let n be an integer (so n is not *a free variable!) and let P be the statement "if n is even, then n^2 is even". Write down the converse and contrapositive of P.*

Solution.
Let A be the statement "n is even', and B be the statement "n^2 is even". Then P is the statement $A \implies B$.

The converse of P is $B \implies A$, that is, if n^2 is even, then n is even.

The contrapositive of P is $\neg B \implies \neg A$, that is, if n^2 is not even, then n is not even.

Note that, in the example above, P is true (we shall prove this formally in the next section), and so are its converse and contrapositive. It is important to be careful — one example does not allow us to conclude that it is always the case that the truth value of an implication is in any way related to the truth value of its contrapositive or converse, and if we want to say anything then we need a formal proof. To help us guess what the relationship may be, if any, here is another example:

Example 1.1.5

Let n be an integer and let Q be the statement "if n is positive, then $n > 17$". Write down the converse and contrapositive of Q.

Solution.
In this case, we have a statement $A \implies B$ where A is "n is positive" and B is "$n > 17$". The converse is $B \implies A$; that is, "if $n > 17$ then n is positive"; the contrapositive is $\neg B \implies \neg A$, i.e. "if $n \leq 17$ then n is not positive".

Here, we see that Q is false (it is not true that every positive number is greater than 17), and so is the contrapositive (there are numbers less than or equal to 17 which *are* positive); but the converse of Q (if a number is greater than 17, then it is positive) *is* true.

We shall study later the relationship between the truth values of $A \implies B$ and its contrapositive (see Proposition 1.2.6). However based on these examples alone we may say something about the relationship between $A \implies B$ and $B \implies A$: the two are not equivalent.

Warning.
These examples show that even if $B \implies A$ it is not necessarily true that $A \implies B$. *In order to prove an implication, it is not enough to prove the converse implication: the two statements are logically unrelated to each other.*

Exercise 1.1.6

Let A and B be statements and let P be the proposition $(A \wedge B) \implies (A \vee \neg B)$. Write down the truth tables for P, for the converse of P, and for the contrapositive of P.

1.2 Proofs

We discuss direct proof and proof by contradiction. As in the last section, we will use even (and odd) numbers to illustrate some of the concepts. It will be useful to have a proper definition.

Definition 1.2.1

An integer n is called ***even*** *if there exists an integer m such that $n = 2m$. It is called* ***odd*** *if there exists an integer m such that $n = 2m + 1$.*

We do *not* define odd numbers to be 'integers which are not even', or even numbers to be 'integers which are not odd': we need to check that our definition matches our usual intuition about evenness and oddness. This is handled by the following formal proposition.

Proposition 1.2.2

Every integer is exactly one of even or odd.

While Proposition 1.2.2 may appear obvious, it requires proof! We recommend trying to prove this yourself once you have learned induction.

1.2.1 Direct proof

A direct proof uses a logical sequence of arguments to show that a statement is true. We often use a mix of mathematical expressions and sentences in words to formulate the argumentation. For example, the proof of property (2) in Proposition 1.1.1 is a direct proof formulated with a mix of truth tables and words. The words are important to ensure that the reader can follow the logical argumentation. We give another example of a direct proof.

Example 1.2.3

Prove that $1 + 2 + 3 + \cdots + 10 = 55$

Proof. While cumbersome, the sum of the first ten positive integers can be shown to equal 55 by adding the integers 1 through 10 one by one as follows: We know that $1+2 = 3$, so $1+2+3 = 2+3 = 6$, which implies that $1+2+3+4 = 6+4 = 10$, so that $1+2+3+4+5 = 10+5 = 15$. Then $1+2+3+4+5+6 = 15+6 = 21$ and thus, $1+2+3+4+5+6+7 = 21+7 = 28$, so that $1+2+3+4+5+6+7+8 = 28+8 = 36$. Finally, $1+2+3+4+5+6+7+8+9$ must then equal $36+9 = 45$, and we conclude that $1 + 2 + 3 + \cdots + 10 = 45 + 10$, which is 55 as claimed. □

You may know an easier way to add the integers 1 through 10, given by the formula

$$1 + 2 + 3 + \cdots + 10 = \frac{10 \cdot (10 + 1)}{2}.$$

This suggests an alternative proof that is more mathematical, but also shorter:

Alternative proof for Example 1.2.3. Suppose $1+2+3+\cdots+10=k$ for some integer k. Note that we can swap the order, that is, we also have $k=10+9+8+\cdots+1$. By adding these two summations term by term, we have

$$\begin{array}{rcl} k+k & = & (1+10)+(2+9)+(3+8)+\cdots+(10+1) \\ & = & \quad 11 \quad + \quad 11 \quad + \quad 11 \quad +\cdots+ \quad 11. \end{array}$$

Here, the right-hand side contains ten terms, and we get

$$2\,k = 10\cdot 11 \iff k=\tfrac{1}{2}11\cdot 10 = 55$$

as required. □

To give a direct proof of the implication $A \implies B$, we suppose that A is true, and use a series of steps to deduce that B must also be true.

Example 1.2.4

Prove that if an integer n is even, then n^2 is even.

Proof. Let n be an even integer. By Definition 1.2.1, there exists an integer m such that $n=2m$. Thus $n^2=(2m)^2=4m^2=2(2m^2)=2k$, where we have introduced a new letter k to denote the number $2m^2$. Because $2m^2$ is an integer (if you multiply integers together, the result is an integer) we have written $n^2=2k$ where k is an integer; again by the definition, we conclude that n^2 is even. □

Observe that the statement of Example 1.2.4 concerns not just one even number n, but **all** integers n that are even. Hence, one or even several examples with n^2 even will not constitute a proof. For example, the fact that the integer 6 is even and so is $6^2=36$ is not a proof of the statement. On the other hand, to show that a statement of the form "all … have a certain property" is **false**, it suffices to give a **counterexample**.

Example 1.2.5

Prove that the statement "all integers are even" is false.

Proof. The number 7 is an integer, but $7=2m+1$ for $m=3$, so by Definition 1.2.1, the number 7 is odd. Proposition 1.2.2 implies that 7 is, therefore, not even. Hence, not all integers are even. □

1.2.2 Proof by contraposition

We begin with the promised relationship between an implication $A \implies B$ and its contrapositive, $\neg B \implies \neg A$. In the examples above (Examples 1.1.4 and 1.1.5), we computed the truth values for two implications along with their contrapositives. We saw that in both cases, the implication was true if and only if its contrapositive was true. This evidence is not enough to conclude that it is always the case that implications are equivalent to their contrapositives; we must state and prove this guessed equivalence formally.

Proposition 1.2.6

For every pair of statements A and B, we have

$$(A \implies B) \iff (\neg B \implies \neg A).$$

Proof. Let us compute the truth table for this statement, using the truth table definitions of the symbols:

A	B	$\neg B$	$\neg A$	$\neg B \implies \neg A$	$A \implies B$
T	T	**F**	**F**	**T**	**T**
T	F	**T**	**F**	**F**	**F**
F	T	**F**	**T**	**T**	**T**
F	F	**T**	**T**	**T**	**T**

and thus comparing the highlighted columns,

A	B	$(A \implies B) \iff (\neg B \implies \neg A)$
T	T	**T**
T	F	**T**
F	T	**T**
F	F	**T**

We have proved that

$$(A \implies B) \iff (\neg B \implies \neg A)$$

is always true. □

This proposition and its proof show that an implication is equivalent to its contrapositive. To give a **proof by contraposition** of the implication $A \implies B$, we give a direct proof of the contrapositive, i.e. we assume that B is false and we deduce that A must also be false.

Example 1.2.7

Use a proof by contraposition to show that, if n is an integer for which n^2 is even, then n is even.

Solution.
Let n be an integer and let P be the statement "if n^2 is even, then n is even". The contrapositive of P is "if n is not even, then n^2 is not even". From Proposition 1.2.2, we know that an integer is either even or odd. So the contrapositive of P is "if n is odd, then n^2 is odd".

Recall from Definition 1.2.1, that an integer n is odd if there exists an integer m such that $n = 2m+1$. Thus $n^2 = (2m+1)^2 = 4m^2+4m+1 = 2(2m^2+2m)+1 = 2t+1$, where we introduce t to denote the quantity $2m^2+2m$; this value is a sum of products of integers, and so t is an integer. Thus, n^2 is of the form $2t+1$ for some integer t, and hence is odd by definition.

Exercise 1.2.8

Let n be an integer. Prove the following by contraposition:

$$(n+3 \text{ is odd}) \implies (n \text{ is even})$$

1.2.3 Proof by contradiction

There is another common method of proof which, at first glance, looks similar to proof by contraposition. It is based on another logical equivalence, which we now state and prove.

Proposition 1.2.9

For every statement A, we have

$$(\neg A \implies \mathbf{F}) \iff A.$$

Proof. As earlier, we can use a truth table, and compare the highlighted columns:

A	$\neg A$	$\neg A \implies \mathbf{F}$	$(\neg A \implies \mathbf{F}) \iff A$
T	**F**	**T**	**T**
F	**T**	**F**	**T**

□

So, to prove that A is true, we **assume** that A is false, and then derive something false (a contradiction). This is called a **proof by contradiction**.

Example 1.2.10

Use proof by contradiction to show that the number 7 is odd.

Proof. Let A denote the statement "the number 7 is odd". Hence, $\neg A$ is the statement "the number 7 is even". We now **assume** that A is false, so $\neg A$ is true, and aim to derive a contradiction. According to Definition 1.2.1, this means that we can write $7 = 2m$, for some integer m. However, then we must have $m = 7/2 = 3\frac{1}{2}$, which is not an integer! By contradiction (Proposition 1.2.9), A is true, that is 7 is odd. □

The following example is very similar to Example 1.2.10 but the statement involves an implication. In such cases, the proof by contradiction uses a similar logic to that of a proof by contraposition (compare the assumptions for proof below with your answer for Exercise 1.2.8). On the other hand, the complete proofs are very different.

Example 1.2.11

Let n be an integer. Prove that if $n + 3$ is odd, then n is even.

Proof. Let A be the statement that "$n + 3$ is odd" nad let B be the statement "n is even". We want to prove that $A \implies B$. For a proof by contradiction, we assume the opposite of what we want to prove. That is, we **assume** that $A \implies B$ is false, and aim to derive a contradiction. From the truth table on page 5, we know that this only occurs if A is true and B is false. Hence, we **assume** that $n + 3$ is odd **and** that n is odd. By definition, since $n + 3$ is odd, there exists an integer m such that $n + 3 = 2m + 1$. Since we also assume that n is odd, there exists an integer k such that $n = 2k + 1$. It then follows that $2m+1 = n+3 = (2k+1)+3 = 2k+4$ which implies that $k - m = \frac{3}{2}$. But m and k are both integers, and so $k - m$ is also an integer — but this is false, since $\frac{3}{2}$ is not an integer. This is a contradiction. □

Remark 1.2.12

Note that in our solution to Example 1.2.11, to prove that $A \implies B$ by contradiction, we assumed that A is true, B is false and then derived a contradiction. This is the general strategy to prove an implication by contradiction.

1.2.4 Proof by double implication

We are often interested in logical equivalences. We often prove an equivalence like $A \iff B$ ("A is true if and only if B is true") by proving both $A \implies B$ ("if A is true, then B is true"; or, equivalently, "A is true only if B is true") and $B \implies A$ ("B is true if A is true"). We now state formally the property of $\iff$ that makes this technique valid.

Proposition 1.2.13

For every pair of statements A and B, we have

$$(A \iff B) \iff ((A \implies B) \wedge (B \implies A)).$$

Proof. As earlier, this can be proved with a truth table. We leave it as an exercise. □

Example 1.2.14

Let n be an integer, let A be the statement "n is even" and let B be the statement "n^2 is even". In Example 1.2.4, we proved $A \implies B$, while in Example 1.2.7, we proved $B \implies A$. By Proposition 1.2.13, it follows that $A \iff B$ that is, "n is even if and only if n^2 is even".

Exercise 1.2.15

Let n be an integer. Prove the equivalence:

$$(n + 3 \text{ is odd}) \iff (n \text{ is even})$$

1.3 Sets

1.3.1 Basic definitions

Definition 1.3.1

*A **set** is a collection of objects, called the **elements** of the set. We write $x \in A$ if the object x is an element of the set A, otherwise, we write $x \notin A$.*

Some examples of sets:

- The "set of all elephants in Africa".
- $A := \{a, b, c, d, e\}$. A is the set whose elements are precisely a, b, c, d and e.
- The set $\mathbb{N} := \{0, 1, 2, \ldots\}$ of **natural numbers** (in MATHS 120 the set $\mathbb{N}$ contains the element 0.)
- The set $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ of **integers**.
- The **empty set** $\emptyset$, also denoted $\{\}$, that contains no elements.

There are a few ways to define a set:

Enumeration. In the list above, we defined several sets A, $\mathbb{N}$, and $\mathbb{Z}$ by listing ('enumerating') the elements of the set inside braces.

Set-builder notation. This method involves taking a set which we have already defined and then giving a rule to decide whether elements of the existing set should be part of the new set. For instance, suppose we wish to create a set X consisting of all the natural numbers which are at least 5 and at most 17. Here, our existing set is $\mathbb{N}$ and our rule is "if $n \in \mathbb{N}$, then n is in our new set if $5 \leq n \leq 17$". We write this symbolically using **set-builder notation**: our new set is $X := \{n \in \mathbb{N} \mid 5 \leq n \leq 17\}$. Another set defined in this way is $Y := \{n \in \mathbb{N} \mid n \text{ is odd and } 1 \leq n \leq 17\}$.

Using an indexing set. This method involves giving an existing set (the **indexing set**) together with a rule that gives, for each element of the old set, a new object; the new set is then the set of all the elements produced by this rule. For instance, we can define a set Z to be the set of all numbers that are of the form $2n - 1$, where n is a natural number. In set-builder notation, the new set is written as follows: $Z := \{2n - 1 \mid n \in \mathbb{N}\}$. Another example is the set $\{3n \mid n \in \{1, 2, 3, 4, 5\}\}$.

We can combine set-builder notation and indexing notation in complex ways. For instance, the set of all even numbers which are at least 3 and at most 7 is the set $\{\, 2n \mid n \in \mathbb{N},\ 3 \leq 2n \leq 7 \,\}$.

Definition 1.3.2

*The **cardinality** (or, more casually, the **size**) of a set S is the number of distinct elements in S. This number is written as $|S|$, and can be either be a natural number or 'infinity' (denoted by the symbol ∞). If $|S| \in \mathbb{N}$, then S is called a **finite** set. If S has infinitely many elements then we call it an **infinite** set.*

We will be able to formulate a more precise definition of cardinality later; see Remark 1.4.20. For the purposes of this course, though, the definition here suffices.

Example 1.3.3

$\{1, 2, 5\}$ is a finite set since its cardinality is $|\{|1, 2, 5\} = 3$. The sets $\mathbb{N}$ and $\mathbb{Z}$ are infinite sets.

Definition 1.3.4

*A **subset** of a set A is a set S with the property that every element of S is also an element of A. We write this $S \subseteq A$; so $S \subseteq A$ is shorthand for the statement* $(x \in S) \implies (x \in A)$.

Example 1.3.5

We have that $\mathbb{N} \subseteq \mathbb{Z}$.

Example 1.3.6

For every set X, we have that $X \subseteq X$ and $\emptyset \subseteq X$.

Warning.
Do not mix up $x \in A$ and $X \subseteq A$. This is illustrated by the next example.

Example 1.3.7

Let $X := \{0, 1, 2, 3, 4\}$. Then the following properties hold:

- $\emptyset \subseteq X$
- $\emptyset \notin X$
- $\{4\} \subseteq X$
- $\{4\} \notin X$.

On the other hand, let $Y := \{\emptyset, 1, 2, 3, \{4\}\}$. Then:

- $\emptyset \subseteq Y$ *(similar to X)*
- $\emptyset \in Y$ *(different to X)*
- $\{4\} \not\subseteq Y$ *(different to X)*
- $\{4\} \in Y$ *(different to X).*

Proposition 1.3.8: Transitivity of set inclusion

Let A, B, C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof. Suppose $x \in A$. Then $x \in B$, because $A \subseteq B$. But $B \subseteq C$, so $x \in C$. Thus $x \in A$ implies that $x \in C$. So $A \subseteq C$. □

Definition 1.3.9

Two sets A and B are ***equal*** *if they have exactly the same elements. We write this as $A = B$; this is shorthand for the logical statement $(x \in A) \iff (x \in B)$.*

Example 1.3.10

- $\{1, 2, 3\} = \{3, 3, 2, 1\} = \{\, x \in \mathbb{N} \mid 1 \leq x \leq 3 \,\}$
- $\{\emptyset, a, b, c\} \neq \{a, b, c\}$

One way to prove that $A = B$ is to prove $A \subseteq B$ and $B \subseteq A$. This is sometimes called a proof by **double inclusion**.

Example 1.3.11

If $A = \{2n + 1 \mid n \in \mathbb{Z}\}$ and $B = \{2n + 7 \mid n \in \mathbb{Z}\}$, then $A = B$.

Indeed, let $a \in A$, i.e. $a = 2n + 1$ for some $n \in \mathbb{Z}$. Then $a = 2(n - 3) + 7 = 2n' + 7$ with $n' = n - 3 \in \mathbb{Z}$ and hence $a \in B$. So $A \subseteq B$. Similarly one can show that $B \subseteq A$.

1.3.2 Union, intersection, and set difference

Just like we have symbols (connectives) which allow the building of complex statements from simpler ones, we have constructions which allow us to build more complex set structures from simpler ones.

Definition 1.3.12

Let A and B be sets. The ***union*** *of A and B is the set*

$$A \cup B := \{\, x \mid x \in A \text{ or } x \in B \,\}.$$

The ***intersection*** *of A and B is the set*

$$A \cap B := \{\, x \mid x \in A \text{ and } x \in B \,\}.$$

The ***difference*** *of A and B is the set*

$$A \setminus B := \{\, x \mid x \in A \text{ and } x \notin B \,\}.$$

Example 1.3.13

Let $A := \{a, b, c, d, e, f, g\}$ *and* $B := \{a, e, i, o, u\}$. *Find* $A \cup B$, $A \cap B$, $A \setminus B$ *and* $B \setminus A$.

Solution.

- $A \cup B = \{a, b, c, d, e, f, g, i, o, u\}$,
- $A \cap B = \{a, e\}$,
- $A \setminus B = \{b, c, d, f, g\}$ and
- $B \setminus A = \{i, o, u\}$.

We may use **Venn diagrams** to illustrate these; see Figure 1.1 on the next page.

Many properties of the set operations follow directly from the logical laws we proved earlier in the course, as Proposition 1.1.1 and in Exercise 1.1.2.

Proposition 1.3.14: Properties of set operations

Let A, B *and* C *be sets. The following holds:*

1. $A \cup B = B \cup A$; *(Commutativity of union)*
2. $A \cap B = B \cap A$; *(Commutativity of intersection)*
3. $(A \cup B) \cup C = A \cup (B \cup C)$; *(Associativity of union)*
4. $(A \cap B) \cap C = A \cap (B \cap C)$; *(Associativity of intersection)*
5. $A \subseteq A \cup B$;
6. $A \cap B \subseteq A$.

Proof. We will prove properties (1), (4), and (5), and leave the others as an exercise.

1. Observe that "$A \cup B = B \cup A$" is equivalent to the statement "$(x \in A \cup B) \iff (x \in B \cup A)$". Now note, "$x \in A \cup B$" is equivalent (by definition of union) to the statement "$(x \in A) \vee (x \in B)$". We now use that "$P \vee Q \iff Q \vee P$" (this statement is proved using a truth table), with P the statement "$x \in A$" and Q the statement "$x \in B$", to see that "$(x \in A) \vee (x \in B)$" is equivalent to "$(x \in B) \vee (x \in A)$". Using the definition of union again, "$(x \in B) \vee (x \in A)$" is equivalent to "$x \in B \cup A$". This shows that "$(x \in A \cup B) \iff (x \in B \cup A)$" as desired.

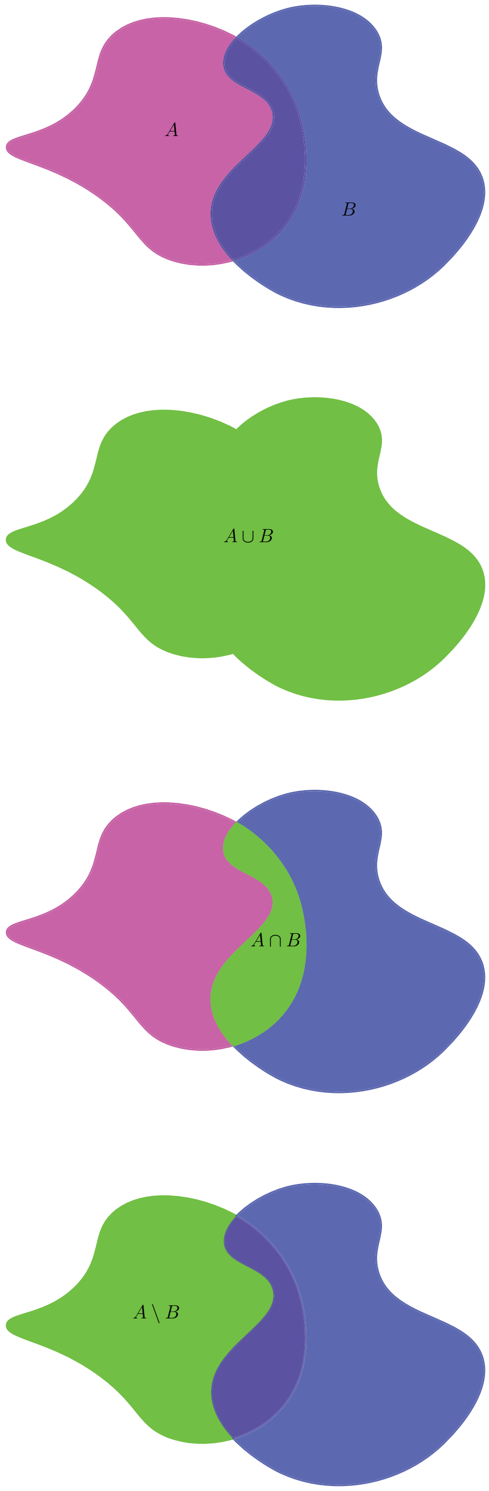


Figure 1.1: Venn diagrams for the set operations.

4. The statement "$(A \cap B) \cap C = A \cap (B \cap C)$" is equivalent to "$(x \in (A \cap B) \cap C) \iff (x \in A \cap (B \cap C))$". Let P, Q, and R denote the statements "$x \in A$", "$x \in B$", and "$x \in C$" respectively. By definition of the intersection, "$x \in (A \cap B) \cap C$" is equivalent to "$(P \wedge Q) \wedge R$" and "$x \in A \cap (B \cap C)$" is equivalent to "$P \wedge (Q \wedge R)$"; but "$((P \wedge Q) \wedge R) \iff (P \wedge (Q \wedge R))$" by the associative law for logical or, and hence "$(x \in (A \cap B) \cap C) \iff (x \in A \cap (B \cap C))$".

5. Let P denote the statement "$x \in A$", and let Q denote the statement "$x \in B$". Then "$A \subseteq A \cup B$" is equivalent to "$P \implies (P \vee Q)$", and using a truth table we see that this final statement is always true. □

Proposition 1.3.15: Distributivity of union over intersection

If A, B and C are sets, then

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Proof. We use the distributivity law for logical statements.

$$\begin{aligned} x \in A \cup (B \cap C) &\iff (x \in A) \vee (x \in B \cap C) \\ &\iff (x \in A) \vee ((x \in B) \wedge (x \in C)) \\ &\iff ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C)) \\ &\iff (x \in A \cup B) \wedge (x \in A \cup C) \\ &\iff x \in (A \cup B) \cap (A \cup C) \end{aligned}$$ □

Proposition 1.3.16: Distributivity of intersection over union

If A, B and C are sets, then

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Proof. Exercise. □

Definition 1.3.17

*Given a set U (which we call a **universal set**) and a subset $S \subseteq U$, we define the **complement of** S **in** U to be*

$$S^{\mathcal{C}}_U := U \setminus S = \{x \in U \mid x \notin S\}.$$

*If the universal set U is clear from the context, we may simply write $S^{\mathcal{C}}$ and refer to it as the **complement** of S.*

Proposition 1.3.18: De Morgan's Laws

For any subsets $A \subseteq U$ and $B \subseteq U$, we have the equality

$$(A \cup B)^{\mathcal{C}}_U = A^{\mathcal{C}}_U \cap B^{\mathcal{C}}_U \quad \text{and} \quad (A \cap B)^{\mathcal{C}}_U = A^{\mathcal{C}}_U \cup B^{\mathcal{C}}_U.$$

Proof. Exercise. □

Note the strong parallel between Propositions 1.3.15, 1.3.16, and 1.3.18, and the earlier Proposition 1.1.1 and Exercise 1.1.2. For every logical law, we get a set-theoretic law. This is because we have a dictionary of sorts: statements correspond to set membership statements, implication to set inclusion, logical equivalence to set equality, and negation to set complements. Despite this strong analogy, it is important to remember the difference between statements (which can be true or false), and sets (which are collections of objects).

Warning.
We can only write truth tables for statements: when proving propositions about sets using truth tables, the column headers should be statements like "$x \in A \cup B$", not names of sets. You cannot assign a truth value to the set $A \cup B$, only to the statement that a given object is an element of $A \cup B$.

Example 1.3.19

Let A and B be sets. Prove that $A \cap B \subseteq A \cup B$.

Solution.
By part (6) of Proposition 1.3.14, $A \cap B \subseteq A$; by part (5) of the same proposition, $A \subseteq A \cup B$; and by transitivity of set inclusion (Proposition 1.3.8) we are done.

Example 1.3.20

Let X be a set and let $A, B, C \subseteq X$. Suppose that $A \cap B = A \cap C$ and that $A^{\mathcal{C}}_X \cap B = A^{\mathcal{C}}_X \cap C$. Prove that $B = C$.

Solution.
Let $b \in B$. If $b \in A$, then $b \in A \cap B = A \cap C$ and hence $b \in C$. If $b \in A^{\mathcal{C}}_X$ then $b \in A^{\mathcal{C}}_X \cap B = A^{\mathcal{C}}_X \cap C$ and hence also $b \in C$. So $B \subseteq C$.

A similar proof yields $C \subseteq B$ and thus $B = C$.

Exercise 1.3.21

Let A and B be sets. Show that if $A = A \cup B$, then $B \subseteq A$; similarly, show that if $A = A \cap B$, then $A \subseteq B$.

1.3.3 Power sets and Cartesian products

Definition 1.3.22

The collection of all subsets of a set A is called the ***power set*** *of A, written $\mathcal{P}(A)$.*

In other words, $S \in \mathcal{P}(A)$ if and only if $S \subseteq A$.

Example 1.3.23

If $A = \{1, 2, 3\}$, then

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Observe that in this example, $|\mathcal{P}(A)|$ is a lot larger than $|A|$. This is generally the case for a finite set A; see Example 1.4.40 on page 38.

Example 1.3.24

Let A and B be sets. Show that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

Solution.
Let $S \in \mathcal{P}(A \cap B)$. Then $S \subseteq A \cap B$; since $A \cap B$ is a subset of both A and B, we have that $S \subseteq A$ and $S \subseteq B$. Thus $S \in \mathcal{P}(A)$ and $S \in \mathcal{P}(B)$; i.e. $S \in \mathcal{P}(A) \cap \mathcal{P}(B)$. This shows that $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.

Conversely, let $S \in \mathcal{P}(A) \cap \mathcal{P}(B)$; then $S \subseteq A$ and $S \subseteq B$, so each element of S lies in both A and B and thus $S \subseteq A \cap B$; i.e. $S \in \mathcal{P}(A \cap B)$. This shows that $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.

Definition 1.3.25

The ***Cartesian product*** *of sets A and B is the set of ordered pairs*

$$A \times B \coloneqq \{(a, b) \mid a \in A,\ b \in B\}$$

We often write A^2 for $A \times A$.

Remark 1.3.26

More generally, we define the Cartesian product of sets A_1, A_2, $\ldots$, A_n to be the set of ordered n-tuples

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

Given an n-tuple $(a_1, \ldots, a_n)$ for each $1 \leq i \leq n$, we call a_i its ith ***component****. For any set A, we will often write A^n for the n-fold product of A with itself.*

Given two n-tuples $(a_1, \ldots, a_n), (a'_1, \ldots, a'_n) \in A_1 \times \cdots \times A_n$, note that they are equal if and only if all of their respective components are equal, i.e.,

$$(a_1, \ldots, a_n) = (a'_1, \ldots, a'_n) \iff a_1 = a'_1 \text{ and } \cdots \text{ and } a_n = a'_n.$$

Example 1.3.27

Given $A := \{1, 3\}$ and $B := \{a, b\}$, we have

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

Example 1.3.28

The set $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$ is the set of all pairs of integers. We can view this as the set of coordinates of ***lattice points*** *in the plane; see Figure 1.2.*

Exercise 1.3.29

Let A and B be finite sets, with $|A| = m$ and $|B| = n$. Show that $|A \times B| = mn$.

1.4 Functions

1.4.1 Basic definitions

We often have relationships between different sets that are of a different nature than just the relationships of inclusion and equality. For instance, consider the set of even numbers $E = \{\ldots, -2, 0, 2, 4, 6, \ldots\}$; this is a

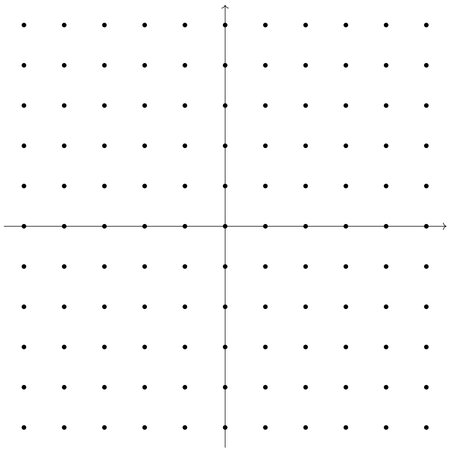


Figure 1.2: The elements of $\mathbb{Z}^2$ correspond to coordinates of lattice points.

subset of $\mathbb{Z}$ which contains exactly those elements which are obtained by taking elements of $\mathbb{Z}$ and multiplying by 2. (This is the same as saying that $E = \{2n \mid n \in \mathbb{Z}\}$.) We have a rule which, given an element of $\mathbb{Z}$, gives us another number in E in a predictable way.

A rule like this is called a function. We now give a precise definition.

Definition 1.4.1

A ***function*** f *is defined by the following data:*

- *a set* X *called its* ***domain****,*
- *a set* Y *called its* ***codomain****,*
- *a* ***rule*** *which, to every* $x \in X$*, assigns a unique element* $f(x) \in Y$*, called the* ***image of*** x ***under*** f*. We also sometimes say that* f ***maps*** x *to* $f(x)$*.*

We often summarize this data by writing

$$\begin{aligned} f: \quad X &\longrightarrow Y \\ x &\longmapsto f(x). \end{aligned}$$

A function is not the same thing as a formula: whenever we have a specific rule that produces a single element of the codomain for every element of the domain, we have a function.

Example 1.4.2

Here are some examples of functions.

1. *The function $f : \mathbb{Z} \to \mathbb{N}$ given by the rule $f(x) := x^2$. We can summarize this by writing*

$$\begin{aligned} f :\ \mathbb{Z} &\longrightarrow \mathbb{N} \\ x &\longmapsto x^2. \end{aligned}$$

2. *The function g with domain "the set of English words" and codomain "the set of letters in the English alphabet", defined to map every word to its first letter. For example, $g(\text{dolphin}) = \text{d}$.*

3. *Let $X := \{1, 2, 3\}$ and $Y := \{a, b, c, d\}$; define $h : X \to Y$ by the following rule:*

$$\begin{tikzcd}
1 \arrow[r, mapsto] & a \\
2 \arrow[rdd, mapsto] & b \\
3 \arrow[ru, mapsto] & c \\
 & d
\end{tikzcd}$$

Remark 1.4.3

Sometimes, one may encounter an expression that seems to define a function but really does not. There are various ways this can happen. For example,

$$\begin{aligned} f :\ \mathbb{N} &\longrightarrow \mathbb{N} \\ x &\longmapsto x - 1 \end{aligned}$$

may superficially seem to define a function, but it does not. This is because $f(0) = 0 - 1 = -1$ does not belong to the codomain $\mathbb{N}$.

*Another example is the "function" $g : X \to Y$ with $X := \{1, 2, 3\}$ and $Y := \{2, 3, 4\}$, defined by the rule that, for every $x \in X$, $g(x)$ is "the" element of Y that is even and such that $g(x) > x$. This is **not a function**, because $1 \in X$ but $g(1)$ is not uniquely defined: it could be either 2 or 4. You may be tempted to map 1 to the subset $\{2, 4\}$, but this is not an element of the codomain Y! We will see more examples later.*

Definition 1.4.4

Let $f : X \to Y$ and $g : A \to B$ be functions. We say that f and g are ***equal*** *and write $f = g$ if and only if*

1. $X = A$;
2. $Y = B$;
3. *for every $x \in X$, $f(x) = g(x)$.*

In other words, two functions are equal if and only if they have the same domain, the same codomain and every element of their common domain has the same image.

Example 1.4.5

For each of the following pairs of functions, determine whether they are equal.

1. (a) $f_1 : \mathbb{Z} \to \mathbb{Z}$ *given by* $f_1(x) = x^2$.
   (b) $f_2 : \mathbb{Z} \to \mathbb{N}$ *given by* $f_2(x) = x^2$.
2. (a) $g_1 : \{0, 1\} \to \{0, 1\}$ *given by* $g_1(x) = x^2$.
   (b) $g_2 : \{0, 1\} \to \{0, 1\}$ *given by* $g_2(x) = x$.

Solution.

1. f_1 and f_2 do not have the same codomain, so $f_1 \neq f_2$.

2. g_1 and g_2 have the same domain, the same codomain and $g_1(0) = 0 = g_2(0)$ and $g_2(1) = 1 = g_2(1)$ so $g_1 = g_2$.

Definition 1.4.6

We sometimes denote the set of <u>all</u> possible functions from a set X to a set Y by Y^X.

Exercise 1.4.7

Let $X := \{a, b, c\}$ and $Y := \{1, 2\}$. Write down all possible functions with domain X and codomain Y. What is the cardinality $\left|Y^X\right|$?

Exercise 1.4.8

Let X and Y be finite sets. Prove that the cardinality of the set of all functions from X to Y is given by the formula

$$\left|Y^X\right| = |Y|^{|X|}.$$

(Hint: when inventing the rule for a function $f : X \to Y$, for each input value $x \in X$, how many possible choices to do you have for the output value $f(x) \in Y$?)

Definition 1.4.9

Given a function $f : X \to Y$ and a subset $S \subseteq X$, we write

$$f(S) := \{\, f(s) \mid s \in S \,\}$$

and call this ***image*** *of S under f.*

In the special case where S to be the entire domain X, then we call $f(X)$ the ***range****) of f.*

Remark 1.4.10

Note that $f(S)$ is a subset *of the codomain Y,* not *an element of this set.*

Example 1.4.11

Define a function $f : \mathbb{N} \to \mathbb{Z}$ by the rule $f(x) = -x$. What are the domain, codomain, and range of f?

Solution.
The domain of f is $\mathbb{N}$, the codomain is $\mathbb{Z}$, and the range of f is the set

$$\{\, 0 \,\} \cup \mathbb{Z} \setminus \mathbb{N} = \{0, -1, -2, \ldots\}.$$

Exercise 1.4.12

Let $X = \{1, 2, 3\}$ and $Y = \{a, b\}$. Define two (different) functions with domain X and codomain Y that do not have the same range.

Can you do the same for two functions with domain Y and codomain X? If yes, define them; if no, explain why not.

1.4.2 Injective, surjective and bijective functions

Definition 1.4.13

A function $f : X \to Y$ is called

- **injective** *if, for every $x, x' \in X$, $f(x) = f(x')$ implies $x = x'$;*
- **surjective** *if, for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$;*
- **bijective** *if it is injective and surjective.*

Example 1.4.14

- *Let $X = \{1, 2, 3\}$ and $Y = \{a, b, c\}$, then:*
  - *The function from X to Y given by $f(1) = b, f(2) = c, f(3) = a$ is bijective.*
  - *The function from X to Y given by $f(1) = f(2) = b, f(3) = c$ is neither injective nor surjective.*
- *If $X = \{1, 2, 3\}$ and $Y = \{a, b, c, d\}$, then the function from X to Y given by $f(1) = b, f(2) = c, f(3) = a$ is injective but not surjective.*
- *If $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c\}$, then the function from X to Y given by $f(1) = b, f(2) = c, f(3) = a, f(4) = b$ is surjective but not injective.*

Exercise 1.4.15

Prove that a function $f : X \to Y$ is surjective if and only if $f(X) = Y$.

Example 1.4.16

Let $f : \mathbb{Z}^2 \to \mathbb{Z}$ where $f(a, b) = a + b$. Is f injective? Is f surjective?

Solution.
f is not injective since, for example, $f(0, 0) = 0 = f(1, -1)$. f is surjective since, for every $y \in \mathbb{Z}$, we have $(y, 0) \in \mathbb{Z}^2$ and $f(y, 0) = y$.

Example 1.4.17

Let $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ where $f(a,b) = (a+b, 2a-3b)$. Show that f is injective but not surjective.

Solution.

- We first show that f is injective. Let $(a,b),(c,d) \in \mathbb{Z}^2$ such that $f(a,b) = f(c,d)$. We want to show that $(a,b) = (c,d)$. Since $f(a,b) = f(c,d)$, we have $(a+b, 2a-3b) = (c+d, 2c-3d)$ and hence

$$\begin{aligned} a+b &= c+d \\ 2a-3b &= 2c-3d. \end{aligned}$$

  By adding three times the first equation to the second one, we get $5a = 5c$ hence $a = c$ and $b = d$. It follows that $(a,b) = (c,d)$ and f is injective.

- We now consider surjectivity of f. Let (x,y) be an element of the codomain $\mathbb{Z}^2$. We must find (a,b) in the domain $\mathbb{Z}^2$ such that $f(a,b) = (x,y)$. Using the definition of f, this is $(a+b, 2a-3b) = (x,y)$, in other words:

$$\begin{aligned} a+b &= x \\ 2a-3b &= y \end{aligned}$$

  Adding three times the first equation to the second one, we get $5a = 3x+y$. This does not always have a solution. For example, if $x = 0$ and $y = 1$, then this becomes $5a = 1$, which has no solution with $a \in \mathbb{Z}$. It follows that f is not surjective.

Proposition 1.4.18: Functions on finite sets

Let X and Y be finite sets, with $|X| = n$ and $|Y| = m$. Let f be a function with domain X and codomain Y.

1. *If $n > m$, then f is not injective.*
2. *If $n < m$, then f is not surjective.*
3. *If $n = m$, then f is injective if and only if it is surjective.*

Proof. Write $X = \{x_1, \ldots, x_n\}$, with $x_1, \ldots, x_n$ all distinct.

1. Let $n > m$. Suppose by contradiction that f is injective. Then each input value must have a distinct output value, so $|f(X)| = |\{f(x_1), \ldots, f(x_n)\}| = n$. But this contradicts the assumption that the codomain has fewer than n elements.

2. Since $n < m$, $f(X) = \{f(x_1), \dots, f(x_n)\}$ must be a proper subset of Y, so f is not surjective.

3. We assume $n = m$, and prove the conclusion by double implication. First, if f is injective, then the elements $f(x_1), \dots, f(x_n)$ are all distinct, so $|f(X)| = |\{f(x_1), \dots, f(x_n)\}| = n = m$ and hence $f(X) = Y$ and f is surjective. Conversely, if f is surjective, then $Y = f(X) = \{f(x_1), \dots, f(x_n)\}$. Since $|Y| = m = n$, the elements $f(x_1), \dots, f(x_n)$ must all be distinct and so f is injective. □

Exercise 1.4.19

Use Proposition 1.4.18 parts (1) and (2) to deduce that if X and Y are finite sets, and if $f : X \to Y$ is a bijection, then $|X| = |Y|$.

Remark 1.4.20

*Earlier we remarked that it is possible to make the definition of cardinality (Definition 1.3.2) more precise. We do this by using the hypotheses and conclusions of Proposition 1.4.18 and Exercise 1.4.19 as definitions. First, we say that two sets A and B have **equal cardinality** and write $|A| = |B|$ if there is a bijective function $f : A \to B$; this is a reversal of Exercise 1.4.19. If a set A has equal cardinality to the set $\{1, 2, \dots, n\}$ (where n is a positive integer), then we say that A has cardinality (or size) n and write $|A| = n$. If there exists some positive integer n with $|A| = n$, then we call A **finite**; otherwise we call A **infinite**.*

Part (1) of Proposition 1.4.18 is sometimes called the **Pigeonhole Principle**, in analogy to the following situation: we have a set P of pigeonholes, and a set X of objects. An assignment of objects to pigeonholes corresponds to a function $f : X \to P$: namely, we set $f(x)$ to the pigeonhole into which we place the object x. The function f is not injective if there are two objects $x, y \in X$ such that $f(x) = f(y)$; in other words, if the objects x and y are placed into the same pigeonhole. The Pigeonhole Principle states that, if $|X| > |P|$, then *no* function with domain X and codomain P is injective: i.e., every assignment of objects to pigeonholes must end up with at least one pigeonhole containing more than one object.

Example 1.4.21

Suppose 5 pairs of socks, each pair a different colour, lie in a drawer. You are not allowed to look into the drawer; how many socks do you need to pull out to make sure that you have pulled out at least one same-coloured pair?

Solution.
We apply the Pigeonhole Principle. Let S be the set of socks in the drawer, and let C be the set of colours (so $|S| = 10$, and $|C| = 5$). For every $A \in \mathcal{P}(S)$, define a function $\chi_A : A \to C$ by $f(a) =$ the colour of a for $a \in A$. By the Pigeonhole Principle, for all sets $A \in \mathcal{P}(S)$ such that $|A| > 5$, the function χ_A cannot be injective; so if we pick out a set A of six socks, the function assigning each sock in A a colour is not injective and there must be two socks of the same colour. On the other hand, for every $n \leq 5$ there is a possible set $A \in \mathcal{P}(S)$ such that χ_A *is* injective; so to gurantee getting a pair of socks we must pull out at least six socks.

We have now seen that existence of surjections and injections is related to size of sets. This allows us to answer the following natural question: we know that $\mathbb{Z}$ is infinite, but are there 'larger sets' than $\mathbb{Z}$? We now give **Cantor's Theorem**, which states that whenever we have a set A we can always construct a set A' which is strictly larger than A, in the sense that there is no surjective function from A to A'. In fact, we can take the set A' to be the powerset of A, as in Definition 1.3.22.

Example 1.4.22: Cantor's Theorem

Let A be a set; show that there is no surjective function $f : A \to \mathcal{P}(A)$.

Solution.
Suppose for the sake of contradiction that there is a surjection $f : A \to \mathcal{P}(A)$. Then, for all $a \in A$, we have that $f(a) \subseteq A$. For a given $a \in A$, there are two possibilities: either $a \in f(a)$, or $a \notin f(a)$. Define a set $C = \{a \in A : a \notin f(a)\}$. This is a subset of A; i.e. $C \in \mathcal{P}(A)$. Since f is surjective, there exists $c \in A$ such that $f(c) = C$. Now observe that if $c \in f(c)$, then $c \notin C = f(c)$ by definition of C; and if $c \notin f(c)$, then $c \in f(c)$. This is a contradiction, so the initial assumption that a surjection existed was false.

Thus we have an infinitely ascending chain of infinite sets, each strictly larger than the last: $\mathbb{Z} \subseteq \mathcal{P}(\mathbb{Z}) \subseteq \mathcal{P}(\mathcal{P}(\mathbb{Z})) \subseteq \cdots$!

1.4.3 Function composition

A function is a rule for producing a specific object when given an object as input. We now consider the application of two such rules, one after the other.

Definition 1.4.23

If $f : X \to Y$ and $g : Y \to Z$ are functions, then the ***composition*** *of g and f is the function $g \circ f$ defined as follows:*

$$\begin{aligned} g \circ f &: X \to Z \\ (g \circ f)(x) &= g(f(x)). \end{aligned}$$

If the domain of g is not equal to the codomain of f, then $g \circ f$ is *not defined*!

Example 1.4.24

If $f : \mathbb{Z} \to \mathbb{Z}$ with $f(x) = x + 1$ and $g : \mathbb{Z} \to \mathbb{Z}$ with $g(x) = 2x$, then

$$\begin{aligned} g \circ f &: \mathbb{Z} \to \mathbb{Z} \\ (g \circ f)(x) &= 2x + 2 \end{aligned}$$

while

$$\begin{aligned} f \circ g &: \mathbb{Z} \to \mathbb{Z} \\ (f \circ g)(x) &= 2x + 1. \end{aligned}$$

Note that composition of functions is generally *not commutative*. In other words, we may *not* have $f \circ g = g \circ f$, as can be seen in the example above. On the other hand, we do have the following:

Proposition 1.4.25: Composition is associative

If $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are functions, then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Proof. Note that the domain of $h \circ (g \circ f)$ is X, while its codomain is W. Similarly for $(h \circ g) \circ f$. Finally, for $x \in X$, we have

$$\begin{aligned} (h \circ (g \circ f))(x) &= h((g \circ f)(x)) \\ &= h(g(f(x))) \end{aligned}$$

$$\begin{aligned} &= (h \circ g)(f(x)) \\ &= ((h \circ g) \circ f)(x). \end{aligned}$$

This shows that $h \circ (g \circ f) = (h \circ g) \circ f$. □

This property is called **associativity** of composition of functions. It allows us to omit parentheses and write simply $h \circ g \circ f$. Using induction (see Section 1.5), one can generalise it to expressions involving an arbitrary number of functions.

1.4.4 Identity and inverse functions

In some sense, the simplest possible rule for producing an object given an input object is the rule that says "just give the input back". While this is quite a boring rule, it turns out that the associated function (or rather, class of functions — one for each set) is of significant importance.

Definition 1.4.26

Let X be a set. The ***identity function*** id_X *on X is defined as follows:*

$$\begin{aligned} \mathrm{id}_X &: X \to X \\ \mathrm{id}_X(x) &= x. \end{aligned}$$

In other words, id_X maps every element of X to itself. Note that each set has its own identity function! (For example, $\mathrm{id}_{\mathbb{N}}$ is not equal to $\mathrm{id}_{\mathbb{Z}}$, as they have different domains.)

Proposition 1.4.27

For every function $f : X \to Y$, we have $f \circ \mathrm{id}_X = f$.

Proof. Since the identity id_X has X as both its domain and codomain, the composition $f \circ \mathrm{id}_X$ is well defined with domain X and codomain Y. Hence, $f \circ \mathrm{id}_X$ has the same domain and codomain as f. It remains to show that, for every $x \in X$, the image of x under $f \circ \mathrm{id}_X$ is also the same as the image of x under f. We have

$$(f \circ \mathrm{id}_X)(x) = f(\mathrm{id}_X(x)) = f(x).$$

Therefore, it follows from Definition 1.4.4 that $f \circ \mathrm{id}_X = f$. □

Exercise 1.4.28

Let $f : X \to Y$ be a function. Explain why $\mathrm{id}_X \circ f = f$ is not necessarily true.

Definition 1.4.29

If $f : X \to Y$ is a function, we say that a function $g : Y \to X$ is

- *a* ***left-inverse*** of f *if* $g \circ f = \mathrm{id}_X$,
- *a* ***right-inverse*** of f *if* $f \circ g = \mathrm{id}_Y$ *and*
- *an* ***inverse*** of f *if it is both a left- and right-inverse.*

Example 1.4.30

Consider the function

$$f : \mathbb{N} \to \mathbb{N}$$
$$f(x) = x + 1$$

Then the function

$$g : \mathbb{N} \to \mathbb{N}$$
$$g(0) = 0, g(x) = x - 1 \text{ for } x \geq 1$$

is a left-inverse for f.

It is not necessarily the case that a right-inverse is also a left-inverse, or vice versa.

Example 1.4.31

Define $f : \{a, b, c\} \to \{a, b\}$ by $f(a) = a, f(b) = b, f(c) = a$. *Define the function* $g : \{a, b\} \to \{a, b, c\}$ by $g(a) = a, g(b) = b$. *Then* g *is a right-inverse for* f. *It is not a left-inverse for* f.

Example 1.4.32

The function

$$g : \mathbb{Z} \to \mathbb{Z}$$
$$g(x) = x - 1$$

is an inverse of the function

$$f : \mathbb{Z} \to \mathbb{Z}$$
$$f(x) = x + 1.$$

Example 1.4.33

Define a function $s : \mathbb{Z} \to \mathbb{Z}$ by $s(n) = n^2$ for all $n \in \mathbb{Z}$. Show that s has neither a right-inverse nor a left-inverse.

Solution.
Suppose $h : \mathbb{Z} \to \mathbb{Z}$ is a right-inverse for s; then in particular, $s(h(-1)) = -1$. But the square of every integer is positive, so there is no possible value for $h(-1)$ making this equality true.

Suppose now that $k : \mathbb{Z} \to \mathbb{Z}$ is a left-inverse for s; then $1 = k(s(1)) = k(1^2) = k((-1)^2) = k(s(-1)) = -1$, which is a contradiction.

Exercise 1.4.34

Show that:

1. *The function $s : \mathbb{N} \to \mathbb{N}$ defined by $s(n) = n^2$ for all $n \in \mathbb{N}$ has a left-inverse but not a right-inverse.*
2. *The function $f : \{1, 2, 3\} \to \{a, b, c, d\}$ defined by $f(1) = a$, $f(2) = d$, $f(3) = c$ has a left-inverse but not a right-inverse.*
3. *The function $g : \mathbb{Z} \to \{1\}$ given by $g(n) = 1$ for all $n \in \mathbb{Z}$ has a right-inverse but not a left-inverse.*
4. *There is an invertible function between the set $\{\, 2n \mid n \in \mathbb{Z} \,\}$ of even numbers, and the set $\{\, 2n+1 \mid n \in \mathbb{Z} \,\}$ of odd numbers.*
5. *Every function with domain $\{1, 2, 3, 4, 5\}$ and codomain $\mathbb{Z}$ is not invertible.*

Proposition 1.4.35

If f is a function with a right-inverse g and a left-inverse h, then $g = h$.

Proof. Let $f : X \to Y$, and let $g, h : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $h \circ f = \mathrm{id}_X$. We have $g = \mathrm{id}_X \circ g = h \circ f \circ g = h \circ \mathrm{id}_Y = h$. □

It follows from Proposition 1.4.35 that, if a function f has an inverse, then it is *unique*. In this case, we say that f is **invertible** and denote its inverse by f^{-1}.

Theorem 1.4.36

If f is an invertible function, then so is f^{-1} and $(f^{-1})^{-1} = f$.

Proof. If $f : X \to Y$ is invertible, then $f^{-1} : Y \to X$ exists. We have $f \circ f^{-1} = \mathrm{id}_Y$ and $f^{-1} \circ f = \mathrm{id}_X$. But this is also the definition for f^{-1} having an inverse, with f playing the role of the inverse. □

Theorem 1.4.37

Let $f : X \to Y$ and $g : Y \to Z$ be functions. If f and g are invertible, then $g \circ f$ is also invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. Since f and g are both invertible, $f^{-1} : Y \to X$ and $g^{-1} : Z \to Y$ exist. Hence, the composition $f^{-1} \circ g^{-1} : Z \to X$ is well defined. Using Propositions 1.4.25 and 1.4.27, we have

$$\begin{aligned}(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ f \circ f^{-1} \circ g^{-1} \\ &= g \circ (f \circ f^{-1}) \circ g^{-1} \\ &= g \circ \mathrm{id}_Y \circ g^{-1} \\ &= g \circ g^{-1} = \mathrm{id}_Z\end{aligned}$$

Using similar arguments, we also have $(f^{-1} \circ g^{-1}) \circ (g \circ f)$. Hence $g \circ f$ is invertible and its inverse is, indeed, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

Theorem 1.4.38

Let X be a non-empty set. A function $f : X \to Y$ is

1. *injective if and only if it has a left-inverse;*
2. *surjective if and only if it has a right-inverse;*
3. *bijective if and only if it has an inverse.*

Proof.

1. Suppose f is injective. Let $x_0 \in X$. We define $g : Y \to X$ by the following rule: if there is $x \in X$ such that $f(x) = y$, then there is a unique one, and we define $g(y) = x$. If there is no so such x, then we define $g(y) = x_0$. Now, for $x \in X$, we have $g(f(x)) = x$, so g is a left-inverse.

   Conversely, if f has a left-inverse g and $f(x) = f(y)$, then $x = g(f(x)) = g(f(y)) = y$, which proves that f is injective.

2. Suppose f is surjective. We define $g : Y \to X$ in the following way: for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$. We pick one of these x, and declare $g(y) = x$. (This actually uses the axiom of choice, but this is outside the scope of this course.) One then has $f(g(y)) = f(x) = y$, so g is a right-inverse for f.

   Conversely suppose g is a right-inverse for f. Then, for $y \in Y$, we have that $f(g(y)) = y$ so f is surjective.

3. Follows immediately from (a) and (b). □

Exercise 1.4.39

Let $\frac{1}{3}\mathbb{Z}$ denote the set $\{n/3 \mid n \in \mathbb{Z}\}$. Construct functions $f, g, h : \mathbb{Z} \to \frac{1}{3}\mathbb{Z}$ such that f has a left-inverse but no right-inverse, g has a right-inverse but no left-inverse, and h is invertible.

Example 1.4.40

Let A be a finite set, with $|A| = n$. Show that $\mathcal{P}(A)$ is finite, and that $|\mathcal{P}(A)| = 2^n$.

Solution.
We will show that there is a bijection between the set $\mathcal{P}(A)$, and the set X of binary sequences of length n (i.e. the set of objects of the form $(\beta_1, \dots, \beta_n)$ where each $\beta_i \in \{0, 1\}$). Suppose that $A = \{a_1, \dots, a_n\}$, where the a_i are all distinct. If $S \in \mathcal{P}(A)$, define $f(S)$ to be the binary sequence with a 1 in the ith position if $a_i \in S$, and with a 0 in the ith position if $a_i \notin S$. This defines a function $f : \mathcal{P}(A) \to X$. Conversely, define a function $g : X \to \mathcal{P}(A)$ as follows: if $(\beta_1, \dots, \beta_n) \in X$ is a binary sequence, then define $g((\beta_1, \dots, \beta_n))$ to be the subset of A which contains a_i if and only if $\beta_i = 1$. It is easy to see that $f \circ g = \mathrm{id}_X$ and that $g \circ f = \mathrm{id}_{\mathcal{P}(A)}$, so f is a bijection from X to $\mathcal{P}(A)$. Now note that there are 2^n possible binary sequences of length n and use the result of Exercise 1.4.19.

Exercise 1.4.41

Let A and B be finite sets, with $|A| = m$ and $|B| = n$. Let $F(A, B)$ be the set of functions with domain A and codomain B. Show that $F(A, B)$ is finite, and that $|F(A, B)| = n^m$.

1.5 Mathematical induction

The set $\mathbb{N}$ of natural numbers has the following very important property:

Axiom 1.5.1: Well-Ordering Principle

Every nonempty subset of $\mathbb{N}$ contains a smallest member.

Example 1.5.2

- *The smallest member of* $\{3, 7, 8\}$ *is* 3.
- *The smallest member of* $\mathbb{N}$ *is* 0.

Note that many other familiar sets do not have this property.

Example 1.5.3

- $\mathbb{Z}$ *does not have a smallest member.*
- *The set* $\{x \in \mathbb{R} \mid x > 0\}$ *of strictly positive real numbers does not have a smallest member.*

The Well-Ordering Principle is one of the defining properties of the natural numbers. We will not prove the Well-Ordering Principle. In fact, we will take it as an axiom, which means that we assume it to be true, and use it as a starting point to prove other results. The most important of these result is mathematical induction, which can be used to prove that some proposition $P(n)$ is true for all natural numbers n.

Theorem 1.5.4: Principle of Mathematical Induction (PMI)

Let $P(n)$ *be a sequence of statements with* $n \in \mathbb{N}$. *If*

- $P(0)$ *is true, and*
- *for every* $k \in \mathbb{N}$, *if* $P(k)$ *is true, then* $P(k+1)$ *is true,*

then $P(n)$ *is true for all* $n \in \mathbb{N}$.

Proof. We prove the theorem using the method of proof by contradiction, that is, we assume that the conclusion is false, that is there exists at least one $m \in \mathbb{N}$ for which $P(m)$ is false, and derive a contradiction. Let

$$S := \{m \in \mathbb{N} : P(m) \text{ is false}\} \subseteq \mathbb{N}.$$

As discussed earlier, we assume that $S \neq \emptyset$. By the Well-Ordering Principle, S has a smallest element, say s. Since we are given that $P(0)$ is true, we must have $s \geq 1$. Therefore, $s - 1 \in \mathbb{N}$, but $s - 1 \notin S$, because s is the smallest element of S. Hence, $P(s-1)$ is true, which implies that $P(s-1+1) = P(s)$ is true, so $s \notin S$, which is a contradiction. □

The Principle of Mathematical Induction yields a very powerful method of proof. In a proof by induction, $P(0)$ is called the **base case**, while the fact that, for every $k \in \mathbb{N}$, $P(k) \implies P(k+1)$, is called the **inductive step**. The hypothesis of this implication, namely $P(k)$, is called the

inductive hypothesis. To prove a sequence of statements for all natural numbers, it thus suffices to prove the base case and the inductive step.

Example 1.5.5

Prove that, for all $n \in \mathbb{N}$, we have

$$2^n \geq n + 1.$$

Solution.
We will use a proof by induction. For $n \in \mathbb{N}$, let $P(n)$ be the statement "$2^n \geq n+1$".

Base case:
The statement $P(0)$ is "$2^0 \geq 0+1$" and it is true.

Inductive step:
Let $k \in \mathbb{N}$ and suppose that the statement $P(k)$ is true, that is, "$2^k \geq k+1$" is true. Given this inductive hypothesis, we want to show that $P(k+1)$ is true. In other words, we want to show that

$$2^{k+1} \geq ((k+1)+1) = k+2.$$

Now $2^{k+1} = 2 \cdot 2^k$, and by the inductive hypothesis, we have

$$2^{k+1} = 2 \cdot 2^k \geq k+2 \iff 2\,(k+1) \geq k+2$$

Hence, we require $2\,k + 2 \geq k + 2$, which simplifies to $k \geq 0$. Since $k \in \mathbb{N}$, this is satisfied.

Hence, by the Principle of Mathematical Induction, $P(n)$ is true for all $n \in \mathbb{N}$.

Exercise 1.5.6

Using induction, prove that for all $n \in \mathbb{N}$, we have

$$\sum_{i=0}^{n} i := 0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Exercise 1.5.7

Given the following sums, find a simple formula for each (in the style of Exercise 1.5.6 above) and prove that it is correct using induction.

1. $\sum_{i=0}^{n}(2i+1) = 0+1+3+5+\cdots+2n+1$

2. $\sum_{i=1}^{n}(4i-1) = 3+7+11+\cdots+4n-1$

Sometimes, instead of proving that the sequence of statements $P(n)$ hold for every $n \in \mathbb{N}$, we want to prove they hold for every $n \in \mathbb{N}$ with $n \geq s$. We can still use the Principle of Mathematical Induction in this case, with two modification:

- The base case that we must prove is $P(s)$, rather than $P(0)$;

- In the inductive step, we may use the fact that $k \geq s$.

Example 1.5.8

For all $n \in \mathbb{N}$ with $n \geq 3$, the sum of the interior angles of an n-gon is equal to $(n-2)\pi$.

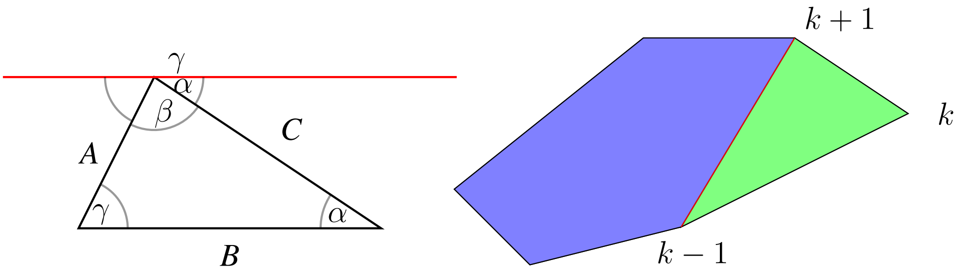
Proof. We prove this by induction on n. For $n \in \mathbb{N}$ with $n \geq 3$, let $P(n)$ be the statement that "the sum of the interior angles of an n-gon is equal to $(n-2)\pi$".

Base case.

(See Figure 1.3a.) The statement $P(3)$ is that "the sum of the interior angles of a 3-gon (triangle) is equal to π". Call the sides of the triangle A, B and C and the angles opposite them α, β and γ. Consider the unique line parallel to the line containing B, and containing the vertex not on B. Using corresponding angles, we see that $\alpha+\beta+\gamma=\pi$.

Inductive step.

(See Figure 1.3b.) Let $k \in \mathbb{N}$ with $k \geq 3$, and suppose that $P(k)$ is true, that is, "the sum of the interior angles of a k-gon is equal to $(k-2)\pi$". We want to show that $P(k+1)$ is true, that is, "the sum of the interior angles of a $(k+1)$-gon is equal to $(k-1)\pi$". Consider a $(k+1)$-gon, with vertices labelled $(1,\ldots,k+1)$, in order. Add an extra edge between $k-1$ and $k+1$. This subdivides the $(k+1)$-gon into a k-gon and a triangle, so the sum of its interior angles is $(k-2)\pi+\pi=(k-1)\pi$.



(a) Base case.

(b) Inductive step.

Figure 1.3: Illustrations for Example 1.5.8.

Therefore, by the Principle of Mathematical Induction, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$ with $n \geq 3$. □

Another variant occurs when we want to prove $P(n)$ for every natural number n greater than s, but are only able to prove the inductive step for $k \geq t$, where $t > s$. In this situation, we can try to start with the base case $P(t)$ and then prove $P(s), P(s+1), \ldots, P(t-1)$ case-by-case.

Exercise 1.5.9

Using induction, prove that for all $n \in \mathbb{N}$, we have

$$3^n > n^2.$$

Note that in the proof of Example 1.5.8, in the inductive step, we not only assumed that $P(k)$ is true, but also used that $P(3)$ is true. Technically, the inductive hypothesis is only $P(k)$, but assuming $P(3)$ is fine since we already proved it. This idea can be pushed further and leads to a stronger variant of the Principle of Mathematical Induction, often called **complete induction** or **strong induction**.

Theorem 1.5.10: Principle of Strong Induction

Let $P(n)$ be a sequence of statements with $n \in \mathbb{N}$. If

- *$P(0)$ is true, and*
- *for every $k \in \mathbb{N}$, if $P(j)$ is true for every $j \in \{0, \ldots, k\}$, then $P(k+1)$ is true,*

then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. The proof is essentially the same as the proof of Theorem 1.5.4, using the Well-Ordering Principle. □

Strong induction (Theorem 1.5.10) is a stronger variant of usual induction because the inductive hypothesis is stronger: to prove that $P(k+1)$ is true, we not only get to assume that $P(k)$ is true, but that $P(j)$ is true for all $0 \leq j \leq k$. This is useful for many problems.
Note that, just as with usual induction, we can adapt strong induction to situations with bases cases larger than 0.

Example 1.5.11

Consider a chocolate bar made up of $n \geq 1$ squares arranged in a rectangular grid. Prove that, to break the bar into its n squares requires $n-1$ breaks.

Solution.
Let $P(n)$ be the statement: "Breaking a bar made up of n squares requires $n-1$ breaks". Using strong induction, we prove that $P(n)$ is true for every $n \in \mathbb{N}$ with $n \geq 1$.

Base case.

The base case $P(1)$ is "breaking a bar made up of 1 square requires 0 breaks", which is clearly true.

Inductive step.

For the inductive step, let $k \geq 1$ and assume that $P(j)$ is true for every $j \in \{1, \dots, k\}$. We want to show that $P(k+1)$ is true, that is "breaking a bar made up of $k+1$ square requires k breaks".

So, consider a chocolate bar made up of $k+1$ squares. After one break, we we will have two pieces, one made up of x squares, the other made up of $k+1-x$ squares. Note that $x, k+1-x \in \{1, \dots, k\}$ so, by the inductive hypothesis, breaking the piece made up of x squares requires $x-1$ breaks, while breaking the piece made up of $k+1-x$ squares requires $k+1-x-1$ breaks. Thus, breaking a bar with $k+1$ squares requires $1+(x-1)+(k+1-x-1) = k$ breaks.

Therefore, by the Principle of Mathematical Induction, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$ with $n \geq 1$.

1.6 Larger systems of numbers

1.6.1 Rational numbers

You may recall from your early childhood that distributing 10 lollies amongst 3 people leads to problems. A more formal way of saying this is that the equation $3x = 10$ has no solution with $x \in \mathbb{Z}$. So the need for a larger number system naturally arises.

Definition 1.6.1

*A **rational number** is a pair of integers a/b with $b \neq 0$. Two such pairs a/b and c/d represent the same rational number if $ad = bc$. The set of rational numbers is denoted $\mathbb{Q}$.*

Note that, for every $x \in \mathbb{Q}$ with $x \neq 0$ there is a unique pair of integers $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$, $a > 0$ and $x = a/b$.

Exercise 1.6.2

Show that $\mathbb{Z} \subseteq \mathbb{Q}$, but $\mathbb{Q} \not\subseteq \mathbb{Z}$.

We can extend the operations $+$ and $\cdot$ from the integers to the rational numbers in a natural way, and they have similar properties. In fact, we obtain a new property: every non-zero element x in $\mathbb{Q}$ has a multiplicative inverse (in other words, there exists $y \in \mathbb{Q}$ such that $xy = 1$). This is the property that allows us to solve linear equations like $3x = 10$ over $\mathbb{Q}$, and it means that $\mathbb{Q}$ is an algebraic object called a **field**.
The extension from $\mathbb{Z}$ to $\mathbb{Q}$ is not sufficient to solve every equation.

Example 1.6.3

There is no rational number r such that $r^2 = 2$.

Solution.
Suppose, for a contradiction, that there exists $r \in \mathbb{Q}$ such that $r^2 = 2$. Clearly, $r \neq 0$, so there exist $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and $r = a/b$. It follows that $(a/b)^2 = 2$ and a little algebra gives $a^2 = 2b^2$, so a^2 is even. By Example 1.2.14, a is even. Thus $a = 2n$ for some $n \in \mathbb{Z}$; substituting, $(2n)^2 = 2b^2$ and thus $2n^2 = b^2$. Again by Example 1.2.14, b is even and so 2 is a common divisor of a and b; i.e., $\gcd(a, b) \geq 2$, which contradicts the assumption that $\gcd(a, b) = 1$. This completes the proof.

Example 1.6.4

$\log_2(3)$ *is not a rational number.*

Solution.
Suppose, for a contradiction that $\log_2(3)$ is a rational number, so that $\log_2(3) = m/n$ for some $m \in \mathbb{Z}$ and $n \in \mathbb{Z}\backslash\{0\}$. Since $\log_2(3) > 0$, we can assume that $m, n > 0$. By definition of logarithms, we have $2^{m/n} = 3$ and, using laws of exponents, $2^m = 3^n$. But 2^m is an even integer (since $m > 0$) whereas 3^n is an odd integer—we have a contradiction! This concludes the proof.

1.6.2 Real numbers

Recall from Example 1.6.3 that there does not exist a rational number r such that $r^2 = 2$. So the need for a large number system arises again, which we will call the **real numbers**. A precise definition of the real numbers is quite elaborate and outside of the scope of this course.

Remark 1.6.5

For the interested reader, let us briefly mention that an algebraic way to define the real numbers is via the use of Dedekind cuts. The basic idea is to partition the rational numbers into those smaller than the number one wants to represent and those bigger; for example, for $\sqrt{2}$ the sets A and B forming the partition would be $A = \{a \in \mathbb{Q}|$ either $a < 0$ or $a \geq 0$ and $a^2 < 2\}$ and $B = \{b \in \mathbb{Q}|b > 0$ and $b^2 > 2\}$. The set of real numbers is then defined to be the set of these cuts; the details of the definition of the algebraic operations and the order are very technical and will be discussed in a course on analysis or set theory.

1.6.3 Complex numbers

It is clear that the equation $x^2 + 1 = 0$ cannot have a solution in the real numbers since the square of every real number is nonnegative. This motivates the definition of the **imaginary unit** i, which has the property that $\mathrm{i}^2 = -1$, and thus is a solution to this equation.

Remark 1.6.6

Following the standard ISO 80000-2:2009, we will use the Roman i for the imaginary unit. This allows us to use an italic i to represent some other variable—often a row index in a matrix or column vector in the later part of this course.

Definition 1.6.7: The complex numbers

*The set of **complex numbers**, denoted $\mathbb{C}$, is the set of all formal expressions of the form $a + b\mathrm{i}$, with $a, b \in \mathbb{R}$.*
We can add complex numbers in the obvious way: for $a, b, c, d \in \mathbb{R}$, we have $(a + b\mathrm{i}) + (c + d\mathrm{i}) = (a + c) + (b + d)\mathrm{i}$.
We can also multiply complex numbers by using distributivity and the definition $\mathrm{i}^2 = -1$:

$$\begin{aligned}(a + b\mathrm{i})(c + d\mathrm{i}) &= (ac + ad\mathrm{i} + bc\mathrm{i} + bd\mathrm{i}^2)\\ &= (ac - bd) + (ad + bc)\mathrm{i}.\end{aligned}$$

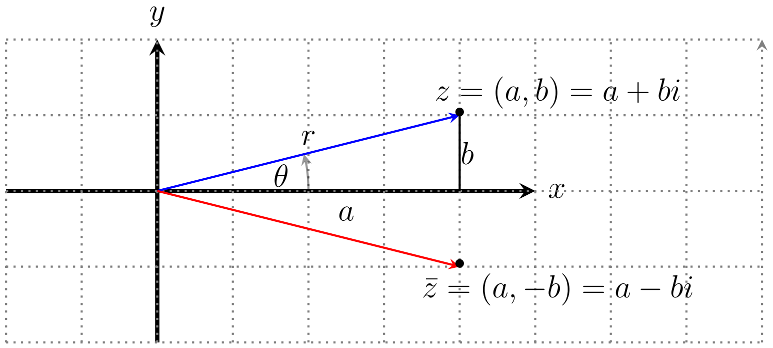


Figure 1.4: An Argand diagram.

Proposition 1.6.8: Properties of complex multiplication

Let $x, y, z \in \mathbb{C}$.

1. *$1z = z1 = z$;   (Identity)*
2. *$xy = yx$;   (Commutativity)*
3. *$x(yz) = (xy)z$;   (Associativity)*

Proof. Exercise. □

Definition 1.6.9

*Let $z, w \in \mathbb{C}$ be of the form $z = a + \mathrm{b}i$ and $w = c + d\mathrm{i}$ with $a, b, c, d \in \mathbb{R}$. We say that $z = w$, that is, z and w are **equal** if and only if $a = c$ and $b = d$.*

Definition 1.6.10: Cartesian representation

*A complex number $z = a + \mathrm{b}i$ with $a, b \in \mathbb{R}$ can be identified with the ordered pair (a, b) of real numbers, i.e. a point in the plane $\mathbb{R}^2$. We call (a, b) the **Cartesian representation** of z.*

*Because of this identification, the set of complex numbers is sometimes called the **complex plane**, with each complex number being a point of the plane. A plot showing complex numbers as points in this way is called an **Argand diagram**, and an example is Figure 1.4.*

Remark 1.6.11

Two complex number $z, w \in \mathbb{C}$ are equal if their Cartesian representations correspond to the same point in the Argand diagram.

Definition 1.6.12: Polar Coordinates

*Let p be a point in the plane $\mathbb{R}^2$. We can use Cartesian coordinates to specify p, but we can also specify it by giving the distance r to the origin, together with the angle θ between the x-axis, and the line through the origin and p. In this case, (r, θ) are the **polar coordinates** for p.*

Remark 1.6.13: About the angle

- *Note that the angle θ is not unique for a given point, since adding 2π to θ leaves the point unchanged. We will use the convention that an angle is always in the interval $[0, 2\pi)$.*
- *The origin $(0, 0)$ does not have a well-defined θ. It is the unique point with $r = 0$ and in polar notation we will denote it 0.*

Given the coordinates of a point in one representation, how do we determine its coordinates in the other representation?

Lemma 1.6.14: Changing coordinates

Given a point with Cartesian coordinates (a, b), its polar coordinates are given by

$$r = \sqrt{a^2 + b^2}$$

and

$$\tan\theta = \frac{b}{a}, \text{ with } \theta \in [0, 2\pi).$$

Conversely, given a point with polar coordinates (r, θ), its Cartesian coordinates are given by

$$a = r\cos\theta$$

and

$$b = r\sin\theta.$$

Proof. Pythagoras' formula tells us that $r^2 = a^2 + b^2$. Moreover, $\cos\theta = \dfrac{a}{\sqrt{a^2+b^2}}$ and $\sin\theta = \dfrac{b}{\sqrt{a^2+b^2}}$, So we obtain $r = \sqrt{a^2+b^2}$ and $\tan\theta = \dfrac{b}{a}$.

The second part follows from basic trigonometry. □

Definition 1.6.15: Polar Representation

*We have already seen that a complex number z can be identified with a point of the Cartesian plane $\mathbb{R}^2$. We can then use the above to express z in polar coordinates. In this setting, we call θ the **argument** and r the **modulus** of z; we denote r sometimes by $|z|$. The argument and modulus are indicated on Figure 1.4.*

Definition 1.6.16: Complex conjugate

*The **complex conjugate** of a complex number $z = a + b\mathrm{i}$, with $a, b \in \mathbb{R}$, is given by the complex number $a - b\mathrm{i}$, and denoted $\bar{z}$.*

In the Cartesian representation, the complex conjugate of (a, b) is the point $(a, -b)$, which is geometrically obtained from (a, b) by a reflection with respect to the x-axis.

Exercise 1.6.17

Let $z \in \mathbb{C}$ correspond to the point (a, b) in the Argand diagram.

1. *Express the point that is geometrically obtained from (a, b) by a reflection with respect to the y-axis in terms of z and/or $\bar{z}$.*

2. *Express in terms of z and/or $\bar{z}$ the point that is geometrically obtained from (a, b) by a reflection with respect to first the x- and then the y-axis.*

Lemma 1.6.18: Inverse of a complex number

*For every $z \in \mathbb{C}$, $z \neq 0$ there exists a unique complex number, denoted by z^{-1}, with the property that $zz^{-1} = z^{-1}z = 1$. We call z^{-1} the **inverse** of z and it can be computed as $z^{-1} = \frac{1}{|z|^2}\bar{z}$.*

Proof. It can readily be verified that z^{-1} has the desired property. To prove uniqueness assume that z had two inverses, say, u and w with the above property. Then $u = u1 = u(zw) = (uz)w' = 1w = w$ so $u = w$ and the inverse of z is unique. □

Recall that given two complex numbers in Cartesian form, adding them was straightforward, whereas multiplying them was a little more complicated. We will see that, in polar coordinates, the reverse is true: multiplication is easy, while addition is more difficult.

Proposition 1.6.19: Multiplying using polar coordinates

If z_1 and z_2 are complex numbers given in polar coordinates by (r_1, θ_1) and (r_2, θ_2), then $z_1 z_2$ is given by the polar coordinates

$$(r_1 r_2, \theta_1 + \theta_2).$$

Proof. Switching to Cartesian coordinates, we get

$$z_1 = (r_1 \cos\theta_1, r_1 \sin\theta_1)$$

and

$$z_2 = (r_2 \cos\theta_2, r_2 \sin\theta_2).$$

Applying the formula for multiplication in complex coordinates, we find

$$\begin{aligned} z_1 z_2 &= (r_1 \cos\theta_1 + r_1 \sin\theta_1 \mathrm{i}) \cdot (r_2 \cos\theta_2 + r_2 \sin\theta_2 \mathrm{i}) \\ &= (r_1 r_2 \cos\theta_1 \cos\theta_2 - r_1 r_2 \sin\theta_1 \sin\theta_2) + \\ &\quad (r_1 r_2 \cos\theta_1 \sin\theta_2 + r_1 r_2 \sin\theta_1 \cos\theta_2)\mathrm{i} \\ &= r_1 r_2 \cos(\theta_1 + \theta_2) + r_1 r_2 \sin(\theta_1 + \theta_2)\mathrm{i}. \end{aligned}$$

Switching back to polar coordinates, we get $(r_1 r_2, \theta_1 + \theta_2)$, as claimed. □

Example 1.6.20: On the sum of angles

In polar coordinates, if we multiply $(2, 5\pi/3)$ with $(3, 4\pi/3)$, then applying the formulas we obtain $(6, 3\pi)$; recall though our convention that an angle is always in the interval $[0, 2\pi)$, and so subtracting 2π we obtain the result $(6, \pi)$.

Exercise 1.6.21: Properties of the modulus

Let w and z be complex numbers. Show that $|wz| = |w||z|$, and that $|z|^2 = z\bar{z}$.

From now on, we will write $re^{\mathrm{i}\theta}$ for the complex number with polar coordinates (r, θ). This makes sense, because we can apply the familiar rules for exponentiation to multiply numbers in polar form:

$$(r_1 e^{\mathrm{i}\theta_1})(r_2 e^{\mathrm{i}\theta_2}) = r_1 r_2 e^{\mathrm{i}(\theta_1 + \theta_2)}.$$

Remark 1.6.22

This notation can be shown to have a deeper meaning which you will see (for example) in a course on Complex Analysis.

The polar form also makes it easier to compute powers of complex numbers.

Lemma 1.6.23: De Moivre's formula

If $re^{\mathrm{i}\theta} \in \mathbb{C}$ and $n \in \mathbb{Z}$, then

$$\left(re^{\mathrm{i}\theta}\right)^n = r^n e^{\mathrm{i}n\theta}.$$

Proof. When $n = 0$, both left- and right-hand sides become 1, so the formula is trivial. For $n > 0$, this formula can be proved by induction using Proposition 1.6.19. Note that

$$\left(r^{-n}e^{-\mathrm{i}n\theta}\right)\left(re^{\mathrm{i}\theta}\right)^n = \left(r^{-n}e^{-\mathrm{i}n\theta}\right)\left(r^n e^{\mathrm{i}n\theta}\right) = r^{n-n}e^{\mathrm{i}(n-n)\theta} = 1,$$

so $\left(re^{\mathrm{i}\theta}\right)^{-n} = \left(\left(re^{\mathrm{i}\theta}\right)^n\right)^{-1} = \left(r^{-n}e^{-\mathrm{i}n\theta}\right)$. Hence, if $n < 0$ then the formula holds as well. □

Exercise 1.6.24

- *What is the complex conjugate of $re^{\mathrm{i}\theta}$?*
- *If $r \neq 0$, what is the inverse of $re^{\mathrm{i}\theta}$?*
- *Find all $x, y \in \mathbb{R}$ such that $(x + \mathrm{i}y)^2 = \mathrm{i}$.*
- *Let $v := 1 + \mathrm{i}$. Show that the set of all points $z \in \mathbb{C}$ such that $|z - v| = |vz|$ is a circle in the complex plane, and find its centre and radius. Further show that the set of all points $z \in \mathbb{C}$ such that $|z - v| = |z + v|$ is a line in the complex plane. What are the points of intersection between the circle and the line?*

We will encounter the complex numbers in a few more places in this course in connection to the other topics we discuss.

Linear algebra

Linear algebra is the branch of mathematics concerning linear equations and functions. It is used in almost all areas of mathematics, science and engineering.

2.1 Systems of linear equations

2.1.1 Basic definitions

Definition 2.1.1

A ***linear equation*** *in n* ***variables*** *$x_1, x_2, \ldots, x_n$ with* ***coefficients*** *$a_1, \ldots, a_n, d \in \mathbb{R}$ is an equation of the form*

$$a_1x_1 + \cdots + a_nx_n = d.$$

A ***solution*** *(in $\mathbb{R}^n$) to the equation is an n-tuple $(s_1, s_2, \ldots, s_n) \in \mathbb{R}^n$ such that when we substitute these numbers for the respective variables the equation holds:*

$$a_1s_1 + \cdots + a_ns_n = d.$$

The ***solution set*** *(in $\mathbb{R}^n$) to the equation is the set of <u>all</u> solutions to the equation:*

$$\{(s_1, \ldots, s_n) \in \mathbb{R}^n \mid a_1s_1 + \cdots + a_ns_n = d\}.$$

We often call an equation linear if it can be re-written in the form above. For example, $y = x + 1$ can be re-written as $-x + y = 1$.

Example 2.1.2

- $2x + 3y + z = 1$ *is a linear equation in the variables* x, y *and* z. *You can check that* $(x, y, z) = (0, 0, 1)$ *is a solution to this equation, but* $(x, y, z) = (1, 1, 1)$ *is not.*

- $2x\,y - 3 = 0$ *is not a linear equation in the variables* x *and* y *because the variables are multiplied together.*

- $x - 17 = 0$ *is a linear equation; its unique solution is* $x = 17$.

- $z + (1 + 2\mathrm{i})w = \mathrm{i}$ *is a linear equation with complex coefficients. Its solution set (in* $\mathbb{C}^2$*) is*

$$\left\{(z, w) \in \mathbb{C}^2 \mid z = -\mathrm{i} - (1 + 2\mathrm{i})w\right\}.$$

Remark 2.1.3

The example $y = x + 1$ *above suggests that the equation is effectively a function that relates* $x \in \mathbb{R}$ *to* $y := y(x) \in \mathbb{R}$. *The graph of the function* $y : \mathbb{R} \to \mathbb{R}$ *is a straight line, which is another way to understand why we call such equations linear equations.*

In the general case of a single equation with (unknown) variables $x_1, \ldots, x_n$, *if there exists* $1 \leq k \leq n$ *such that* $a_k \neq 0$ *we can rewrite the equation as*

$$x_k = \tfrac{1}{a_k}\left(d - a_1x_1 - \cdots a_{k-1}x_{k-1} - \cdots a_{k+1}x_{k+1} \cdots - a_nx_n\right).$$

The graph of the function $x_k : \mathbb{R}^{n-1} \to \mathbb{R}$ *is a hyperplane, which is much harder to draw!*

We conclude from Remark 2.1.3 that a linear equation often has infinitely many solutions. We need an efficient way to find and express the set of all solutions.

Example 2.1.4

Find all solutions to the linear equation $2x + 3y + z = 1$.

Solution.
We can rearrange the equation to get:

(i) $x = \frac{1}{2}(1 - 3y - z)$ with $y, z \in \mathbb{R}$, or

(ii) $y = \frac{1}{3}(1 - 2x - z)$ with $x, z \in \mathbb{R}$, or

(iii) $z = 1 - 2x - 3y$ with $x, y \in \mathbb{R}$.

Each of these equations provides a complete solution. We can assign any values to y and z in (i) or x and z in (ii) or x and y in (iii):

$$\begin{aligned} & \left\{ (x,y,z) \in \mathbb{R}^3 \;\middle|\; 2x + 3y + z = 1 \right\} \\ = & \left\{ (x,y,z) \in \mathbb{R}^3 \;\middle|\; x = \tfrac{1}{2}(1 - 3y - z) \right\} \\ = & \left\{ (x,y,z) \in \mathbb{R}^3 \;\middle|\; y = \tfrac{1}{3}(1 - 2x - z) \right\} \\ = & \left\{ (x,y,z) \in \mathbb{R}^3 \;\middle|\; z = 1 - 2x - 3y \right\}. \end{aligned}$$

In the last three expressions two of the three parameters are freely chosen and determine the third one. Hence the solution set can still be viewed as the graph of a function, say, $z : \mathbb{R}^2 \to \mathbb{R}$, but the input to this function is now a point in $\mathbb{R}^2$, because both x and y are used for the function rule. The graph of such a function will be a plane in (x, y, z)-space. It again does not matter whether you express z as a function of x and y, or y as a function of x and z, and so on; the graph will always be the same plane.

Definition 2.1.5

*A **system of linear equations** is a collection of linear equations on the same set of variables. A **solution** to a system of linear equations is an assignment of values to all the variables that simultaneously solves all the equations in the system.*

Example 2.1.6

This is a system of three linear equations in x_1, x_2, x_3 and x_4:

$$\begin{cases} 2x_1 - x_2 + x_3 + 2x_4 = 1 \\ 6x_1 - 2x_2 + x_3 + 6x_4 = 4 \\ 2x_1 \phantom{{}-2x_2} - x_3 + 3x_4 = 4 \end{cases}$$

Example 2.1.7

Find all solutions to the following systems of linear equations:

(i) $$\begin{cases} 2x + 3y = 1 \\ 2x + 3y = 2 \end{cases}$$

(ii) $$\begin{cases} 2x + y = 1 \\ x + y = 1 \end{cases}$$

(iii) $$\begin{cases} 2x + y = 1 \\ 4x + 2y = 2 \end{cases}$$

Solution. (i) Note that $2x + 3y = 1 \neq 2 = 2x + 3y$, so the two equations cannot simultaneously be satisfied and this system of two equations and two unknowns has no solution.

(ii) Observe that $2x + y = x + (x + y)$. Hence, if $x + y = 1$ then $2x + y = 1 \Leftrightarrow x + 1 = 1$ and we must have $x = 0$. This implies $y = 1$, so this system of two equations has a unique solution.

(iii) Let

$$S = \left\{ (x, y) \in \mathbb{R}^2 \;\middle|\; 2x + y = 1 \text{ and } 4x + 2y = 2 \right\}.$$

Note that all coefficients in the second equation are the double of the corresponding ones in the first equation, so that

$$\begin{aligned} S &= \left\{ (x, y) \in \mathbb{R}^2 \;\middle|\; 2x + y = 1 \right\} \\ &= \left\{ (x, y) \in \mathbb{R}^2 \;\middle|\; y = 1 - 2x \right\} \\ &= \left\{ (x, 1 - 2x) \;\middle|\; x \in \mathbb{R} \right\}, \end{aligned}$$

So this system of two equations has infinitely many solutions that lie on a straight line in $\mathbb{R}^2$.

2.1.2 Echelon form

Definition 2.1.8

*After arranging a system of linear equations in rows as above, the first nonzero coefficient in each row is called the **pivot**. A system of linear equations is in **row echelon form** if each pivot is successively further to the right as we move downwards. In this case, variables corresponding to columns with a pivot are called **leading variables**. Other variables are called **free variables**.*

When a system is in row echelon form, we can solve the system one equation at a time. We start at the bottom and progressively work our way upwards, expressing the leading variables in terms of free variables. The free variables can take on value. This process is known as **back substitution**.

Example 2.1.9

Solve the following (real) system of linear equations:

$$\begin{cases} u + 2v + w - x \qquad + \; z = 3 \\ \qquad v \qquad - x + y \qquad = 0 \\ \qquad\qquad\quad x \qquad + 3z = 3 \\ \qquad\qquad\qquad\quad y + 2z = 4 \end{cases}$$

Solution.
This system is in row echelon form; u, v, x and y are the leading variables while w and z are the free variables. We start with the bottom equation and obtain $y = 4 - 2z$. Then from the equation above this, we obtain $x = 3 - 3z$. By continuing upwards we further obtain $v = x - y = (3 - 3z) - (4 - 2z) = -1 - z$. Finally from the top equation we can deduce that:

$$\begin{aligned} u &= 3 - 2v - w + x - z \\ &= 3 - 2(-1 - z) - w + (3 - 3z) - z \\ &= 8 - w - 2z. \end{aligned}$$

Therefore, $(u, v, w, x, y, z) \in \mathbb{R}^6$ is a solution if and only if it is an element of the following set:

$$\left\{ (u, v, w, x, y, z) \in \mathbb{R}^6 \;\middle|\; \begin{array}{ll} u = 8 - w - 2z, & \\ v = -1 - z, & \\ x = 3 - 3z, & \\ y = 4 - 2z & \text{and } w, z \in \mathbb{R} \end{array} \right\}$$

$$= \{ (8 - w - 2z, -1 - z, w, 3 - 3z, 4 - 2z, z) \mid w, z \in \mathbb{R} \}$$

$$= \left\{ \begin{array}{ll} & (8, -1, 0, 3, 4, 0) \\ + & (-w, 0, w, 0, 0, 0) \\ + & (-2z, -z, 0, -3z, -2z, z) \end{array} \;\middle|\; w, z \in \mathbb{R} \right\}$$

$$= \left\{ \begin{array}{lr} & (8, -1, 0, 3, 4, 0) \\ + & w\ (-1, 0, 1, 0, 0, 0) \\ + & z(-2, -1, 0, -3, -2, 1) \end{array} \;\middle|\; w, z \in \mathbb{R} \right\}.$$

Example 2.1.10

For the following systems of (real) linear equations in row echelon form,

(a) identify the leading variables;

(b) identify the free variables;

(c) find the general solution.

(i) $$\begin{cases} 3x + 2y = 1 \\ \qquad\quad y = -1 \end{cases}$$

(ii) $$\begin{cases} w - x - y - \ z = 0 \\ \qquad\quad y + 2z = 0 \end{cases}$$

Solution.

(i) (a) x and y;

(b) none;

(c) $x = 1$ and $y = -1$.

(ii) (a) w and y;

(b) x and z;

(c) $y = -2z$ and $w = x - z$, where $x, z \in \mathbb{R}$. Therefore, the general solution for $(x, y, z, w) \in \mathbb{R}^4$ is the set

$$\begin{aligned} & \{\, (x,\ -2z,\ z,\ x-z) \mid x, z \in \mathbb{R} \,\} \\ = \ & \{\, x\,(1,0,0,1) + z\,(0,-2,1,-1) \mid x, z \in \mathbb{R} \,\}\,. \end{aligned}$$

2.1.3 Gaussian elimination

We now know how to solve systems of linear equations that are in row echelon form. What is now required is a technique for transforming an arbitrary system of linear equations into row echelon form. What we want are operations on systems of linear equations that leave the set of solutions unchanged. Some examples of such operations are:

1. interchanging two equations;
2. replacing an equation by a non-zero multiple of itself;
3. adding a multiple of an equation to another equation.

These operations are called **elementary row operations**. Using them, we can transform every system of linear equations into row echelon form.

Example 2.1.11

Solve the following systems of linear equations, by first putting them in row echelon form using row operations:

(i) $$\begin{cases} x + 2y = 3 \\ 2x + 5y = 7 \end{cases}$$

(ii) $$\begin{cases} \phantom{x+{}} y + z = 1 \\ x + y + z = 1 \\ 2x + 2y + 3z = 1 \end{cases}$$

Solution.

(i) $$\begin{cases} x + 2y = 3 \\ 2x + 5y = 7 \end{cases} \iff \begin{cases} x + 2y = 3 \\ y = 1 \qquad R_2 \leftarrow R_2 - 2R_1 \end{cases}$$

Using back substitution, we find that there is a unique solution, which is $(x, y) = (1, 1)$.

Note that the row echelon form is not unique. Any multiple of either of the equations is also in row echelon form, such as

$$\begin{cases} 2x + 4y = 6 & R_1 \leftarrow 2R_1 \\ \quad\ \ - \ \ y = -1 & R_2 \leftarrow -R_2 \end{cases}$$

or we can swap the two equations and use the pivot 2 in the second equation instead:

$$\begin{cases} 2x + 5y = 7 \\ \ \ x + 2y = 3 \end{cases} \iff \begin{cases} 2x + 5y = 7 \\ \quad\ -\frac{1}{2}y = -\frac{1}{2} & R_2 \leftarrow R_2 - \frac{1}{2}R_1 \end{cases}$$

which leads to the same solution.

(ii)
$$\begin{cases} \qquad\ \ y + \ z = 1 \\ \ \ x + \ y + \ z = 1 \\ 2x + 2y + 3z = 1 \end{cases} \iff \begin{cases} \ \ x + \ y + \ z = 1 & R_1 \leftarrow R_2 \\ \qquad\ \ y + \ z = 1 & R_2 \leftarrow R_1 \\ 2x + 2y + 3z = 1 \end{cases}$$

$$\iff \begin{cases} x + y + z = 1 \\ \quad\ \ y + z = 1 \\ \qquad\quad\ \ z = -1 & R_3 \leftarrow R_3 - 2R_1 \end{cases}$$

Using back substitution, we conclude that $(x, y, z) = (0, 2, -1)$ is the unique solution.

The general process, known as **Gaussian Elimination**, goes as follows.

Algorithm 2.1.12: Gaussian Elimination Algorithm

In order to solve a system of linear equations given in row form like the examples above:

1. *Ensure that there is a pivot in the top-left position, interchanging rows if necessary.*
2. *Eliminate the first variable from all the subsequent equations by adding a suitable multiple of the first row.*
3. *Consider the system consisting of all but the first equation; go back to Step 1 and repeat the process on the new system. Repeat until the last equation is reached.*

The system is now in a row echelon form and can directly be solved via back substitution.

Remark 2.1.13

The process of Gaussian elimination is not unique; in particular, there is often a choice in selecting a pivot in the top-left position. Humans prefer choosing a pivot that is a divisor for all (or most of the) other coefficients in its column; this makes the arithmetic operations easier. Computer codes for solving linear equations will choose the (first) largest coefficient (in absolute value) as the pivot, because this ensures a smallest possible round-off error in subsequent arithmetic operations; you can learn more about this in a course on numerical computation.

Example 2.1.14

By using Gaussian Elimination and back substitution, solve the system of equations

$$\begin{cases} w + 2x + 4y + 2z = 3 \\ w \phantom{{}+2x} + y + 2z = -1 \\ 2w - 2x - 2y + 2z = -6. \end{cases}$$

Solution.

1. We do not need to exchange any rows, as the top left position contains a pivot.

2. We eliminate the pivots from the second and third equations by adding multiples of R_1:

$$\begin{cases} w + 2x + 4y + 2z = 3 & \\ - 2x - 3y \phantom{{}+2z} = -4 & R_2 \leftarrow R_2 - R_1 \\ - 6x - 10y - 2z = -12 & R_3 \leftarrow R_3 - 2R_1. \end{cases}$$

3. We now remove the first equation, and consider the new system:

$$\begin{cases} -2x - 3y \phantom{{}-2z} = -4 \\ -6x - 10y - 2z = -12. \end{cases}$$

4. There is a pivot in the top left position, so we use it to eliminate the x in the second equation:

$$\begin{cases} -2x - 3y \phantom{{}-2z} = -4 & \\ - y - 2z = 0 & R_2 \leftarrow R_2 - 3R_1. \end{cases}$$

5. Removing the first equation again leaves us with a single equation; thus we are done. Adding back in the removed equations we have the system in row echelon form (with free variable z):

$$\begin{cases} w + 2x + 4y + 2z = 3 \\ \quad - 2x - 3y \qquad = -4 \\ \qquad\quad - \ y - 2z = 0. \end{cases}$$

Now, by back substitution we have that the solutions $(w, x, y, z) \in \mathbb{R}^4$ are given by the set

$$\begin{aligned} & \{ (-1,\, 2 + 3z,\, -2z,\, z) \mid z \in \mathbb{R} \} \\ = \ & \{ (-1, 2, 0, 0) + z\,(0, 3, -2, 1) \mid z \in \mathbb{R} \}. \end{aligned}$$

2.1.4 Matrix notation

While doing Gaussian Elimination, it is not necessary to write which variable corresponds to which coefficient, as this is indicated by the position. This allows us to lighten our notation. For example,

$$\begin{cases} 3x + 4y + 5z = 2 \\ \ \ x + 2y + 3z = 4 \\ 2x + 5y + \ \ z = 3 \end{cases}$$

can be rewritten as

$$\left[\begin{array}{ccc|c} 3 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 \\ 2 & 5 & 1 & 3 \end{array}\right]$$

as long as we remember that the first column corresponds to the variable x, the second column to y, the third to z and the last to the constant coefficients. This is called the **augmented matrix** corresponding to the the system of linear equations.

Example 2.1.15

For each of the following systems of linear equations:

(a) write the system in augmented matrix form;

(b) reduce the matrix to row echelon form;

(c) find the general solution.

(i) $$\begin{cases} 2x+4y+2z=6 \\ \quad\quad y+\ z=1 \\ x+3y+3z=5 \end{cases}$$

(ii) $$\begin{cases} x+y+\ z=1 \\ 2x-y+3z=2 \\ 4x+y+5z=5 \end{cases}$$

(iii) $$\begin{cases} x+\ y+\ z=1 \\ 2x+2y+2z=2 \\ 3x+3y+3z=3 \end{cases}$$

Solution.

(i) (a) The augmented matrix is

$$\left[\begin{array}{ccc|c} 2 & 4 & 2 & 6 \\ 0 & 1 & 1 & 1 \\ 1 & 3 & 3 & 5 \end{array}\right]$$

(b) One such reduction is done as follows:

$$\left[\begin{array}{ccc|c} 2 & 4 & 2 & 6 \\ 0 & 1 & 1 & 1 \\ 1 & 3 & 3 & 5 \end{array}\right] \iff \left[\begin{array}{ccc|c} 1 & 2 & 1 & 3 \\ 0 & 1 & 1 & 1 \\ 1 & 3 & 3 & 5 \end{array}\right] R_1 \leftarrow \tfrac{1}{2}R_1$$

$$\iff \left[\begin{array}{ccc|c} 1 & 2 & 1 & 3 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \end{array}\right] R_3 \leftarrow R_3 - R_1$$

$$\iff \left[\begin{array}{ccc|c} 1 & 2 & 1 & 3 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right] R_3 \leftarrow R_3 - R_2$$

Echelon form

(c) From the answer to part (b), we see that:

$$\begin{cases} x+2y+z=3 \\ \quad\quad y+z=1 \\ \quad\quad\quad z=1 \end{cases}$$

and so the unique solution is $(x, y, z) = (2, 0, 1)$.

(ii) (a) The augmented matrix is

$$\left[\begin{array}{rrr|r} 1 & 1 & 1 & 1 \\ 2 & -1 & 3 & 2 \\ 4 & 1 & 5 & 5 \end{array}\right]$$

(b) Reduction to row echelon form could be:

$$\left[\begin{array}{rrr|r} 1 & 1 & 1 & 1 \\ 2 & -1 & 3 & 2 \\ 4 & 1 & 5 & 5 \end{array}\right] \iff \left[\begin{array}{rrr|r} 1 & 1 & 1 & 1 \\ 0 & -3 & 1 & 0 \\ 4 & 1 & 5 & 5 \end{array}\right] R_2 \leftarrow R_2 - 2R_1$$

$$\iff \left[\begin{array}{rrr|r} 1 & 1 & 1 & 1 \\ 0 & -3 & 1 & 0 \\ 0 & -3 & 1 & 1 \end{array}\right] R_3 \leftarrow R_3 - 4R_1$$

$$\iff \left[\begin{array}{rrr|r} 1 & 1 & 1 & 1 \\ 0 & -3 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] R_3 \leftarrow R_3 - R_2$$

Echelon form

(c) From part (b) we have:

$$\begin{cases} x + y + z & = 1 \\ - 3y + z & = 0 \\ & 0 = 1 \end{cases}$$

hence, there are no solutions.

(iii) (a) The augmented matrix is

$$\left[\begin{array}{rrr|r} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 \end{array}\right]$$

(b) Reduction to row echelon form gives:

$$\left[\begin{array}{rrr|r} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 \end{array}\right] \iff \left[\begin{array}{rrr|r} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 3 & 3 & 3 & 3 \end{array}\right] R_2 \leftarrow R_2 - 2R_1$$

$$\iff \left[\begin{array}{rrr|r} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] R_3 \leftarrow R_3 - 3R_1$$

Echelon form

(c) From part (b) we have:

$$\begin{cases} x + y + z = 1 \\ 0 = 0 \\ 0 = 0 \end{cases}$$

and so the set of solutions is

$$\left\{\, (1,0,0) + y\,(-1,1,0) + z\,(-1,0,1) \;\middle|\; (y,z) \in \mathbb{R}^2 \,\right\}.$$

Exercise 2.1.16

Find the solution set in $\mathbb{C}^3$ of the following linear system:

$$\begin{aligned} z_1 + (1-\mathrm{i})z_3 &= 0 \\ (1+\mathrm{i})z_1 + z_2 &= 1 \\ (2-2\mathrm{i})z_2 - 4z_3 &= 2. \end{aligned}$$

2.1.5 Reduced row echelon form

Definition 2.1.17

A system of linear equations is in ***reduced row echelon form*** *if*

1. *it is in row echelon form;*
2. *all the pivots are equal to one;*
3. *the pivots are the only non-zero entries in their columns.*

Example 2.1.18

The following system is in reduced row echelon form:

$$\begin{cases} w \quad + 3y = 2 \\ x + 2y = 1 \\ z = 3 \end{cases}$$

or in matrix form,

$$\left[\begin{array}{cccc|c} 1 & 0 & 3 & 0 & 2 \\ 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right]$$

To reduce a system of linear equations into reduced row echelon form, we use the following procedure.

Algorithm 2.1.19

1. *Reduce the system to row echelon form;*
2. *Divide each equation by its pivot, so all pivots become* 1*;*
3. *Eliminate each leading variable from the other equations above it, starting from the right most leading variable and moving to the left.*

Example 2.1.20

Bring the system from Example 2.1.14 into reduced row echelon form.

Solution.
Recall that the system of equations is given by

$$\begin{cases} w + 2x + 4y + 2z = 3 \\ w \qquad\; + \; y + 2z = -1 \\ 2w - 2x - 2y + 2z = -6. \end{cases}$$

1. We already reduced this system to row echelon form in step 5. from Example 2.1.14:

$$\begin{cases} w + 2x + 4y + 2z = 3 \\ \quad - 2x - 3y \qquad = -4 \\ \qquad\quad - \; y - 2z = 0. \end{cases}$$

2. Writing the above system as an augmented matrix, we divide the second row by -2 and the third row by -1 to set all pivots to 1:

$$\left[\begin{array}{cccc|c} 1 & 2 & 4 & 2 & 3 \\ 0 & -2 & -3 & 0 & -4 \\ 0 & 0 & -1 & -2 & 0 \end{array}\right]$$

$$\iff \left[\begin{array}{cccc|c} 1 & 2 & 4 & 2 & 3 \\ 0 & 1 & \frac{3}{2} & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 \end{array}\right] \begin{array}{l} \\ R_2 \leftarrow -\frac{1}{2}R_2 \\ R_3 \leftarrow -R_3 \end{array}$$

3. In the last step, we remove the non-zero entries in the second and third columns, to get the equivalent augmented matrix:

$$\left[\begin{array}{cccc|c} 1 & 2 & 0 & -6 & 3 \\ 0 & 1 & 0 & -3 & 2 \\ 0 & 0 & 1 & 2 & 0 \end{array}\right] \begin{array}{l} R_1 \leftarrow R_1 - 4R_3 \\ R_2 \leftarrow R_2 - \frac{3}{2}R_3 \\ \end{array}$$

$$\iff \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -3 & 2 \\ 0 & 0 & 1 & 2 & 0 \end{array}\right] \begin{array}{l} R_1 \leftarrow R_1 - 2R_2 \\ \\ \end{array}$$

Note that the solution to this system in reduced row echelon form is given by the equations

$$\begin{cases} w &= -1 \\ x &= 2+3z \\ y &= -2z \end{cases}$$

which leads to the same solution set as in Example 2.1.14.

General solution to a system of linear equations

Once a system of linear equations is in reduced row echelon form, it is very easy to find the general solution, using the following method:

1. Complete rows of zeros are ignored.
2. If there is a row of zeros except the last entry (the one in the augmented part) is non-zero, then the system has no solution.
3. Otherwise, we express the leading variables in terms of the free variables, as explained earlier.
4. If there is no free variable, then the system has a unique solution, otherwise, it has infinitely many solutions.

It follows from the above that a system of linear equations either has no solution, one solution, or infinitely many solutions. If it has at least one solution, we say that it is **consistent**, otherwise, it is **inconsistent**.

A system of m linear equations in n variables is typically inconsistent if $m > n$; the only exception is when the system in reduced row echelon form contains $m - n$ rows of the form $0 = 0$. Similarly, such a system is likely consistent if $m < n$, but we expect to have $n - m$ free variables. In other words, for a general system of m linear equations in n variables, we **expect** to have:

- no solutions if $m > n$;
- infinitely many solutions if $m < n$;
- a unique solution if $m = n$.

Our expectations are realised if the system in reduced row echelon form does not contain any rows of the form $0 = 0$; this means that the system does not contain any redundant equations.

We summarise the above discussion as the following theorem:

Theorem 2.1.21

Consider the general system of m linear equations in n variables:

$$\begin{cases} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \cdots & + & a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + & \cdots & + & a_{2,n}x_n & = & b_2 \\ \vdots & & \vdots & & \ddots & & \vdots & = & \vdots \\ a_{m,1}x_1 & + & a_{m,2}x_2 & + & \cdots & + & a_{m,n}x_n & = & b_m \end{cases}$$

Assume that this system has been brought into reduced row echelon form and there are no rows of the form $0 = 0$. Then its solution set S satisfies one of the following:

- *S consists of a single unique solution if and only if $m = n$ and all pivots lie on the diagonal of the augmented matrix, that is, the reduced row echelon form looks like*

$$\begin{cases} x_1 & & & & = & c_1 \\ & x_2 & & & = & c_2 \\ & & \ddots & & = & \vdots \\ & & & x_n & = & c_m \end{cases}$$

- *S contains infinitely many solutions if and only if $m < n$ and the system of equations is consistent;*
- *$S = \emptyset$ if and only if the system is inconsistent.*

A system of linear equations where all the constant coefficients are zero is called **homogeneous**. Note that a homogeneous system is always consistent: assigning 0 to every variable always yields a solution. Moreover, if a homogeneous system has more variables than equations, then it has infinitely many solutions. We shall return to this later, as Exercise 2.6.38.

Example 2.1.22

For each of the following systems of linear equations:

(a) write it in matrix form;

(b) reduce it to row echelon form;

(c) reduce it to reduced row echelon form;

(d) find the solution set in $\mathbb{R}^3$.

$$\text{(i)}\quad \left\{\begin{array}{rrrrl} x_1 & & +x_3 & +4x_4 & =-1\\ 2x_1 & -x_2 & +x_3 & +7x_4 & =-2\\ -2x_1 & +x_2 & & -6x_4 & =2\\ x_1 & +x_2 & +x_3 & +4x_4 & =-1 \end{array}\right.$$

$$\text{(ii)}\quad \left\{\begin{array}{rrrrl} a & & +\ c & & =2\\ a+ & b+ & c+ & d & =3\\ 2a+ & b+ & 2c+ & 2d & =6\\ a+ & 2b+ & c & & =4 \end{array}\right.$$

$$\text{(iii)}\quad \left\{\begin{array}{rrrl} -x_1 & +3x_2 & +4x_3 & =0\\ x_1 & & +9x_3 & =0\\ x_1 & -2x_2 & +\ x_3 & =-2 \end{array}\right.$$

Solution.

(i) (a) The augmented matrix is $\left[\begin{array}{rrrr|r} 1 & 0 & 1 & 4 & -1\\ 2 & -1 & 1 & 7 & -2\\ -2 & 1 & 0 & -6 & 2\\ 1 & 1 & 1 & 4 & -1 \end{array}\right]$

(b) The reduction is done column by column using elementary row operations as follows:

$$\left[\begin{array}{rrrr|r} 1 & 0 & 1 & 4 & -1\\ 2 & -1 & 1 & 7 & -2\\ -2 & 1 & 0 & -6 & 2\\ 1 & 1 & 1 & 4 & -1 \end{array}\right]$$

$$\Longleftrightarrow \left[\begin{array}{rrrr|r} 1 & 0 & 1 & 4 & -1\\ 0 & -1 & -1 & -1 & 0\\ 0 & 1 & 2 & 2 & 0\\ 0 & 1 & 0 & 0 & 0 \end{array}\right] \begin{array}{l} \\ R_2 \leftarrow R_2 - 2R_1\\ R_3 \leftarrow R_3 + 2R_1\\ R_4 \leftarrow R_4 - R_1 \end{array}$$

$$\Longleftrightarrow \left[\begin{array}{rrrr|r} 1 & 0 & 1 & 4 & -1\\ 0 & 1 & 0 & 0 & 0\\ 0 & 1 & 2 & 2 & 0\\ 0 & -1 & -1 & -1 & 0 \end{array}\right] \begin{array}{l} \\ R_2 \leftarrow R_4\\ \\ R_4 \leftarrow R_2 \end{array}$$

$$\Longleftrightarrow \left[\begin{array}{cccc|c} 1 & 0 & 1 & 4 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & -1 & -1 & 0 \end{array}\right] \begin{array}{l} \\ \\ R_3 \leftarrow R_3 - R_2 \\ R_4 \leftarrow R_4 + R_2 \end{array}$$

$$\Longleftrightarrow \left[\begin{array}{cccc|c} 1 & 0 & 1 & 4 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right] \begin{array}{l} \\ \\ R_3 \leftarrow \frac{1}{2}R_3 \\ R_4 \leftarrow -R_4 \end{array}$$

$$\Longleftrightarrow \left[\begin{array}{cccc|c} 1 & 0 & 1 & 4 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right] \begin{array}{l} \\ \\ \\ R_4 \leftarrow R_4 - R_3 \end{array}$$

Echelon form

(c) The reduced row echelon form is obtained similarly column by column, but working from the right to left. Here, only one step is needed using elementary row operations, which leads to:

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 3 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right] \begin{array}{l} R_1 \leftarrow R_1 - R_3 \\ \\ \\ \\ \end{array}$$

Reduced row echelon form

(d) The solution set can then be found with back substitution: $\left\{\, (-1,0,0,0) + x_4\,(-3,0,-1,1) \;\middle|\; x_4 \in \mathbb{R} \,\right\}$.

(ii) (a) The augmented matrix is $\left[\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 2 \\ 1 & 1 & 1 & 1 & 3 \\ 2 & 1 & 2 & 2 & 6 \\ 1 & 2 & 1 & 0 & 4 \end{array}\right]$

(b) Reduction column by column leads to:

$$\left[\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 2 \\ 1 & 1 & 1 & 1 & 3 \\ 2 & 1 & 2 & 2 & 6 \\ 1 & 2 & 1 & 0 & 4 \end{array}\right]$$

$$\Longleftrightarrow \left[\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 2 & 0 & 0 & 2 \end{array}\right] \begin{array}{l} \\ R_2 \leftarrow R_2 - R_1 \\ R_3 \leftarrow R_3 - 2R_1 \\ R_4 \leftarrow R_4 - R_1 \end{array}$$

$$\iff \left[\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -2 & 0 \end{array}\right] \begin{array}{l} \\ \\ R_3 \leftarrow R_3 - R_2 \\ R_4 \leftarrow R_4 - 2R_2 \end{array}$$

$$\iff \left[\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{array}\right] \begin{array}{l} \\ \\ \\ R_4 \leftarrow R_4 + 2R_3 \end{array}$$

Echelon form

(c) Again only one step is needed to obtain the reduced row echelon form:

$$\left[\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{array}\right] \begin{array}{l} \\ R_2 \leftarrow R_2 - R_3 \\ \\ \\ \end{array}$$

Reduced row echelon form

(d) The last row has all variable coefficients 0 and constant coefficient 2, which is impossible. Therefore, there are no solutions.

(iii) (a) The augmented matrix is $\left[\begin{array}{ccc|c} -1 & 3 & 4 & 0 \\ 1 & 0 & 9 & 0 \\ 1 & -2 & 1 & -2 \end{array}\right]$

(b) Reduction column by column leads to:

$$\left[\begin{array}{ccc|c} -1 & 3 & 4 & 0 \\ 1 & 0 & 9 & 0 \\ 1 & -2 & 1 & -2 \end{array}\right]$$

$$\iff \left[\begin{array}{ccc|c} -1 & 3 & 4 & 0 \\ 0 & 3 & 13 & 0 \\ 0 & 1 & 5 & -2 \end{array}\right] \begin{array}{l} \\ R_2 \leftarrow R_2 + R_1 \\ R_3 \leftarrow R_3 + R_1 \end{array}$$

$$\iff \left[\begin{array}{ccc|c} 1 & -3 & -4 & 0 \\ 0 & 1 & 5 & -2 \\ 0 & 3 & 13 & 0 \end{array}\right] \begin{array}{l} R_1 \leftarrow -R_1 \\ R_2 \leftarrow R_3 - 3R_2 \\ R_3 \leftarrow R_2 \end{array}$$

$$\iff \left[\begin{array}{ccc|c} 1 & -3 & -4 & 0 \\ 0 & 1 & 5 & -2 \\ 0 & 0 & -2 & 6 \end{array}\right] \begin{array}{l} \\ \\ R_3 \leftarrow R_3 - 3R_2 \end{array}$$

Echelon form

(c) The reduced row echelon form is obtained by setting all pivots equal to 1, followed by elementary row operations on the third and then the second column:

$$
\begin{aligned}
&\left[\begin{array}{ccc|c} 1 & -3 & -4 & 0 \\ 0 & 1 & 5 & -2 \\ 0 & 0 & -2 & 6 \end{array}\right] \\
\iff &\left[\begin{array}{ccc|c} 1 & -3 & -4 & 0 \\ 0 & 1 & 5 & -2 \\ 0 & 0 & 1 & -3 \end{array}\right] \begin{array}{l} \\ \\ R_3 \leftarrow -\frac{1}{2}R_3 \end{array} \\
\iff &\left[\begin{array}{ccc|c} 1 & -3 & 0 & -12 \\ 0 & 1 & 0 & 13 \\ 0 & 0 & 1 & -3 \end{array}\right] \begin{array}{l} R_1 \leftarrow R_1 + 4R_3 \\ R_2 \leftarrow R_2 - 5R_3 \\ \end{array} \\
\iff &\left[\begin{array}{ccc|c} 1 & 0 & 0 & 27 \\ 0 & 1 & 0 & 13 \\ 0 & 0 & 1 & -3 \end{array}\right] \begin{array}{l} R_1 \leftarrow R_1 + 3R_2 \\ \\ \\ \end{array}
\end{aligned}
$$

Reduced row echelon form

(d) Back substitution is a formality: we can read off the solution: $(x_1, x_2, x_3) = (27, 13, -3)$ is the unique solution.

2.2 Vector spaces

2.2.1 $\mathbb{R}$-coordinate space

“What is a vector?" is a common question asked by students learning linear algebra. The answer to this question is “a vector is an element of a vector space". But then what is a “vector space"? The answer will be given in Definition 2.2.7 if you’d like to skip ahead, but first we will examine the prototypical example of a vector space to get our bearings.

Definition 2.2.1

*For each $n \in \mathbb{N}$, **n-dimensional $\mathbb{R}$-coordinate space** is the set*

$$\mathbb{R}^n := \left\{ \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} \;\middle|\; u_1, u_2, \ldots, u_n \in \mathbb{R} \right\}.$$

*An element $\mathbf{u} \in \mathbb{R}^n$ is called a **column vector**, and we will typically write u_i for its ith **component**.*

Notice that rather than writing an element $\mathbf{u} \in \mathbb{R}^n$ as an n-tuple $(u_1, \ldots, u_n)$ as we did in Remark 1.3.26, we have instead written it in this new column notation. The reason for this will become apparent when we introduce the rule for matrix multiplication later in the course. Since vectors in $\mathbb{R}^n$ are just n-tuples written in this new column notation, it follows that any two column vectors $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ are equal if and only if each of their n components are equal.

The column vector in $\mathbb{R}^n$ whose components are all 0 is called the **zero vector** and is denoted

$$\mathbf{0} := \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in \mathbb{R}^n$$

We often visualise a vector $\mathbf{v}$ as a directed line segment by drawing a line from $\mathbf{0}$ to the point with coordinates given by $\mathbf{v}$; here, $\mathbf{0}$ corresponds to the origin in $\mathbb{R}^n$. An example in $\mathbb{R}^2$ is given in Figure 2.1.

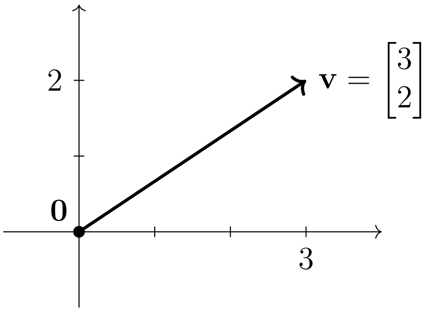


Figure 2.1: A vector visualised as a directed line segment.

We define two operations on $\mathbb{R}^n$: **vector addition** and **scalar multiplication**.

Definition 2.2.2: Vector addition

For any $\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix}, \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \in \mathbb{R}^n$*, we define*

$$\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} := \begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{bmatrix}.$$

Example 2.2.3

For example, if $\mathbf{v} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$ *and* $\boldsymbol{w} = \begin{bmatrix} 2 \\ -1 \end{bmatrix}$, *then* $\mathbf{v} + \boldsymbol{w} = \begin{bmatrix} 5 \\ 1 \end{bmatrix}$. *Depicting these vectors as arrows in the plane, we see that* $\mathbf{v} + \boldsymbol{w}$ *is one diagonal of the parallelogram spanned by* $\mathbf{v}$ *and* $\boldsymbol{w}$ *(Figure 2.2); because of this, the rule for vector addition is often called the* ***parallelogram rule****.*

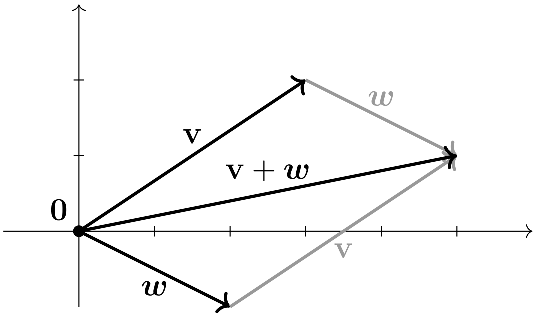


Figure 2.2: The sum of $\mathbf{v}$ and $\boldsymbol{w}$ is one diagonal of the parallelogram that they define.

Remark 2.2.4

In Figure 2.2, we drew arrows from the endpoints of $\mathbf{v}$ *and* $\mathbf{w}$ *to* $\mathbf{v} + \mathbf{w}$, *and labelled them respectively* $\mathbf{w}$ *and* $\mathbf{v}$. *This is because when we draw pictures we often identify a vector with the arrow it represents —that is, we identify a vector* $\mathbf{v}$ *with any arrow with the same length and direction as the arrow from* $\mathbf{0}$ *to* $\mathbf{v}$. *Strictly speaking, a vector is simply a point in space and so this does not make sense with regards to our definitions. It is possible to make mathematical sense of this in the field of mathematics called* ***affine geometry****.*

Definition 2.2.5: Scalar multiplication

For any $\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} \in \mathbb{R}^n$ *and* $c \in \mathbb{R}$, *we define*

$$c \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} := \begin{bmatrix} cu_1 \\ cu_2 \\ \vdots \\ cu_n \end{bmatrix}.$$

We follow the convention of denoting $-1\mathbf{v}$ by $-\mathbf{v}$.

If $\mathbf{v} \in \mathbb{R}^n$ is a non-zero vector and $c \in \mathbb{R}$ is a non-zero real number then we can visualise $c\mathbf{v}$ as the vector whose length is $|c|$ times the length of $\mathbf{v}$. Its direction is the same as $\mathbf{v}$ if $c > 0$ and opposite to $\mathbf{v}$ if $c < 0$.

Example 2.2.6

Consider the vector $\mathbf{v} := \begin{bmatrix} 3 \\ 2 \end{bmatrix} \in \mathbb{R}^2$. *The equalities*

$$3\mathbf{v} = 3\begin{bmatrix} 3 \\ 2 \end{bmatrix} = \begin{bmatrix} 9 \\ 6 \end{bmatrix} \quad \text{and} \quad -\mathbf{v} = -\begin{bmatrix} 3 \\ 2 \end{bmatrix} = \begin{bmatrix} -3 \\ -2 \end{bmatrix}.$$

are depicted graphically in Figure 2.3.

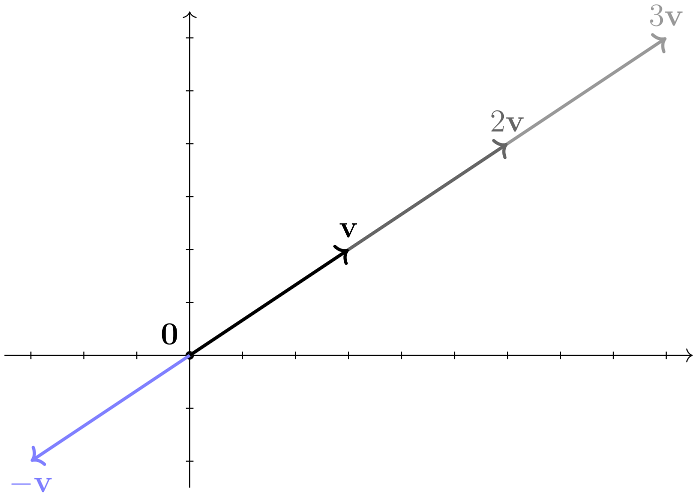
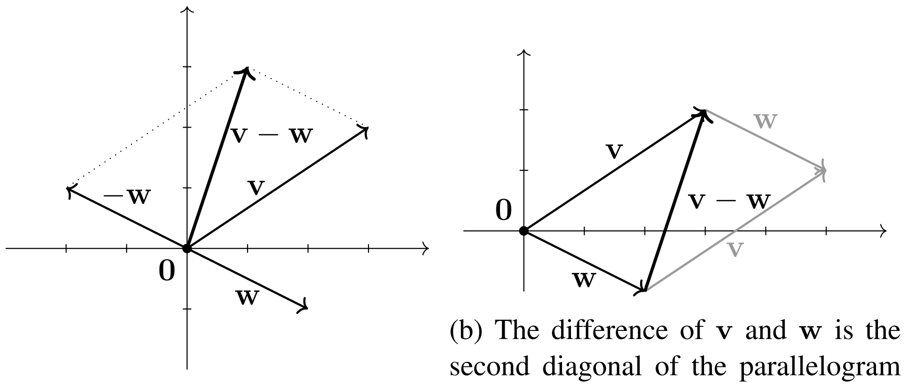


Figure 2.3: Scalar multiples of the vector $\mathbf{v}$.



(a) The formal definition of $\mathbf{v} - \mathbf{w}$.

(b) The difference of $\mathbf{v}$ and $\mathbf{w}$ is the second diagonal of the parallelogram that they define.

Figure 2.4: Two visualisations of the difference between two vectors.

We can also define subtraction:

$$\mathbf{u} - \mathbf{v} := \mathbf{u} + (-\mathbf{v}).$$

This is shown visually in Figure 2.4.

These operations behave in many ways as expected, which we will prove in 2.2.8 .

2.2.2 Abstract vector spaces

Now that we have seen the rules for adding and scaling vectors in $\mathbb{R}^n$, we will give the definition of an abstract vector space.

Definition 2.2.7

An $\mathbb{R}$***-vector space*** *is a set* V*, whose elements we call* ***vectors****, equipped with two operations:*

- ***vector addition***

$$\begin{aligned} V \times V &\longrightarrow V \\ (\mathbf{u}, \mathbf{v}) &\longmapsto \mathbf{u} + \mathbf{v}, \end{aligned}$$

- ***scalar multiplication*** *(or* ***scaling****)*

$$\begin{aligned} \mathbb{R} \times V &\longrightarrow V \\ (a, \mathbf{v}) &\longmapsto a\mathbf{v}. \end{aligned}$$

We will call the elements of $\mathbb{R}$ ***scalars****. The addition operation is required to satisfy the following properties:*

1. ***Associative law****. For all* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$*,*

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

2. ***Commutative law****. For all* $\mathbf{u}, \mathbf{v} \in V$*,*

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

3. ***Existence of zero****. There exists a zero element* $\mathbf{0} \in V$ *such that for all* $\mathbf{v} \in V$*,*

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

4. ***Existence of additive inverses****. For each* $\mathbf{v} \in V$*, there exists an element* $-\mathbf{v} \in V$ *such that*

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

The scaling operation is required to satisfy the following compatibility properties:

1. ***Distributive laws****. For all* $a, b \in \mathbb{R}$*,* $\mathbf{u}, \mathbf{v} \in V$*,*
   - $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$,
   - $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$.

2. ***Compatibility of multiplication****. For all* $a, b \in \mathbb{R}$*,* $\mathbf{v} \in V$*,*

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

3. ***Compatibility of multiplicative identity****. For all* $\mathbf{v} \in V$*,*

$$1\mathbf{v} = \mathbf{v}.$$

That is quite the list to remember! This definition might seem intimidating at first read, but with a bit more experience we'll come to see that the properties we require of vector addition and scalar multiplication are actually fairly intuitive. To summarize, a vector space is a set V equipped with sensible rules for adding and scaling vectors. Indeed, let's check that our prototypical $\mathbb{R}$-vector space $\mathbb{R}^n$ satisfies these properties.

Proposition 2.2.8

Equipped with the addition rule given by Definition 2.2.2 and the scaling rule given in Definition 2.2.5, $\mathbb{R}^n$ is an $\mathbb{R}$-vector space.

Proof. We prove associativity of addition and the existence of additive inverses, and leave the remainder as an exercise.

- Associativity follows from the following calculation:

$$\begin{aligned}
\mathbf{u} + (\mathbf{v} + \mathbf{w}) &= \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} + \left(\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} + \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \right) \\
&= \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} + \begin{bmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{bmatrix} \\
&= \begin{bmatrix} u_1 + (v_1 + w_1) \\ \vdots \\ u_n + (v_n + w_n) \end{bmatrix} \\
&= \begin{bmatrix} (u_1 + v_1) + w_1 \\ \vdots \\ (u_n + v_n) + w_n \end{bmatrix} \\
&= \begin{bmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{bmatrix} + \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \\
&= \left(\begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} + \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \right) + \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \\
&= (\mathbf{u} + \mathbf{v}) + \mathbf{w}.
\end{aligned}$$

- That $-\mathbf{u}$ is an additive inverse for $\mathbf{u}$ follows from the following calculation:

$$\begin{aligned}\mathbf{u}+(-\mathbf{u}) = \mathbf{u}+(-1)\mathbf{u} &= \begin{bmatrix}u_1\\ \vdots\\ u_n\end{bmatrix} + \begin{bmatrix}-u_1\\ \vdots\\ -u_n\end{bmatrix}\\ &= \begin{bmatrix}u_1+(-u_1)\\ \vdots\\ u_n+(-u_n)\end{bmatrix}\\ &= \begin{bmatrix}0\\ \vdots\\ 0\end{bmatrix} = \mathbf{0}. \qquad \square\end{aligned}$$

The advantage of the abstract definition is that if we prove something about vector spaces, then it will apply to all vector spaces. This is the approach used in abstract algebra. Let's have a look at a couple important examples of vector spaces.

Example 2.2.9

The following are examples of $\mathbb{R}$-vectors spaces. It is a good exercise to check that these satisfy all of the properties required in Definition 2.2.7.

1. *The set*

$$\mathbb{R}[x] := \left\{ \sum_{j=0}^{k} a_j x^j \;\middle|\; k \in \mathbb{N},\ a_j \in \mathbb{R} \right\},$$

which consists of all polynomials in one variable x with coefficients in $\mathbb{R}$. Addition and scalar multiplication are defined in the obvious way.

2. *Let X be a set, let V be an $\mathbb{R}$-vector space, and consider the set V^X consisting of all functions from X to V (recall Definition 1.4.6). We define addition and scaling **pointwise** on V^X. In detail, the sum of two functions $f, g : X \to V$ is defined to be the function*

$$\begin{aligned} f+g :\quad & X \longrightarrow V \\ & x \longmapsto f(x)+g(x). \end{aligned}$$

Similarly, the result of scaling a function $f : X \to V$ by a scalar $c \in \mathbb{R}$ is defined to be the function

$$\begin{aligned} cf :\quad & X \longrightarrow V \\ & x \longmapsto cf(x). \end{aligned}$$

The zero vector in V^X is the constant zero function

$$\begin{aligned} 0 :\quad & X \longrightarrow V \\ & x \longmapsto \mathbf{0}. \end{aligned}$$

2.2.3 Linear subspaces

When we define some type of mathematical object, such as a set or vector space, we also want to have a good definition of sub-objects. For example, in Definition 1.3.4 we defined the notion of a subset of a set. Similarly, we would now like to give a good definition of what it means to be a "sub-vector space".

Definition 2.2.10

Let V be an $\mathbb{R}$-vector space. A subset $S \subseteq V$ is said to be a ***linear subspace*** *(or* ***vector subspace****) of V if*

1. ***Closed under addition.*** *If $\mathbf{s}_1, \mathbf{s}_2 \in S$ then $\mathbf{s}_1 + \mathbf{s}_2 \in S$.*
2. ***Closed under scalar multiplication.*** *If $c \in \mathbb{R}$, $\mathbf{s} \in S$ then $c\mathbf{s} \in S$.*
3. *Addition and scalar multiplication in S satisfy the properties in Definition 2.2.7*

In other words, a subset $S \subseteq V$ of a vector space V is said to be a linear subspace if it inherits a vector space structure from V. As a working mathematician (or computer scientist, physicist, or engineer), most of the vector spaces that you encounter "in the wild" will be linear subspaces of some larger vector space, often $\mathbb{R}^n$, $\mathbb{R}[x]$, or V^X (where X is some set and V is a vector space).

You are likely a bit concerned about the third point in the definition above: it would be a lot of work to verify all of the properties in Definition 2.2.7 every time that we want to check if a subset is a linear subspace. But don't fear! The proposition below comes to the rescue:

Proposition 2.2.11: Linear subspace criteria

Let V be an $\mathbb{R}$-vector space. A subset $S \subseteq V$ is a linear subspace of V if and only if it satisfies the following properties:

1. ***Closed under addition.*** *If $\mathbf{s}_1, \mathbf{s}_2 \in S$ then $\mathbf{s}_1 + \mathbf{s}_2 \in S$.*
2. ***Closed under scalar multiplication.*** *If $c \in \mathbb{R}$, $\mathbf{s} \in S$ then $c\mathbf{s} \in S$.*
3. ***Contains the origin.*** $\mathbf{0} \in S$.

Proof. Let $S \subseteq V$ be a subset of a vector space V. Clearly, if S is a linear subspace then it satisfies the three criteria above.

Conversely, suppose that $S \subseteq V$ satisfies the three criteria in the proposition. We need to check that it satisfies the properties in Definition 2.2.7. This is very straightforward, but tedious to write out explicitly, so let's just check commutativity of addition in S to give you the idea:

Let $\mathbf{s}_1, \mathbf{s}_2 \in S$. But since $S \subseteq V$ then $\mathbf{s}_1, \mathbf{s}_2 \in V$ as well, and we already know that addition in V is commutative. Thus,

$$\mathbf{s}_1 + \mathbf{s}_2 = \mathbf{s}_2 + \mathbf{s}_1.$$

□

While the definition is likely new to you, it turns out that you are actually already familiar with many examples of linear subspaces! Indeed, we will show that the solution set of any *homogeneous* system of linear equations is a linear subspace.

Proposition 2.2.12

Consider the linear system

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

in n variables $x_1, \ldots, x_n$, where $a_{ij} \in \mathbb{R}$, $b_i \in \mathbb{R}$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. Let $S \subseteq \mathbb{R}^n$ denote the solution set of this linear system. If $\mathbf{b} = \mathbf{0}$ then S is a linear subspace of $\mathbb{R}^n$.

Proof. We just apply Proposition 2.2.11.

- Clearly $\mathbf{0}$ is a solution to this homogeneous linear system:

$$\begin{aligned} \sum_{j=1}^{n} a_{1j}0 &= 0 \\ &\vdots \\ \sum_{j=1}^{n} a_{mj}0 &= 0. \end{aligned}$$

- Let $\mathbf{x} := \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ and $\mathbf{y} := \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ be solutions to this homogeneous linear system, i.e.,

$$\begin{aligned} \sum_{j=1}^{n} a_{1j}x_j &= 0 \\ &\vdots \\ \sum_{j=1}^{n} a_{mj}x_j &= 0 \end{aligned}$$

  and

$$\sum_{j=1}^{n} a_{1j}y_j = 0$$

$$\vdots$$

$$\sum_{j=1}^{n} a_{mj} y_j = 0.$$

Then we have

$$\begin{aligned}\sum_{j=1}^{n} a_{1j}(x_j + y_j) &= \sum_{j=1}^{n} a_{1j}x_j + \sum_{j=1}^{n} a_{1j}y_j = 0 + 0 = 0\\ &\vdots\\ \sum_{j=1}^{n} a_{mj}(x_j + y_j) &= \sum_{j=1}^{n} a_{mj}x_j + \sum_{j=1}^{n} a_{mj}y_j = 0 + 0 = 0.\end{aligned}$$

so $\mathbf{x} + \mathbf{y}$ is also a solution.

- Let $\mathbf{x} := \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ be a solution to this homogeneous linear system, and let $c \in \mathbb{R}$. Then

$$\begin{aligned}\sum_{j=1}^{n} a_{1j}(cx_j) &= c\sum_{j=1}^{n} a_{1j}x_j = c0 = 0\\ &\vdots\\ \sum_{j=1}^{n} a_{mj}(cx_j) &= c\sum_{j=1}^{n} a_{mj}x_j = c0 = 0.\end{aligned}$$

Thus, $cvecx$ is also a solution to this homogeneous linear system.

□

Exercise 2.2.13

Continuing with the notation established in Proposition 2.2.12, show that if $\mathbf{b} \neq \mathbf{0}$, then S is not a linear subspace of $\mathbb{R}^n$.

Example 2.2.14

Let V be an $\mathbb{R}$-vector space.

1. $\{\mathbf{0}\}$ *is a linear subspace of* V.

2. V *is a linear subspace of itself.*

3. $\emptyset$ *is* not *a linear subspace of* V.

4. *For any fixed $k \in \mathbb{N}$, consider the subset of $\mathbb{R}[x]$ consisting of all polynomials of degree at most k, denoted by*

$$\mathbb{R}_k[x] := \left\{ \sum_{j=0}^{k} a_j x^j \;\middle|\; a_j \in \mathbb{R} \right\}.$$

For any $\displaystyle\sum_{j=0}^{k} a_j x^j, \sum_{j=0}^{k} b_j x^j \in \mathbb{R}_k[x]$ *and $c \in \mathbb{R}$ we have*

- $\sum_{j=0}^{k} a_j x^j + \sum_{j=0}^{k} b_j x^j = \sum_{j=0}^{k} (a_j + b_j) x^j \in \mathbb{R}_k[x]$
- $c \sum_{j=0}^{k} a_j x^j = \sum_{j=0}^{k} (c a_j) x^j \in \mathbb{R}_k[x]$
- $0 = \sum_{j=0}^{k} 0 x^j \in \mathbb{R}_k[x]$

Thus, we have shown that $\mathbb{R}_k[x]$ is a linear subspace of $\mathbb{R}[x]$.

Exercise 2.2.15

Let V be a vector space, and let S_1 and S_2 be linear subspaces of V. Show that $S_1 \cap S_2$ is a linear subspace of V.

Exercise 2.2.16

For those students who have seen the definition of continuity in MATHS 130, let $C^0(\mathbb{R}, \mathbb{R}) \subseteq \mathbb{R}^{\mathbb{R}}$ denote the subset of all continuous functions from $\mathbb{R}$ to itself. This is a linear subspace of the vector space $\mathbb{R}^{\mathbb{R}}$.

Exercise 2.2.17

For each of the following subsets of $\mathbb{R}^2$, decide whether or not it is a linear subspace.

1. *A straight line passing through the origin;*
2. *A straight line which does not contain the origin;*
3. *The circle of radius $r > 0$ centred at the origin: $\left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2 \;\middle|\; x^2 + y^2 = r^2 \right\}$;*
4. *The lattice $\mathbb{Z}^2$ shown in Figure 1.2.*
5. *The union of the horizontal and vertical axes, i.e.,*

$$\left\{ c_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \;\middle|\; c_1 \in \mathbb{R} \right\} \cup \left\{ c_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \;\middle|\; c_2 \in \mathbb{R} \right\}.$$

2.3 Linear combinations

2.3.1 Linear combinations and span

Definition 2.3.1

*Let V be an $\mathbb{R}$-vector space, and let $X \subseteq V$. A **linear combination** of vectors in X is an expression of the form*

$$c_1\mathbf{x}_1 + \cdots + c_k\mathbf{x}_k,$$

*where $c_1, \ldots, c_k \in \mathbb{R}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \in X$. The set of <u>all</u> possible linear combinations of vectors in X is called the **span** of X, and is denoted $\operatorname{Span} X$.*

Example 2.3.2

Consider the vectors $\mathbf{u} := \begin{bmatrix}1\\1\end{bmatrix}$ *and* $\mathbf{v} := \begin{bmatrix}1\\0\end{bmatrix}$ *in* $\mathbb{R}^2$.
Clearly, $\mathbf{w} := 3\mathbf{u} + 2\mathbf{v}$ *(Figure 2.5) is one linear combination of* $\mathbf{u}$ *and* $\mathbf{v}$.
More generally, every intersection point in Figure 2.5 is a linear combination of the form $a\mathbf{u} + b\mathbf{v}$ *for* $a, b \in \mathbb{Z}$*. In fact, for each intersection point there is* exactly one way *to express it as a linear combination of the vectors* $\mathbf{u}$ *and* $\mathbf{v}$
Even more generally, if we allow $a, b \in \mathbb{R}$*, then we can see that every point in the plane is a linear combination of the vectors* $\mathbf{u}$ *and* $\mathbf{v}$*. Thus, we conclude that* $\operatorname{Span}\{\mathbf{u}, \mathbf{v}\} = \mathbb{R}^2$.

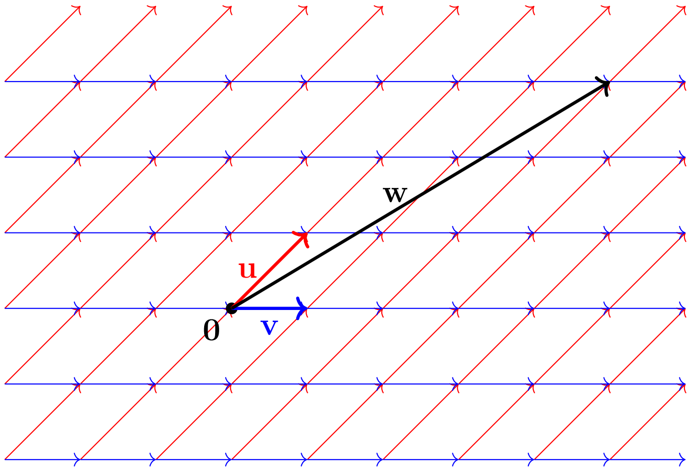


Figure 2.5: Linear combinations of $\mathbf{u}$ and $\mathbf{v}$, as defined in Example 2.3.2.

Let V be a vector space. Given a subset $X \subseteq V$, a natural question to ask is "what is the smallest linear subspace containing X?" The answer is $\operatorname{Span} X$, as stated (in more technical language) in the proposition below:

Proposition 2.3.3

Let V be a vector space, and let $X \subseteq V$. Then the following hold:

1. $X \subseteq \operatorname{Span} X$.
2. $\operatorname{Span} X$ *is a linear subspace of* V.
3. *For any linear subspace* $S \subseteq V$,

$$X \subseteq S \implies \operatorname{Span} X \subseteq S.$$

Proof. Let $\mathbf{u}, \mathbf{v} \in \operatorname{Span} X$ be arbitrary, and let $c \in \mathbb{R}$. By definition,

$$\mathbf{u} = \sum_{i=1}^{k} a_i \mathbf{x}_i = a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k,$$
$$\mathbf{v} = \sum_{j=1}^{l} b_j \mathbf{y}_j = b_1\mathbf{y}_1 + \cdots + b_l\mathbf{y}_l,$$

for some scalars $a_i, b_j \in \mathbb{R}$ and vectors $\mathbf{x}_i, \mathbf{y}_j \in X$.

1. Obvious.
2. - $\mathbf{0}$ is a linear combination of vectors from X.
   - Sums of linear combinations of vectors from X are linear combinations of vectors from X:

     $$\mathbf{u} + \mathbf{v} = a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k + b_1\mathbf{y}_1 + \cdots + b_l\mathbf{y}_l.$$

   - Scalar multiples of linear combinations of vectors from X are linear combinations of vectors from X:

     $$c\mathbf{u} = c\sum_{i=1}^{k} a_i\mathbf{x}_i = \sum_{i=1}^{k} (ca_i)\mathbf{x}_i.$$

3. Suppose $X \subseteq S$. Since S is assumed to be a linear subspace, then it is closed under addition and scalar multiplication, so $\mathbf{u} = \sum_{i=1}^{k} a_i\mathbf{x}_i \in S$. Thus, $\operatorname{Span} X \subseteq S$.

□

Exercise 2.3.4

Let V be a vector space and let $X \subseteq V$. Prove that $\operatorname{Span}(\operatorname{Span} X) = \operatorname{Span} X$.
(Hint: Use Proposition 2.3.3)

Definition 2.3.5

*Let $S \subseteq V$ be a linear subspace, and let $X \subseteq V$. If $\operatorname{Span} X = S$ then we say that X **spans** S.*

Example 2.3.6

For any vector space V, we of course have the empty subset $\emptyset \subseteq V$. Show that

$$\operatorname{Span} \emptyset = \{\mathbf{0}\}.$$

Solution.
By Proposition 2.3.3, the $\operatorname{Span} \emptyset$ is the smallest linear subspace of V containing $\emptyset$. Since the empty subset is contained in every linear subspace of V, then $\operatorname{Span} \emptyset$ must be the smallest among all the linear subspaces of V. Hence, it must be $\{\mathbf{0}\}$.

Let V be a vector space. Given a subset $X \subseteq V$, and a vector $\mathbf{v} \in V$, we commonly encounter the following questions:

1. Is $\mathbf{v}$ a linear combination of the vectors in X? In other words, is $\mathbf{v} \in \operatorname{Span} X$?
2. If so, in how many ways can we express $\mathbf{v}$ as a linear combination of the vectors in X?

We will now study these questions.

Example 2.3.7

Consider the subset

$$X := \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \right\} \subseteq \mathbb{R}^3.$$

Are the following vectors linear combinations of vectors in X?

(i) $\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$;

(ii) $\begin{bmatrix} 3 \\ 2 \\ 2 \end{bmatrix}$.

Solution. (i) Suppose there exist $c, d \in \mathbb{R}$ such that

$$\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = c \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + d \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} c \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ d \\ d \end{bmatrix} = \begin{bmatrix} c \\ d \\ d \end{bmatrix}.$$

Equating coefficients yields a system of three linear equations in c and d, which has no solution. It follows that $\begin{bmatrix}1\\0\\1\end{bmatrix}$ is **not** a linear combination of X.

(ii) Applying the same method (or by inspection), we find

$$\begin{bmatrix}3\\2\\2\end{bmatrix} = 3\begin{bmatrix}1\\0\\0\end{bmatrix} + 2\begin{bmatrix}0\\1\\1\end{bmatrix}$$

so $\begin{bmatrix}3\\2\\2\end{bmatrix}$ is a linear combination of X.

Generalizing the method we used to solve Example 2.3.7, we come up with the following algorithm for solving these problems:

Algorithm 2.3.8

Problem: *Given vectors* $\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{v} \in \mathbb{R}^n$, *find all possible scalars* $c_1, \ldots, c_k \in \mathbb{R}$ *such that*

$$\sum_{j=1}^{k} c_j \mathbf{u}_j = \mathbf{v}$$

Solution: *Solve the linear system above for* $\mathbf{c} := \begin{bmatrix}c_1\\ \vdots \\ c_k\end{bmatrix}$. *To do this, transform the augmented matrix*

$$\left[\begin{array}{ccc|c}\mathbf{u}_1 & \cdots & \mathbf{u}_k & \mathbf{v}\end{array}\right]$$

into row echelon form, and then back-substitute to get the general solution (if one exists).

Example 2.3.9

Consider the following vectors in $\mathbb{R}^2$

$$\mathbf{v} := \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad \mathbf{u}_1 := \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \mathbf{u}_2 := \begin{bmatrix} 3 \\ 1 \end{bmatrix}, \quad \mathbf{u}_3 := \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Determine if

$$\mathbf{v} \in \operatorname{Span}\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}.$$

If so, express $\mathbf{v}$ *as a linear combination of these three vectors in the most general way possible.*

Solution.
We need to solve the linear system

$$c_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 3 \\ 1 \end{bmatrix} + c_3 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

whose augmented matrix is

$$\left[\begin{array}{ccc|c} 1 & 3 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{array}\right].$$

This is already in row echelon form. Let $t := c_3$. Then by back-sub:

$$\begin{aligned} c_2 &= 1 - t \\ c_1 &= 1 - 3c_2 = -2 + 3t. \end{aligned}$$

Thus, for any $t \in \mathbb{R}$ we have

$$(-2+3t) \begin{bmatrix} 1 \\ 0 \end{bmatrix} + (1-t) \begin{bmatrix} 3 \\ 1 \end{bmatrix} + t \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Exercise 2.3.10

For each $k \geq 3$*, find a set of cardinality* k *which spans* $\mathbb{R}^3$*. (We will see later that no set of cardinality less than 3 may span* $\mathbb{R}^3$*.)*

2.3.2 Linear independence

Definition 2.3.11

Let V be an $\mathbb{R}$-vector space.

- *A finite list of vectors $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ from V is said to be **linearly independent** if for any scalars $c_1, \ldots, c_k \in \mathbb{R}$ we have*
$$\sum_{j=1}^{k} c_j \mathbf{v}_j = \mathbf{0} \implies c_1 = \cdots = c_k = 0.$$
*Otherwise, we say that the list is **linearly dependent**.*

- *A subset $X \subseteq V$ is said to be **linearly independent** if $\underline{\text{every}}$ finite list of $\underline{\text{unique}}$ vectors from X is linearly independent. Otherwise, we say that X is **linearly dependent**.*

In other words, a list of vectors $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ is linearly independent if the only possible way to write $\mathbf{0}$ as a linear combination of these vectors is the trivial one
$$\mathbf{0} = 0\mathbf{v}_1 + \cdots + 0\mathbf{v}_k.$$

On the other hand, if you can find a way to write $\mathbf{0}$ as a linear combination
$$\mathbf{0} = c_1\mathbf{v}_1 + \ldots + c_k\mathbf{v}_k$$
and at least one of the scalars $c_1, \ldots, c_k$ is not zero, then the list $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ is linearly dependent.

When first encountering these concepts, students are often confused by why they deserve to be called “linear (in)dependence”. Proposition 2.3.14 will show why this terminology is appropriate.

Example 2.3.12

Are the following sets of vectors in $\mathbb{R}^3$ linearly independent?

(i) $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right\}$;

(ii) $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ 2 \end{bmatrix} \right\}$.

Solution.
We just apply Algorithm 2.3.8.

(i) Suppose there exist $a, b, c \in \mathbb{R}$ such that

$$\begin{bmatrix}0\\0\\0\end{bmatrix} = a\begin{bmatrix}1\\0\\0\end{bmatrix} + b\begin{bmatrix}0\\1\\1\end{bmatrix} + c\begin{bmatrix}1\\0\\1\end{bmatrix} = \begin{bmatrix}a+c\\b\\b+c\end{bmatrix}.$$

Equating components yields a homogeneous system of three linear equations in a, b and c, and its only solution is $a = b = c = 0$, so the given set of vectors is linearly independent.

(ii) We have

$$\begin{bmatrix}0\\0\\0\end{bmatrix} = 3\begin{bmatrix}1\\0\\0\end{bmatrix} + 2\begin{bmatrix}0\\1\\1\end{bmatrix} - \begin{bmatrix}3\\2\\2\end{bmatrix},$$

so the given set of vectors is linearly dependent.

Example 2.3.13

Let V be a vector space. Then it is vacuously true that the empty subset $\emptyset \subseteq V$ is linearly independent.

In some sense, a subset X of a vector space V is linearly dependent when the information contained within it is 'redundant'—there is a vector you can remove without losing any information, because you can regain it by taking combinations of other vectors in the set.

On the other hand, if X is linearly *in*dependent then it is *ir*redundant in the following way: every linear combination of elements of X is only a linear combination in exactly one way (up to the ordering of the terms in the sum).

This is made precise in the proposition below.

Proposition 2.3.14

Let V be an $\mathbb{R}$-vector space and $X \subseteq V$. Then the following hold:

1. *X is linearly independent if and only if every vector in $\operatorname{Span} X$ can be written uniquely as a linear combination of distinct vectors from X.*

2. *X is linearly dependent if and only if there exists a vector $\mathbf{y} \in X$ and distinct vectors $\mathbf{x}_1, \dots, \mathbf{x}_k \in X$ (distinct from $\mathbf{y}$) such that*

$$\mathbf{y} = \sum_{j=1}^{k} c_j \mathbf{x}_j$$

for some scalars $c_1, \dots, c_k \in \mathbb{R}$.

Proof. 1. • $(\implies)$. Suppose that a vector $\mathbf{u} \in \operatorname{Span} X$ can be expressed in two ways as a linear combination of vectors $\mathbf{x}_1, \dots, \mathbf{x}_k \in X$:

$$\sum_{j=1}^{k} a_j \mathbf{x}_j = \mathbf{u} = \sum_{j=1}^{k} b_j \mathbf{x}_j.$$

Subtracting $\mathbf{u}$ gives us

$$\mathbf{0} = \sum_{j=1}^{k} (a_j - b_j)\mathbf{x}_j.$$

Since X is assumed to be linearly independent then for all $1 \leq j \leq n$ we have

$$a_j - b_j = 0.$$

• $(\impliedby)$. Let $\mathbf{x}_1, \dots, \mathbf{x}_k \in X$ be distinct and suppose that

$$\mathbf{0} = \sum_{j=1}^{k} c_j \mathbf{x}_j$$

for some scalars $c_1, \dots, c_k \in \mathbb{R}$. But we also have

$$\mathbf{0} = \sum_{j=1}^{k} 0\mathbf{x}_j,$$

so by the uniqueness assumption then $c_1 = \cdots = c_k = 0$.

2. • $(\implies)$. Suppose X is linearly dependent. Then by definition there exist distinct vectors $\mathbf{x}_1, \dots, \mathbf{x}_{k+1} \in X$ and scalars $a_1, \dots, a_{k+1} \in \mathbb{R}$ such that

$$\mathbf{0} = \sum_{j=1}^{k+1} a_j \mathbf{x}_j,$$

where at least one of the scalars $a_1, \dots, a_{k+1}$ is non-zero. Without loss of generality, let's assume $a_{k+1} \neq 0$. Then we can rearrange to get

$$\mathbf{x}_{k+1} = \sum_{j=1}^{k} \frac{-a_j}{a_{k+1}} \mathbf{x}_j.$$

- $(\Longleftarrow)$. Suppose there exists a vector $\mathbf{y} \in X$ and distinct vectors $\mathbf{x}_1, \ldots, \mathbf{x}_k \in X$ (distinct from $\mathbf{y}$) such that

  $$\mathbf{y} = \sum_{j=1}^{k} c_j \mathbf{x}_j.$$

  Then rearranging gives us

  $$\mathbf{0} = c_1\mathbf{x}_1 + \cdots c_k\mathbf{x}_k - 1\mathbf{y},$$

  so X is linearly dependent.

□

Exercise 2.3.15

Let V be an $\mathbb{R}$-vector space and $X \subseteq V$. Prove that X is linearly dependent if and only if every vector $\mathbf{v} \in \operatorname{Span} X$ can be expressed in more than one way as a linear combination of the vectors in X.
(Hint: By Definition 2.3.11, X is linearly dependent if and only if $\mathbf{0}$ can be written in more than one way as a linear combination of the vectors in X)

2.3.3 Bases

Definition 2.3.16

A subset $B \subseteq V$ is said to be a ***basis*** *for V if B is linearly independent and $\operatorname{Span} B = V$. If B is totally ordered (i.e. a list), then we call it an* ***ordered basis*** *(or* ***frame****) for V.*

The following Corollary is immediate from part (1) of Proposition 2.3.14.

Corollary 2.3.17

Let V be an $\mathbb{R}$-vector space, and let $B \subseteq V$. B is a basis for V if and only if every vector in V can be written uniquely as a linear combination of distinct vectors from B.

Corollary 2.3.17 says that a basis can serve as a coordinate system—this will be explored in more detail in MATHS 250, but we give a preview in the remark below:

Remark 2.3.18

Let V be an $\mathbb{R}$-vector space, and suppose that $B := (\mathbf{b}_1, \dots, \mathbf{b}_n)$ is an ordered basis for V. Then by Corollary 2.3.17, every vector $\mathbf{v} \in V$ can be expressed uniquely as

$$\mathbf{v} = \sum_{j=1}^{n} c_j \mathbf{b}_j.$$

*The unique scalars $c_j \in \mathbb{R}$ are called the **coordinates** of $\mathbf{v}$ with respect to the ordered basis B. This allows us to define the **coordinate mapping***

$$[\_]_B : \quad V \longrightarrow \mathbb{R}^n$$

where

$$[\mathbf{v}]_B := \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

Notice that for any $\mathbf{x} \in \mathbb{R}^n$ we have

$$\begin{aligned} \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} &= \begin{bmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ x_2 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \begin{bmatrix} 0 \\ 0 \\ \vdots \\ x_n \end{bmatrix} \\ &= x_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + x_n \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}. \end{aligned}$$

By Corollary 2.3.17, we have thus found a basis for $\mathbb{R}^n$.

Definition 2.3.19

*The **standard ordered basis** of $\mathbb{R}^n$ is the list $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ where $\mathbf{e}_j \in \mathbb{R}^n$ is the unique vector such that*

$$\operatorname{row}_i(\mathbf{e}_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Example 2.3.20

It can be shown that $\left\{\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}\right\}$ *(from Example 2.3.12) spans* $\mathbb{R}^3$*. Since we have already shown that this set is linearly independent, then it is a basis for* $\mathbb{R}^3$*.*

Example 2.3.21

Let V be a vector space, and consider the empty subset $\emptyset \subseteq V$. Since $\operatorname{Span}\emptyset = \{\mathbf{0}\}$ *by Example 2.3.6 and $\emptyset$ is linearly independent by Example 2.3.13 then $\emptyset$ is a basis for the linear subspace* $\{\mathbf{0}\} \subseteq V$*.*

Theorem 2.3.22

Let V be an $\mathbb{R}$-vector space. Let $X \subseteq V$ be any subset, and let $B, B' \subseteq V$ both be bases for V. Then the following hold:

1. $|X| > |B| \implies X$ *is linearly dependent;*
2. $|X| < |B| \implies \operatorname{Span} X \neq V$
3. $|B| = |B'|$.

Proof. Though this theorem is true more generally, we will prove it in the case where B and B' are finite sets.

1. Let $B := \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Choose $m > n$ distinct vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m \in X$, and let

$$S := \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}.$$

Since B is a basis, we can express every vector $\mathbf{v}_i$ as a linear combination of the vectors in B, say

$$\mathbf{v}_i = \sum_{j=1}^{n} a_{i,j}\mathbf{b}_j.$$

We have to show that S is linearly dependent, so consider the equation

$$c_1\mathbf{v}_1 + \cdots + c_m\mathbf{v}_m = \mathbf{0}.$$

Replacing and grouping terms together in the $\mathbf{b}_j$'s yields

$$(c_1a_{1,1} + \cdots + c_ma_{m,1})\mathbf{b}_1 + \cdots + (c_1a_{1,n} + \cdots + c_ma_{m,n})\mathbf{b}_n = \mathbf{0}$$

Since the $\mathbf{b}_j$'s are linearly independent all these coefficients have to be zero. This gives us the homogeneous linear system

$$\begin{aligned} c_1 a_{1,1} + \cdots + c_m a_{m,1} &= 0 \\ &\vdots \\ c_1 a_{1,n} + \cdots + c_m a_{m,n} &= 0 \end{aligned}$$

which consists of n equations in the m unknowns $c_1, \ldots, c_m$. Since $m > n$, this system has at least one non-trivial solution, which proves that S is linearly dependent.

2. We can use a similar approach to part (1). It is a bit tedious to write out, so we leave it as a (tricky) exercise for the reader.

3. This follows immediately from parts (1) and (2).

□

Corollary 2.3.23

Let V be an n-dimensional vector space, where $n \in \mathbb{N}$. Let $X \subseteq V$ be a subset with $|X| = n$. Then the following hold:

1. *X linearly independent $\implies$ X is a basis for V*
2. *$\operatorname{Span} X = V \implies X$ is a basis for V*

By part (3) of Theorem 2.3.22, every possible basis of a given vector space must have the same cardinality. Thus, we give this quantity a name:

Definition 2.3.24

*Let V be a vector space, and let $B \subseteq V$ be a basis. The **dimension** of V is defined to be*

$$\dim V := |B|.$$

*If $\dim V$ is finite then we say that V is **finite-dimensional**. If $\dim V$ is infinite then we say that V is **infinite-dimensional**.*

Example 2.3.25

- $\dim \mathbb{R}^n = |\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}| = n$.
- $\dim\{\mathbf{0}\} = |\emptyset| = 0$, *by Example 2.3.21.*

Exercise 2.3.26

1. $\dim(\mathbb{R}_k[x]) =$
2. $\dim(\mathbb{R}[x]) =$

2.4 Geometry

2.4.1 Lines and planes in $\mathbb{R}^n$

Depending on the context, we sometimes call elements of $\mathbb{R}^n$ **points**.

Definition 2.4.1

Let $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ with $\mathbf{v} \neq \mathbf{0}$. The ***line*** *$L$* ***through*** *$\mathbf{w}$* ***with direction vector*** *$\mathbf{v}$ is the set*

$$\{\mathbf{w} + \lambda\mathbf{v} : \lambda \in \mathbb{R}\}.$$

We also call L the ***line through*** *$\mathbf{w}$* ***parallel to*** *$\mathbf{v}$. The set L is depicted in Figure 2.6.*

The equation $\lambda\mathbf{v} + \mathbf{w}$ is called a ***parametric equation*** *for L (λ is the* ***parameter****). The elements of L are usually thought of as points. They are said to be* ***on the line*** *L.*

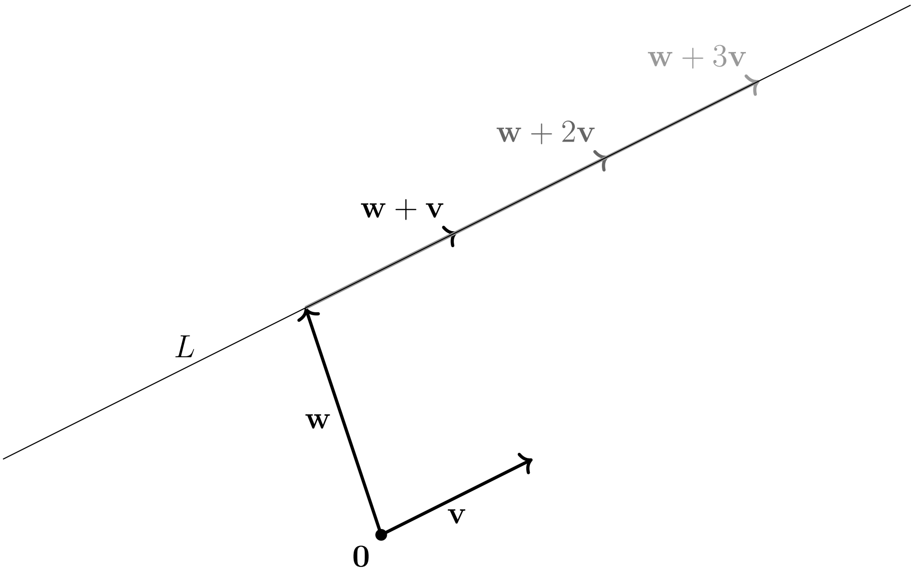

$\mathbf{w} + 3\mathbf{v}$
$\mathbf{w} + 2\mathbf{v}$
$\mathbf{w} + \mathbf{v}$
L
$\mathbf{w}$
$\mathbf{v}$
$\mathbf{0}$

Figure 2.6: The line L with direction vector $\mathbf{v}$ through $\mathbf{w}$.

Note that replacing the direction vector $\mathbf{v}$ by a scalar multiple does not change the line L, and neither does replacing $\mathbf{w}$ by another point on L.

In particular, there are many parametric equations for a given line.

Example 2.4.2: The line through two points

If $\mathbf{u}, \mathbf{w} \in \mathbb{R}^n$*, then*

$$\{\, \lambda(\mathbf{u} - \mathbf{w}) + \mathbf{w} : \lambda \in \mathbb{R} \,\}$$

contains $\mathbf{u}$ *and* $\mathbf{w}$*:* $\lambda = 0$ *yields* $\mathbf{w}$ *and* $\lambda = 1$ *yields* $\mathbf{u}$*. If* $\mathbf{u} \neq \mathbf{w}$*, then this is the equation for a line, and it is unique.*

Note that this can also be written as

$$\{\, \lambda\mathbf{u} + (1 - \lambda)\mathbf{w} : \lambda \in \mathbb{R} \,\}.$$

Definition 2.4.3

Let $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ *with* $\{\mathbf{u}, \mathbf{v}\}$ *linearly independent. The* ***plane*** P ***through*** $\mathbf{w}$ ***with direction vectors*** $\mathbf{u}$ ***and*** $\mathbf{v}$ *is*

$$\{\, \lambda\mathbf{u} + \mu\mathbf{v} + \mathbf{w} : \lambda, \mu \in \mathbb{R} \,\}.$$

We also call P *the* ***plane through*** $\mathbf{w}$ ***parallel to*** $\mathbf{u}$ ***and*** $\mathbf{v}$*.*

The equation $\lambda\mathbf{u} + \mu\mathbf{v} + \mathbf{w}$ *is called a* ***parametric equation*** *for* P *(with* μ *and* λ *being the* ***parameters****). The elements of* P *are usually thought of as points. They are said to be* ***on the plane*** P*.*

As in the case of lines, there are many parametric equations for a given plane: we can replace $\mathbf{w}$ by any vector on the plane, and $\{\mathbf{u}, \mathbf{v}\}$ can be replaced by any two linearly independent vectors that are linear combinations of $\{\mathbf{u}, \mathbf{v}\}$.

Example 2.4.4: Plane through three points

If $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$*, then*

$$\{\, \lambda(\mathbf{u} - \mathbf{w}) + \mu(\mathbf{v} - \mathbf{w}) + \mathbf{w} : \lambda, \mu \in \mathbb{R} \,\}$$

contains $\mathbf{u}$*,* $\mathbf{v}$ *and* $\mathbf{w}$*:* $\lambda = \mu = 0$ *yields* $\mathbf{w}$*,* $(\lambda, \mu) = (1, 0)$ *yields* $\mathbf{u}$ *and* $(\lambda, \mu) = (0, 1)$ *yields* $\mathbf{v}$*. If* $\mathbf{u}$*,* $\mathbf{v}$ *and* $\mathbf{w}$ *are not collinear, then this is a plane, and it is unique.*

Note that this can also be written as

$$\{\, \lambda\mathbf{u} + \mu\mathbf{v} + (1 - \lambda - \mu)\mathbf{w} : \lambda, \mu \in \mathbb{R} \,\}.$$

Remark 2.4.5

One can generalise this procedure and keep increasing the number of direction vectors. If there are m linearly independent direction vectors (and m parameters), the resulting object is an ***affine subspace*** *of $\mathbb{R}^n$ called an* ***(affine) hyperplane*** *of dimension m.*

Example 2.4.6

Let $\mathbf{u}$ and $\mathbf{v}$ be linearly independent vectors in $\mathbb{R}^n$ and let T be the triangle with vertices $\{\mathbf{0}, \mathbf{u}, \mathbf{v}\}$ (Figure 2.7). Suppose that $\mathbf{w} = \frac{1}{2}\mathbf{u} + \frac{1}{2}\mathbf{v}$ and $\mathbf{x} = \frac{1}{2}\mathbf{u}$, and let $\boldsymbol{m}$ be the intersection point of the line through $\mathbf{0}$ and $\mathbf{w}$, and the line through $\mathbf{v}$ and $\mathbf{x}$. Show that $\boldsymbol{m} = \frac{2}{3}\mathbf{w}$.

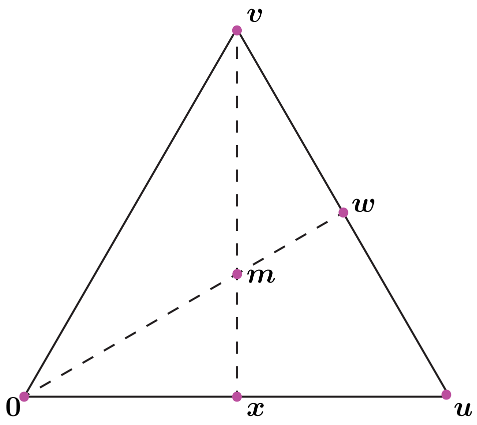


Figure 2.7: The triangle of Example 2.4.6.

Solution.
The line through $\mathbf{0}$ and $\mathbf{w}$ is given by:

$$\{\, \lambda\mathbf{w} : \lambda \in \mathbb{R} \,\} = \left\{\, \lambda\left(\tfrac{1}{2}\mathbf{u} + \tfrac{1}{2}\mathbf{v}\right) : \lambda \in \mathbb{R} \,\right\}.$$

The line through $\mathbf{v}$ and $\mathbf{x}$ is:

$$\{\, \mu\mathbf{x} + (1-\mu)\mathbf{v} : \mu \in \mathbb{R} \,\} = \left\{\, \mu\tfrac{1}{2}\mathbf{u} + (1-\mu)\mathbf{v} : \mu \in \mathbb{R} \,\right\}.$$

Consequently at $\boldsymbol{m}$,

$$\lambda\left(\tfrac{1}{2}\mathbf{u} + \tfrac{1}{2}\mathbf{v}\right) = \mu\tfrac{1}{2}\mathbf{u} + (1-\mu)\mathbf{v}$$

and so

$$\left(\frac{\lambda}{2}-\frac{\mu}{2}\right)\mathbf{u}-\left(1-\mu-\frac{\lambda}{2}\right)\mathbf{v}=\mathbf{0}.$$

Since u and v are linearly independent we have

$$\left(\frac{\lambda}{2}-\frac{\mu}{2}\right)=0 \qquad \text{and} \qquad \left(1-\mu-\frac{\lambda}{2}\right)=0.$$

Therefore $\lambda=\mu=2/3$ and so $\boldsymbol{m}=\frac{1}{3}\mathbf{u}+\frac{1}{3}\mathbf{v}=\frac{2}{3}\mathbf{w}$, as required.

Besides parametric equations, there is another way to describe lines and planes of $\mathbb{R}^n$, namely as solutions to systems of linear equations in the coordinates. This is called a **Cartesian equation**.

The simplest case is when there is just one equation. In this case, the set of solutions has "dimension" one less than the ambient space. For example, starting in $\mathbb{R}^2$, which has dimension 2, we obtain a set of dimension 1, namely a line. Starting in $\mathbb{R}^3$, we obtain a set of dimension 2, namely a plane.

Example 2.4.7

Find a Cartesian equation for

(i) the line through $\begin{bmatrix}2\\3\end{bmatrix}$ *with direction vector* $\begin{bmatrix}4\\1\end{bmatrix}$*;*

(ii) the plane through $\begin{bmatrix}6\\2\\1\end{bmatrix}$ *with directions vectors* $\begin{bmatrix}2\\1\\1\end{bmatrix}, \begin{bmatrix}3\\1\\-1\end{bmatrix}$.

Solution. (i) The line is $\left\{\lambda\begin{bmatrix}4\\1\end{bmatrix}+\begin{bmatrix}2\\3\end{bmatrix}, \lambda\in\mathbb{R}\right\}$. Let $\begin{bmatrix}x\\y\end{bmatrix}$ be a point on the line. Equating coefficients, we find $x=4\lambda+2$ and $y=\lambda+3$. Eliminating the parameter λ yields $x-4y+10=0$.

(ii) The plane is $\left\{\lambda\begin{bmatrix}2\\1\\1\end{bmatrix}+\mu\begin{bmatrix}3\\1\\-1\end{bmatrix}+\begin{bmatrix}6\\2\\1\end{bmatrix}, \lambda,\mu\in\mathbb{R}\right\}$. Let $\begin{bmatrix}x\\y\\z\end{bmatrix}$ be a point on the line. Equating coefficients, we find

$$\begin{aligned}x&=2\lambda+3\mu+6\\y&=\lambda+\mu+2\\z&=\lambda-\mu+1\end{aligned}$$

We may now eliminate the parameters from these two equations to obtain $2x-5y+z-3=0$.

In general, a Cartesian equation for a line in $\mathbb{R}^2$ has the form

$$ax + by + c = 0$$

with $(a, b) \neq (0, 0)$. The line is then the set

$$\left\{ \begin{bmatrix} x \\ y \end{bmatrix} : ax + by + c = 0 \right\}.$$

Similarly, a Cartesian equation for a plane in $\mathbb{R}^3$ has the form

$$ax + by + cz + d = 0$$

with $(a, b, c) \neq (0, 0, 0)$.

Note that, just like for parametric equations, lines and planes have many defining Cartesian equations. For example, we can multiply the whole equation by a non-zero scalar to get an equivalent equation.

We can also reverse the procedure from Example 2.4.7, that is, given a Cartesian equation for a line or a plane we may find find a parametric equation.

Example 2.4.8

Find parametric equations for

1. *the line with Cartesian equation* $2x + y = 4$*;*
2. *the plane with Cartesian equation* $2x + 3y + z = 6$.

Solution.

1. We first find two distinct points on the line, such as $\mathbf{u} = \begin{bmatrix} 0 \\ 4 \end{bmatrix}$ and $\mathbf{w} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$. Next, following Example 2.4.2, the Cartesian equation for the line is

$$\begin{aligned} \{\, \lambda(\mathbf{u} - \mathbf{w}) + \mathbf{w} : \lambda \in \mathbb{R} \,\} &= \left\{ \lambda \left(\begin{bmatrix} 0 \\ 4 \end{bmatrix} - \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right) + \begin{bmatrix} 1 \\ 2 \end{bmatrix} : \lambda \in \mathbb{R} \right\} \\ &= \left\{ \lambda \begin{bmatrix} -1 \\ 2 \end{bmatrix} + \begin{bmatrix} 1 \\ 2 \end{bmatrix} : \lambda \in \mathbb{R} \right\}. \end{aligned}$$

2. Similarly, we can find three non-collinear points on the plane and then follow Example 2.4.4 to find the parametric equation for the plane.

As mentioned earlier, the set of solutions to a single linear equation has "dimension" one less than the ambient space. If we have two "independent" linear equations, then the set of solutions has dimension two less. For example, two linear equations in $\mathbb{R}^3$ usually determine a line. Geometrically, this line is the intersection between the two planes defined by each of the equations. Note that problems arise if the two planes are parallel. What would this imply for the two equations that define these parallel planes?

Example 2.4.9

Find a pair of Cartesian equations that describe the line through $\begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}$ *with direction vector* $\begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}$.

Solution.

The line is $\left\{ \lambda \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} : \lambda \in \mathbb{R} \right\}$. Let $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$ be a point on the line. Equating coefficients, we find

$$\begin{aligned} x &= 2\lambda + 3 \\ y &= \lambda + 2 \\ z &= \lambda + 1. \end{aligned}$$

We can then isolate λ in one of the equations, say $\lambda = z - 1$, and substitute it into the other two, to get

$$\begin{aligned} x &= 2(z-1) + 3 = 2z + 1 \\ y &= (z-1) + 1 = z + 1. \end{aligned}$$

Rewriting, we get a pair of Cartesian equations:

$$\begin{aligned} x - 2z - 1 &= 0 \\ y - z - 1 &= 0. \end{aligned}$$

Exercise 2.4.10

Let P be a plane in $\mathbb{R}^3$. Show that if $\mathbf{0} \in P$, then $(\mathbf{x}, \boldsymbol{y} \in P) \implies (\mathbf{x} + \boldsymbol{y} \in P)$; and $(\mathbf{x} \in P, \lambda \in \mathbb{R}) \implies \lambda\mathbf{x} \in P$.

Conversely, show that if $\mathbf{0} \notin P$, then there exist $\mathbf{x}, \boldsymbol{y} \in P$ such that $\mathbf{x} + \boldsymbol{y} \notin P$; and there exist $\mathbf{x} \in P$ and $\lambda \in \mathbb{R}$ such that $\lambda\mathbf{x} \notin P$.

2.4.2 Euclidean length, distance and angle

The notions of lengths, distances, and angles in $\mathbb{R}^2$ and $\mathbb{R}^3$ will be familiar to you from everyday life and your studies of Euclidean geometry in school. We will show how to define these concepts more generally in $\mathbb{R}^n$, where n is any natural number.

But first, we will define a less familiar operation called the Euclidean scalar product, and we will show that all of the aforementioned concepts in Euclidean geometry follows from this.

Euclidean scalar product

Definition 2.4.11

*The **Euclidean scalar product** (or **dot product**, or **Euclidean inner product**) on $\mathbb{R}^n$ is the binary function*

$$(\_)\cdot(\_):\quad \mathbb{R}^n\times\mathbb{R}^n \longrightarrow \mathbb{R}$$

defined by the formula

$$\mathbf{u}\cdot\mathbf{v} := \sum_{i=1}^{n} u_i v_i = u_1\,v_1 + \cdots + u_n\,v_n.$$

The name "scalar product" comes from the fact that the output is a scalar (a real number). The name "dot product" comes from the notation.

Example 2.4.12

$$\begin{bmatrix}-1\\1\\2\end{bmatrix}\cdot\begin{bmatrix}1\\0\\2\end{bmatrix} = (-1)(1)+(1)(0)+(2)(2) = 3.$$

Proposition 2.4.13: Properties of scalar product

The dot product on $\mathbb{R}^n$ satisfies the following properties for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and all $a \in \mathbb{R}$:

1. ***Bilinear**.*

   (i) ***Biadditive**.*

   - $(\mathbf{u} + \mathbf{v}) \cdot \mathbf{w} = \mathbf{u} \cdot \mathbf{w} + \mathbf{v} \cdot \mathbf{w}$
   - $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$

   (ii) ***Bihomogeneous**.*

   - $(a\mathbf{u}) \cdot \mathbf{v} = a\,(\mathbf{u} \cdot \mathbf{v})$
   - $\mathbf{u} \cdot (a\mathbf{v}) = a(\mathbf{u} \cdot \mathbf{v})$

2. ***Commutative** (or **symmetric**). $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$*

3. ***Positive definite**.*

   (i) $\mathbf{u} \cdot \mathbf{u} \geq 0$

   (ii) $\mathbf{u} \cdot \mathbf{u} = 0 \implies \mathbf{u} = 0$

Proof. We prove that the dot product is positive definite and leave the remainder as an exercise. Let $\mathbf{u} := \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \in \mathbb{R}^n$ be an arbitrary vector. Since $u_i^2 \geq 0$ for each $1 \leq i \leq n$, then we have

$$\mathbf{u} \cdot \mathbf{u} = \sum_{i=1}^{n} u_i u_i = \sum_{i=1}^{n} u_i^2 \geq 0.$$

We can also see that $\mathbf{u} \cdot \mathbf{u} = 0$ if and only if $u_i = 0$ for all $1 \leq i \leq n$. □

Remark 2.4.14

*More generally, a **scalar product** on a real vector space V is a binary operation*

$$\langle \_, \_ \rangle : \quad V \times V \longrightarrow \mathbb{R}$$

which satisfies all three properties in Proposition 2.4.13 above. We will only deal with the Euclidean scalar product on $\mathbb{R}^n$ in this course, but you will see other examples of scalar products in MATHS 250.

The following inequality involving the Euclidean scalar product will be useful shortly:

Theorem 2.4.15: Cauchy-Schwartz inequality

Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$*. Then*

$$|\mathbf{u} \cdot \mathbf{v}|^2 \leq (\mathbf{u} \cdot \mathbf{u})(\mathbf{v} \cdot \mathbf{v}),$$

and equality holds if and only if $\mathbf{u}$ *and* $\mathbf{v}$ *are scalar multiples.*

Proof. It is an exercise to show the following:

- The theorem is true if $\mathbf{u}$ or $\mathbf{v}$ is $\mathbf{0}$.
- If $\mathbf{u}$ and $\mathbf{v}$ are scalar multiples, then $|\mathbf{u} \cdot \mathbf{v}|^2 = (\mathbf{u} \cdot \mathbf{u})(\mathbf{v} \cdot \mathbf{v})$.

Thus we will assume for the remainder of this proof that both $\mathbf{u}$ and $\mathbf{v}$ are non-zero; further, if equality holds, we only need to prove that $\mathbf{u}$ and $\mathbf{v}$ are scalar multiples.

We will use the properties listed in Proposition 2.4.13 without comment. Define the real number $\lambda = (\mathbf{u} \cdot \mathbf{v})\|\mathbf{v}\|^{-2}$; this is allowed, since $\mathbf{v} \neq \mathbf{0}$ so $\|\mathbf{v}\| \neq 0$. Now observe that

$$\begin{aligned} 0 &\leq \|\mathbf{u} - \lambda\mathbf{v}\|^2 \\ &= (\mathbf{u} - \lambda\mathbf{v}) \cdot (\mathbf{u} - \lambda\mathbf{v}) \\ &= \mathbf{u} \cdot \mathbf{u} - 2\lambda\mathbf{v} \cdot \mathbf{u} + \lambda^2\mathbf{v} \cdot \mathbf{v} \\ &= \|\mathbf{u}\|^2 - 2\lambda\mathbf{v} \cdot \mathbf{u} + \lambda^2\|\mathbf{v}\|^2 \\ &= \|\mathbf{u}\|^2 - 2\frac{1}{\|\mathbf{v}\|^2}(\mathbf{v} \cdot \mathbf{u})^2 + \frac{1}{\|\mathbf{v}\|^2}(\mathbf{u} \cdot \mathbf{v})^2 \\ &= \|\mathbf{u}\|^2 - \frac{1}{\|\mathbf{v}\|^2}(\mathbf{v} \cdot \mathbf{u})^2 \end{aligned}$$

Rearranging, we have the desired inequality. If the inequality is an equality, we have $0 = \|\mathbf{u} - \lambda\mathbf{v}\|^2$ and so $\mathbf{u} = \lambda\mathbf{v}$ as desired. □

Remark 2.4.16

While almost all of the linear algebra content in this course works in the same way for the case of real and complex vectors spaces, this subsection is an exception! The standard scalar product on $\mathbb{C}^n$ is defined to be the binary function

$$\langle \_, \_ \rangle : \quad \mathbb{C}^n \times \mathbb{C}^n \longrightarrow \mathbb{C}$$

given by the formula

$$\langle \mathbf{u}, \mathbf{v} \rangle := \sum_{i=1}^{n} \overline{u_i} v_i = \overline{u_1}\, v_1 + \cdots + \overline{u_n}\, v_n.$$

Note that this looks almost the same as in the real case, but we take the complex conjugate of the first vector.

We will not use complex scalar products in this course, but they are essential for quantum mechanics and many areas of mathematics.

Euclidean length and distance

The Euclidean dot product on $\mathbb{R}^n$ allows us to define the length of a vector in $\mathbb{R}^n$. Essentially, the formula is just Pythagoras' Theorem, generalised to $\mathbb{R}^n$.

Definition 2.4.17

The ***Euclidean length*** *(or* ***Euclidean norm****) on $\mathbb{R}^n$ is the function*

$$\|\_\| : \quad \mathbb{R}^n \longrightarrow \mathbb{R}$$

defined by the rule

$$\|\mathbf{u}\| := \sqrt{\mathbf{u} \cdot \mathbf{u}} = \sqrt{\sum_{i=1}^{n} u_i^2}$$

Example 2.4.18

The Euclidean length of the vector $\begin{bmatrix} -1 \\ 2 \\ 3 \end{bmatrix}$ *is*

$$\left\| \begin{bmatrix} -1 \\ 2 \\ 3 \end{bmatrix} \right\| = \sqrt{(-1)^2 + 2^2 + 3^3} = \sqrt{14}.$$

Armed with the definition of Euclidean length, we easily get the following corollary of the Cauchy-Schwartz inequality:

Corollary 2.4.19

For all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$*,*

$$(\mathbf{u} \cdot \mathbf{v}) \leq \|\mathbf{u}\|\|\mathbf{v}\|.$$

Proof. Take the square root of both sides of the Cauchy-Schwartz inequality. □

We will use this to prove the triangle inequality below:

Proposition 2.4.20: Properties of length

The Euclidean length satisfies the following properties for all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ *and all* $a \in \mathbb{R}$.

1. ***Absolutely homogeneous.*** $\|a\mathbf{u}\| = |a|\|\mathbf{u}\|$
2. ***Triangle inequality.*** $\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$
3. ***Positive definite.***

   (i) $\|\mathbf{u}\| \geq 0$

   (ii) $\|\mathbf{u}\| = 0 \implies \mathbf{u} = 0$

Proof. Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$.

1. Using bilinearity of the dot product, we have

   $$\|a\mathbf{u}\|^2 = (a\mathbf{u}) \cdot (a\mathbf{u}) = a^2 (\mathbf{u} \cdot \mathbf{u}) = a^2\|\mathbf{u}\|^2.$$

   We just take the square root to get the desired result.

2.

   $$\|\mathbf{u} + \mathbf{v}\|^2 = (\mathbf{u} + \mathbf{v}) \cdot (\mathbf{u} + \mathbf{v})$$

$$\begin{aligned}
&= \mathbf{u}\cdot\mathbf{u} + 2\mathbf{u}\cdot\mathbf{v} + \mathbf{v}\cdot\mathbf{v} \\
&= \|\mathbf{u}\|^2 + 2\mathbf{u}\cdot\mathbf{v} + \|\mathbf{v}\|^2 \\
&\leq \|\mathbf{u}\|^2 + 2\|\mathbf{u}\|\|\mathbf{v}\| + \|\mathbf{v}\|^2 \\
&= (\|\mathbf{u}\| + \|\mathbf{v}\|)^2,
\end{aligned}$$

where the inequality comes from Corollary 2.4.19.

3. This follows immediately from positive-definiteness of the dot product.

□

It is easy to see why the triangle inequality should be true. Consider Figure 2.8—the triangle inequality simply states that the shortest path from point A to point B cannot travel via any point C not on the straight line between them.

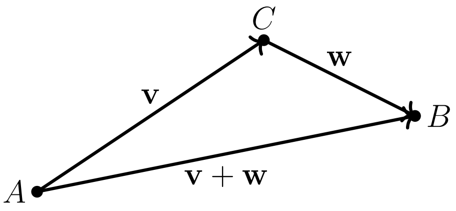


Figure 2.8: The triangle inequality.

Remark 2.4.21

More generally, a ***length function*** *(or* ***norm****) on a vector space V is a function*

$$\|\_\| : \quad V \longrightarrow \mathbb{R}$$

which satisfies all three properties in Proposition 2.4.20 above. We will only deal with the Euclidean length on $\mathbb{R}^n$ in this course, but you will see other examples of length functions in MATHS 254, such as the Manhattan norm.

Armed with the definition of the length of a vector in $\mathbb{R}^n$, we can now define the distance between two points:

Definition 2.4.22

Given $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, the ***Euclidean distance*** *between $\mathbf{u}$ and $\mathbf{v}$ is defined to be*

$$d(\mathbf{u},\mathbf{v}) \coloneqq \|\mathbf{v}-\mathbf{u}\|.$$

Example 2.4.23

$$d\left(\begin{bmatrix}1\\6\end{bmatrix},\begin{bmatrix}4\\-1\end{bmatrix}\right)=\sqrt{(4-1)^2+(-1-6)^2}=\sqrt{58}.$$

Exercise 2.4.24: The midpoint of a segment

Let $\mathbf{v},\mathbf{w}\in\mathbb{R}^3$ with $\mathbf{v}\neq\mathbf{w}$. Show that the set of all points equidistant from $\mathbf{v}$ and $\mathbf{w}$ forms a plane, and show that this plane intersects the line joining $\mathbf{v}$ and $\mathbf{w}$ at a single point, namely $\frac{1}{2}(\mathbf{v}+\mathbf{w})$.

Proposition 2.4.25: Properties of distance

The Euclidean distance satisfies the following properties for all $\mathbf{u},\mathbf{v},\mathbf{w}\in\mathbb{R}^n$.

1. ***Symmetry**. $d(\mathbf{u},\mathbf{v})=d(\mathbf{v},\mathbf{u})$*
2. ***Triangle inequality**. $d(\mathbf{u},\mathbf{w})\leq d(\mathbf{u},\mathbf{v})+d(\mathbf{v},\mathbf{w})$*
3. ***Separation**. $d(\mathbf{u},\mathbf{v})=0 \iff \mathbf{u}=\mathbf{v}$*

Proof. These directly follow from the properties of length proved in Proposition 2.4.20. We leave the details as an exercise. □

Remark 2.4.26

*More generally, a **distance function** (or **metric**) on a set X is a binary function*

$$d:\quad X\times X\longrightarrow[0,\infty)$$

which satisfies all three properties in Proposition 2.4.25 above. We will only deal with the Euclidean distance on $\mathbb{R}^n$ in this course, but you will see other examples of distance functions in MATHS 254, such as the Manhattan metric.

Perpendicular vectors

We will soon use the Euclidean dot product to define the (unsigned) angle between two vectors in $\mathbb{R}^n$. But first, we will consider the special case of perpendicular vectors:

Definition 2.4.27

- *We say that two vectors* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ *are* ***orthogonal*** *(or* ***perpendicular****) if* $\mathbf{u} \cdot \mathbf{v} = 0$.
- *We say that two vectors* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ *are* ***orthonormal*** *if they are orthogonal and both vectors have length* 1.
- *We say that a subset* $X \subseteq \mathbb{R}^n$ *is orthogonal (respectively, orthonormal) if each pair of distinct vectors from* X *is orthogonal (respectively, orthonormal).*

Example 2.4.28

The standard basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ *for* $\mathbb{R}^n$ *is orthonormal since*

$$\mathbf{e}_i \cdot \mathbf{e}_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Definition 2.4.29

Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$*, where* $\mathbf{v} \neq \mathbf{0}$*. The* ***orthogonal projection*** *of* $\mathbf{u}$ *onto* $\mathbf{v}$ *is the unique vector* $\operatorname{proj}_{\mathbf{v}} \mathbf{u} \in \mathbb{R}^n$ *such that*

1. $\operatorname{proj}_{\mathbf{v}} \mathbf{u} \in \operatorname{Span}\{\mathbf{v}\}$
2. $(\mathbf{u} - \operatorname{proj}_{\mathbf{v}} \mathbf{u}) \perp \mathbf{v}$.

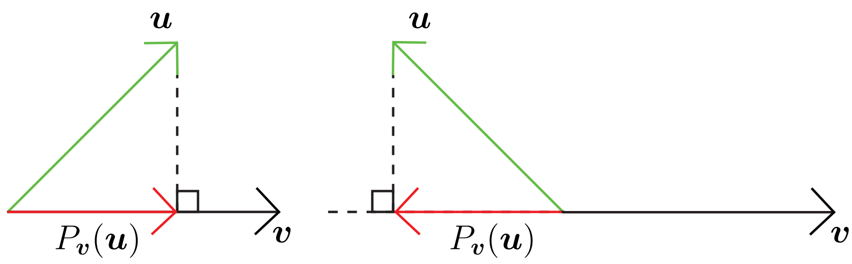


Figure 2.9: The orthogonal projection of a vector onto a line.

Lemma 2.4.30

Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, *where* $\mathbf{v} \neq \mathbf{0}$. *The orthogonal projection of* $\mathbf{u}$ *onto* $\mathbf{v}$ *is given by the formula*

$$\operatorname{proj}_{\mathbf{v}} \mathbf{u} := \left(\frac{\mathbf{v} \cdot \mathbf{u}}{\|\mathbf{v}\|^2}\right) \mathbf{v}.$$

Proof. We want to find $\lambda \in \mathbb{R}$ such that $\operatorname{proj}_{\mathbf{v}}(\mathbf{u}) = \lambda \mathbf{v}$ and such that $\mathbf{u} - \operatorname{proj}_{\mathbf{v}}(\mathbf{u})$ is orthogonal to $\mathbf{v}$, that is, $(\mathbf{u} - \operatorname{proj}_{\mathbf{v}}(\mathbf{u})) \cdot \mathbf{v} = 0$. Combining these, we have

$$0 = (\mathbf{u} - \lambda\mathbf{v}) \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{v} - \lambda \mathbf{v} \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{v} - \lambda \|\mathbf{v}\|^2,$$

so $\lambda \|\mathbf{v}\|^2 = \mathbf{u} \cdot \mathbf{v}$ and

$$\lambda = \frac{\mathbf{u} \cdot \mathbf{v}}{\|\mathbf{v}\|^2}.$$

Hence $\operatorname{proj}_{\mathbf{v}}(\mathbf{u}) = \lambda \mathbf{v} = \left(\frac{\mathbf{u} \cdot \mathbf{v}}{\|\mathbf{v}\|^2}\right) \mathbf{v}$. □

Example 2.4.31

Find the orthogonal projection of $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ *onto* $\begin{bmatrix} -3 \\ 0 \\ 4 \end{bmatrix}$.

Solution.
Let $\mathbf{u} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ and $\mathbf{v} = \begin{bmatrix} -3 \\ 0 \\ 4 \end{bmatrix}$. We have $\mathbf{u} \cdot \mathbf{v} = 1(-3) + 2(0) + 3(4) = 9$, while $\|\mathbf{v}\|^2 = 25$ so $\operatorname{proj}_{\mathbf{v}}(\mathbf{u}) = \frac{9}{25}\mathbf{v}$.

Exercise 2.4.32

Let $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ *be an orthogonal basis for* $\mathbb{R}^n$. *Prove that for any vector* $\mathbf{u} \in \mathbb{R}^n$ *we have*

$$\mathbf{u} = \sum_{i=1}^{n} \operatorname{proj}_{\mathbf{b}_i} \mathbf{u} = \sum_{i=1}^{n} \left(\frac{\mathbf{b}_i \cdot \mathbf{u}}{\|\mathbf{b}_i\|^2}\right) \mathbf{b}_i.$$

Theorem 2.4.33

The vector $\boldsymbol{a} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ *is perpendicular to every direction vector of the hyperplane*

$$S := \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{R}^n \;\middle|\; a_1x_1 + \cdots + a_nx_n + d = 0 \right\}.$$

Further, if $\mathbf{v} \in \mathbb{R}^n$ *also has this property, then* $\mathbf{v} = \lambda\boldsymbol{a}$ *for some* $\lambda \in \mathbb{R}$.

Proof. Writing $\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, we have

$$S = \{\mathbf{x} \in \mathbb{R}^n : \boldsymbol{a} \cdot \mathbf{x} = -d\}.$$

Now, if $\mathbf{v}$ is a direction vector for S, then $\mathbf{v} = \boldsymbol{y} - \mathbf{x}$ for some $\mathbf{x}, \boldsymbol{y} \in S$ and so

$$\boldsymbol{a} \cdot \mathbf{v} = \boldsymbol{a} \cdot (\boldsymbol{y} - \mathbf{x}) = \boldsymbol{a} \cdot \boldsymbol{y} - \boldsymbol{a} \cdot \mathbf{x} = -d - (-d) = 0.$$

The second result follows from the observation that the direction vectors of S together with $\boldsymbol{a}$ form a spanning set for $\mathbb{R}^n$ (exercise: one approach is to consider for arbitrary $\mathbf{x} \in V$ the line through $\mathbf{x}$ with direction vector $\boldsymbol{a}$, and to prove that this line intersects S in some point via the results in the previous section); we may conclude that there is a basis for $\mathbb{R}^n$ consisting of $\boldsymbol{a}$ together with $n-1$ direction vectors of S, say $\boldsymbol{v}_1, \ldots, \mathbf{v}_{n-1}$, and thus by Proposition 2.3.17 we may find $b_0, ..., b_{n-1} \in \mathbb{R}$ such that $\mathbf{v} = b_0\boldsymbol{a} + b_1\boldsymbol{v_1} + \cdots + b_{n-1}\boldsymbol{v_{n-1}}$. Now take the dot product of $\mathbf{v}$ and $\boldsymbol{a}$, and of $\mathbf{v}$ and $\mathbf{v}$:

$$\begin{aligned} \mathbf{v} \cdot \boldsymbol{a} &= b_0\boldsymbol{a} \cdot \boldsymbol{a} + b_1\boldsymbol{v_1} \cdot \boldsymbol{a} + \cdots + b_{n-1}\boldsymbol{v_{n-1}} \cdot \boldsymbol{a} = b_0\|\boldsymbol{a}\|^2, \\ \|\mathbf{v}\|^2 = \mathbf{v} \cdot \mathbf{v} &= b_0\boldsymbol{a} \cdot \mathbf{v} + b_1\boldsymbol{v_1} \cdot \mathbf{v} + \cdots + b_{n-1}\boldsymbol{v_{n-1}} \cdot \mathbf{v} = b_0(\boldsymbol{a} \cdot \mathbf{v}); \end{aligned}$$

hence taking the product of the left-hand side of the top equation and the right-hand side of the bottom equation and setting it equal to the product of the other two quantities, we have $b_0(\mathbf{v} \cdot \boldsymbol{a})^2 = b_0\|\boldsymbol{a}\|^2\|\mathbf{v}\|^2$. We now use the second part of the Cauchy-Schwartz inequality, Theorem 2.4.15, to conclude that $\mathbf{v}$ and $\boldsymbol{a}$ are scalar multiples. □

Note that the set S in Theorem 2.4.33 is defined by a single Cartesian equation and so it produces a line when $n = 2$ and a plane when $n = 3$ (assuming $\boldsymbol{a} \neq 0$).

We say that a non-zero vector is a **normal vector** to a line or plane if it is perpendicular to every direction vector of that line or plane.

Example 2.4.34

Find a Cartesian equation for the plane in $\mathbb{R}^3$ that contains the point $\begin{bmatrix}1\\2\\3\end{bmatrix}$ and has $\begin{bmatrix}2\\9\\6\end{bmatrix}$ as a normal vector.

Solution.
A Cartesian equation must be of the form $2x + 9y + 6z + d = 0$, by Theorem 2.4.33. Since the plane must contain the point $\begin{bmatrix}1\\2\\3\end{bmatrix}$, we have $2(1) + 9(2) + 6(3) + d = 0$, so $d = -38$ and a Cartesian equation is:

$$2x + 9y + 6z = 38.$$

Angles

Definition 2.4.35

Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$. We define the (unsigned) ***angle*** *between $\mathbf{u}$ and $\mathbf{v}$ to be*

$$\measuredangle(\mathbf{u}, \mathbf{v}) := \arccos\left(\frac{\mathbf{u} \cdot \mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|}\right)$$

Example 2.4.36

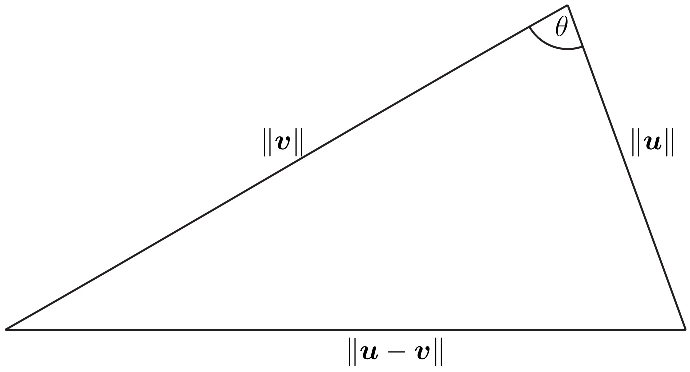
1. *The zero vector is orthogonal to every vector in $\mathbb{R}^n$.*
2. *Two non-zero vectors are orthogonal if and only if the angle between them is $\frac{\pi}{2}$.*
3. *Two non-zero vectors point in the same direction if and only if the angle between them is 0.*
4. *Two non-zero vectors point in opposite direction if and only if the angle between them is π.*

Notice that if two vectors are linearly dependent, then either their angle is 0 if they point in the same direction, or π if they point in opposite directions.

Recall that two linearly independent vectors, say, $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ span a plane in this n-dimensional vector space. Thus, our definition of angle given above should agree with the usual method of computing angles in Euclidean plane geometry.

Theorem 2.4.37

Let $\mathbf{u}$ and $\mathbf{v}$ be non-zero vectors in $\mathbb{R}^n$. Then the formula given in definition 2.4.35 for calculating the angle between them agrees with the traditional method of calculating angles in plane geometry.



$$\|\boldsymbol{u}-\boldsymbol{v}\| = \|\boldsymbol{u}\|^2 + \|\boldsymbol{v}\|^2 + 2\,\|\boldsymbol{u}\|\,\|\boldsymbol{v}\|\cos\theta$$

Figure 2.10: The angle between two vectors.

Proof. Let θ be the angle between $\mathbf{u}$ and $\mathbf{v}$ in the plane spanned by these two vectors—see in Figure 2.10.

In this plane spanned by $\mathbf{u}$ and $\mathbf{v}$, standard rules from Euclidean plane geometry apply.

By the cosine rule, we have

$$\|\mathbf{u}-\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\|\mathbf{u}\|\|\mathbf{v}\|\cos(\theta).$$

On the other hand, we have

$$\begin{aligned}\|\mathbf{u}-\mathbf{v}\|^2 &= (\mathbf{u}-\mathbf{v})\cdot(\mathbf{u}-\mathbf{v})\\ &= \mathbf{u}\cdot(\mathbf{u}-\mathbf{v}) - \mathbf{v}\cdot(\mathbf{u}-\mathbf{v})\\ &= \mathbf{u}\cdot\mathbf{u} - \mathbf{u}\cdot\mathbf{v} - \mathbf{v}\cdot\mathbf{u} + \mathbf{v}\cdot\mathbf{v}\\ &= \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2(\mathbf{u}\cdot\mathbf{v}).\end{aligned}$$

It follows that

$$\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\|\mathbf{u}\|\|\mathbf{v}\|\cos(\theta) = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2(\mathbf{u}\cdot\mathbf{v})$$

and the result follows. □

2.5 Linear functions

2.5.1 Linear functions

We now come to one of the most important concepts in linear algebra, that of a linear function. Given vector spaces U and V, we would like to pick out the functions from U to V that *preserve* the addition and scaling operations. This is made precise in the following definition:

Definition 2.5.1

*Let U and V be $\mathbb{R}$-vector spaces. A function $L : U \to V$ is said to be **linear** if for every $\mathbf{u}_1, \mathbf{u}_2 \in U$ and $c \in \mathbb{R}$, it satisfies the following properties:*

1. ***Additive**. $L(\mathbf{u}_1 + \mathbf{u}_2) = L(\mathbf{u}_1) + L(\mathbf{u}_2)$,*
2. ***Homogeneous**. $L(c\mathbf{u}_1) = c\,L(\mathbf{u}_1)$.*

Linear functions are also commonly called **linear transformations** or **linear maps**—these terms are synonymous. They can equivalently be characterised as functions which preserve linear combinations, in the following sense:

Exercise 2.5.2

Prove that a function $L : U \to V$ is linear if and only if

$$L\left(\sum_{i=1}^{k} c_i\mathbf{u}_i\right) = \sum_{i=1}^{k} c_i L(\mathbf{u}_i)$$

for all $\mathbf{u}_i \in U$ and all scalars c_i ($1 \le i \le k$).

It is easy to see that a linear function always sends the zero vector in the domain to the zero vector in the codomain:

Proposition 2.5.3

Let U and V be vector spaces. If $L : U \to V$ is a linear transformation then $L(\mathbf{0}) = \mathbf{0}$.

Proof. $L(\mathbf{0}) = L(0\mathbf{0}) = 0L(\mathbf{0}) = \mathbf{0}$. □

If you are unsure about whether or not a function $f : U \to V$ is linear, the first thing you should check is if it preserves the zero vector, i.e., check if $f(\mathbf{0}) = \mathbf{0}$. If it fails this test, then by Proposition 2.5.3 you immediately discover that f cannot be linear. Note that the converse of this proposition is false! You cannot conclude that a function is linear just from checking that it preserves the origin. For instance, the function g in the upcoming example below preserves the origin but fails to be linear.

More generally, linear transformations must preserve linear subspaces:

Proposition 2.5.4

Let $L : U \to V$ be a linear function. If $S \subseteq U$ is a linear subspace, then its image $L(S) \subseteq V$ is a linear subspace.

Proof. We leave this as a straightforward exercise.
(Hint: recall Definition 1.4.9, and Proposition 2.2.11.) □

Example 2.5.5

Which of the following functions are linear?

1. $f : \mathbb{R}^2 \to \mathbb{R}$
   $f\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) := \begin{bmatrix} x + y \end{bmatrix}.$
2. $g : \mathbb{R}^2 \to \mathbb{R}$
   $g\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) := \begin{bmatrix} xy \end{bmatrix}.$
3. $h : \mathbb{R} \to \mathbb{R}$
   $h(x) := x + 1.$

Solution. 1. We show that f is a linear transformation.

Let $\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}, \boldsymbol{w} = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \in \mathbb{R}^2$ and $c \in \mathbb{R}$. We have

$$\begin{aligned} f(\mathbf{v} + \boldsymbol{w}) &= f\left(\begin{bmatrix} v_1 \\ v_2 \end{bmatrix} + \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}\right) \\ &= f\left(\begin{bmatrix} v_1 + w_1 \\ v_2 + w_2 \end{bmatrix}\right) \\ &= \begin{bmatrix} v_1 + w_1 + v_2 + w_2 \end{bmatrix} \\ &= \begin{bmatrix} v_1 + v_2 \end{bmatrix} + \begin{bmatrix} w_1 + w_2 \end{bmatrix} \\ &= f\left(\begin{bmatrix} v_1 \\ v_2 \end{bmatrix}\right) + f\left(\begin{bmatrix} w_1 \\ w_2 \end{bmatrix}\right) \end{aligned}$$

$$= f(\mathbf{v}) + f(\boldsymbol{w})$$

and

$$\begin{aligned} f(c\,\mathbf{v}) &= f\left(c\begin{bmatrix} v_1 \\ v_2 \end{bmatrix}\right) \\ &= f\left(\begin{bmatrix} c\,v_1 \\ c\,v_2 \end{bmatrix}\right) \\ &= \begin{bmatrix} c\,v_1 + c\,v_2 \end{bmatrix} \\ &= c\begin{bmatrix} v_1 + v_2 \end{bmatrix} \\ &= c\,f\left(\begin{bmatrix} v_1 \\ v_2 \end{bmatrix}\right) \\ &= c\,f(\mathbf{v}). \end{aligned}$$

It follows that f is a linear transformation.

2. Although $g(\mathbf{0}) = 0$, the function g is not a linear transformation because, for example,

$$2g\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = 2\begin{bmatrix} 1 \end{bmatrix} = \begin{bmatrix} 2 \end{bmatrix}$$

whereas

$$g\left(2\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = g\left(\begin{bmatrix} 2 \\ 2 \end{bmatrix}\right) = \begin{bmatrix} 4 \end{bmatrix}.$$

3. $h(0) = 1 \neq 0$ so h cannot be linear.

Exercise 2.5.6

For each of the following functions, determine whether or not it is linear

1. $$\begin{array}{rrcl} \exp: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & e^x \end{array}$$

2. $$\begin{array}{rcl} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & ax+b \end{array} \qquad a, b \in \mathbb{R}$$

3. $$\begin{array}{rrcl} \mu: & \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ & \begin{bmatrix} x \\ y \end{bmatrix} & \longmapsto & xy \end{array}$$

4. $$\begin{array}{rrcl} R_\theta: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & \begin{bmatrix} x \\ y \end{bmatrix} & \longmapsto & \begin{bmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{bmatrix} \end{array} \qquad \theta \in \mathbb{R}$$

5. $||\_|| : \mathbb{R}^n \to \mathbb{R}$.

6. $$\begin{array}{rrcl} \text{proj}_{\mathbf{v}}: & \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ & \mathbf{u} & \longmapsto & \frac{\mathbf{v}\cdot\mathbf{u}}{||\mathbf{v}||^2}\mathbf{v} \end{array} \qquad \mathbf{v} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$$

7. $$\begin{array}{rrcl} \text{eval}_a: & \mathbb{R}[x] & \longrightarrow & \mathbb{R} \\ & p(x) & \longmapsto & p(a) \end{array} \qquad a \in \mathbb{R}$$

In the case of functions between 1-dimensional vector spaces, it is easy to describe all possible linear transformations:

Example 2.5.7

Let $f : \mathbb{R} \to \mathbb{R}$. Show that f is a linear transformation if and only if there exists a scalar $a \in \mathbb{R}$ such that $f(x) = ax$, for all $x \in \mathbb{R}$.

Solution.
We first assume that f is a linear transformation. Let $a = f(1)$. Now, since f is a linear transformation, $f(x) = f(x\,1) = x\,f(1) = x\,a$, for all $x \in \mathbb{R}$. The converse is easy to check.

Remark 2.5.8

It is possible that, in a previous course, you were taught that if $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = a\,x + b$, then it is linear. In more advanced mathematics courses, such functions are usually called ***affine transformations****, with the name "linear" reserved for the case $b = 0$. (So linear transformations are special cases of affine transformations.)*

Definition 2.5.9

Given $\mathbb{R}$-vector spaces U and V, we will denote the subset of all linear functions from U to V by $\operatorname{Lin}(U, V)$.

Given vector spaces U and V, recall from Example 2.2.9 that the set V^U of all functions from U to V is a vector space. It turns out that the subset $\operatorname{Lin}(U, V) \subseteq V^U$ is a linear subspace. In other words, scaling a linear function or adding together two linear functions produces another linear function!

Proposition 2.5.10

For any $\mathbb{R}$-vector spaces U and V, $\operatorname{Lin}(U, V)$ is a linear subspace of V^U.

Proof. Let $L, T \in \operatorname{Lin}(U, V)$, $\mathbf{u}_1, \mathbf{u}_2 \in U$, and let c be a scalar. We just verify the criteria in Proposition 2.2.11:

- The zero function is linear:

$$\begin{aligned} 0(\mathbf{u}_1 + \mathbf{u}_2) &= \mathbf{0} = \mathbf{0} + \mathbf{0} = 0(\mathbf{u}_1) + 0(\mathbf{u}_2), \\ 0(c\mathbf{u}_1) &= \mathbf{0} = c\mathbf{0} = c0(\mathbf{u}_1). \end{aligned}$$

- Sums of linear functions are linear:

$$\begin{aligned} (L + T)(\mathbf{u}_1 + \mathbf{u}_2) &= L(\mathbf{u}_1 + \mathbf{u}_2) + T(\mathbf{u}_1 + \mathbf{u}_2) \\ &= L(\mathbf{u}_1) + L(\mathbf{u}_2) + T(\mathbf{u}_1) + T(\mathbf{u}_2) \\ &= (L + T)(\mathbf{u}_1) + (L + T)(\mathbf{u}_2) \\ (L + T)(c\mathbf{u}_1) &= L(c\mathbf{u}_1) + T(c\mathbf{u}_1), \\ &= cL(\mathbf{u}_1) + cT(\mathbf{u}_1) \\ &= c(L(\mathbf{u}_1) + T(\mathbf{u}_1)) \\ &= c(L + T)(\mathbf{u}_1). \end{aligned}$$

- Scalar multiples of linear functions are linear. We leave this verification to the reader.

□

In other words, a linear combination of linear transformations is again a linear transformation. But it gets even better: it turns out that a composite of linear transformations is linear as well!

Proposition 2.5.11

Let U, V, and W be $\mathbb{R}$-vector spaces. Then the following hold:

1. *The identity function $\mathrm{id}_U : U \to U$ is linear.*
2. *If $L : U \to V$ and $T : V \to W$ are linear, then the composite $T \circ L : U \to W$ is linear.*

Proof. Let $\mathbf{u}, \mathbf{u}_1, \mathbf{u_2} \in U$, and let c be a scalar.

1. We verify that $\mathrm{id}_U : U \to U$ is linear:

$$\begin{aligned}\mathrm{id}_U(\mathbf{u}_1 + \mathbf{u}_2) &= \mathbf{u}_1 + \mathbf{u}_2 = \mathrm{id}_U(\mathbf{u}_1) + \mathrm{id}_U(\mathbf{u}_2),\\ \mathrm{id}_U(c\mathbf{u}) &= c\mathbf{u} = c\mathrm{id}_U(\mathbf{u}).\end{aligned}$$

2. Suppose that $L : U \to V$ and $T : V \to W$ are linear. We verify that the composite $T \circ L : U \to W$ is linear:

$$\begin{aligned}T(L(\mathbf{u}_1 + \mathbf{u}_2)) &= T(L(\mathbf{u}_1) + L(\mathbf{u}_2)) = T(L(\mathbf{u}_1)) + T(L(\mathbf{u}_2)),\\ T(L(c\mathbf{u})) &= T(cL(\mathbf{u})) = cT(L(\mathbf{u})).\end{aligned}$$

□

Remark 2.5.12

*For the curious student, Proposition 2.5.11 states that the collection of all possible $\mathbb{R}$-vector spaces and linear functions between them is an example of an algebraic structure called a **category**. Category theory is typically introduced in more advanced abstract algebra and topology courses.*

2.5.2 Linear extension

In general, to define a function, one needs to state its domain, its codomain, and a “rule” assigning to each element in the domain an element in the codomain. But what if we only know the rule for a proper subset of the domain: can we figure out what the function does to the rest of its domain?

Example 2.5.13

Suppose that $f : \mathbb{R} \to \mathbb{R}$ *is a function for which we know that* $f(x) = 0$ *for any* $x \in \mathbb{Q}$. *Can we determine the output value* $f\left(\sqrt{2}\right)$*?*

Solution.
No! There are infinitely many possibilities for what $f\left(\sqrt{2}\right)$ could be, and we lack the information to decide. For instance, it could be the case that $f = 0$ (the zero function), in which case $f(\sqrt{2}) = 0$. Alternatively, it could be the case that f is actually the **characteristic function** (also known as the **indicator function**) of the irrational numbers, which is given by the rule:

$$\chi_{\mathbb{R}\setminus\mathbb{Q}} := \begin{cases} 1 & \text{if } x \in \mathbb{R} \setminus \mathbb{Q} \\ 0 & \text{if } x \in \mathbb{Q}. \end{cases}$$

Thus, we see that for a general function, knowing its rule only for a proper subset of the domain does not allow us to recover its rule for the entire domain. In the special case of *linear* functions, we can do much better!

Example 2.5.14

Consider the subset

$$B := \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\} \subset \mathbb{R}^2.$$

Suppose that $L : \mathbb{R}^2 \to \mathbb{R}^3$ *is a linear function which satisfies*

$$L\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 2 \\ 0 \\ -2 \end{bmatrix}, \quad L\left(\begin{bmatrix} 1 \\ 2 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix}.$$

Given an arbitrary vector $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$*, can we find the output vector* $L\left(\begin{bmatrix} x \\ y \end{bmatrix}\right)$*?*

Solution.
Let's try to express $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$ as a linear combination of the vectors in the subset B. To do this, we need to solve the linear system

$$c_1 \begin{bmatrix} 1 \\ 1 \end{bmatrix} + c_2 \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$$

for the scalars c_1 and c_2. We row-reduce the corresponding augmented matrix:

$$\left[\begin{array}{cc|c} 1 & 1 & x \\ 1 & 2 & y \end{array}\right] \sim \left[\begin{array}{cc|c} 1 & 0 & 2x-y \\ 0 & 1 & -x+y \end{array}\right].$$

Thus, we find that the vector $\begin{bmatrix} x \\ y \end{bmatrix}$ can be expressed *uniquely* as a linear combinator of the vectors in B, namely

$$\begin{bmatrix} x \\ y \end{bmatrix} = (2x-y)\begin{bmatrix} 1 \\ 1 \end{bmatrix} + (-x+y)\begin{bmatrix} 1 \\ 2 \end{bmatrix},$$

Note that Corollary 2.3.17 tells us that B is a basis. Because we know that L is linear, we must have

$$\begin{aligned} L\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) &= L\left((2x-y)\begin{bmatrix} 1 \\ 1 \end{bmatrix} + (-x+y)\begin{bmatrix} 1 \\ 2 \end{bmatrix}\right) \\ &= (2x-y)L\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) + (-x+y)L\left(\begin{bmatrix} 1 \\ 2 \end{bmatrix}\right) \\ &= (2x-y)\begin{bmatrix} 2 \\ 0 \\ -2 \end{bmatrix} + (-x+y)\begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 4x-2y \\ -2x+2y \\ -4x+2y \end{bmatrix}. \end{aligned}$$

From the above example, you might (correctly) guess that the rule for a linear function is completely determined by what the function does to a basis for its domain. Indeed, we will show this in the proof of Theorem 2.5.17. First, we need to prove the following Lemma:

Lemma 2.5.15

Let $L, T : U \to V$ be linear functions, and let $X \subseteq U$ be a subset such that $\operatorname{Span} X = U$. Then

$$L(\mathbf{x}) = T(\mathbf{x}) \text{ for all } \mathbf{x} \in X \implies L = T.$$

Proof. Suppose that $L(\mathbf{x}) = T(\mathbf{x})$ for all $\mathbf{x} \in X$. Let $\mathbf{u} \in U$ be arbitrary. Since $U = \operatorname{Span} X$ then we can write

$$\mathbf{u} = \sum_{i=1}^{k} c_i \mathbf{x}_i$$

for some scalars c_i and some vectors $\mathbf{x}_i \in X$. Using the fact the L and T are linear and agree on X, we see that

$$L(\mathbf{u}) = L\left(\sum_{i=1}^{k} c_i \mathbf{x}_i\right)$$

$$
\begin{aligned}
&= \left(\sum_{i=1}^{k} c_i L(\mathbf{x}_i)\right) \\
&= \left(\sum_{i=1}^{k} c_i T(\mathbf{x}_i)\right) \\
&= T\left(\sum_{i=1}^{k} c_i \mathbf{x}_i\right) \\
&= T(\mathbf{u}).
\end{aligned}
$$

□

In other words, Lemma 2.5.15 states that for any two linear functions with the same domain and codomain, if they agree on a spanning set for their domain, then in fact the two linear functions must be the equal!

Definition 2.5.16

Let U and V be $\mathbb{R}$-vector spaces, and let $X \subseteq U$ be a subset. Given a function $f : X \to V$, a ***linear extension*** *of f is a linear function $F : U \to V$ which satisfies*

$$F(\mathbf{x}) = f(\mathbf{x})$$

for all $\mathbf{x} \in X$.

If X is an arbitrary subset of the domain, a linear extension of $f : X \to V$ may not exist, or may not be unique. However, in the special case where X is a basis for the domain, then we can always construct a linear extension $F : U \to V$ and there is only one way to do so!

Theorem 2.5.17

Let U and V be $\mathbb{R}$-vector spaces, and $B \subseteq U$ be a basis. Given a function $f : B \to V$, there exists a unique linear extension $F : U \to V$.

Proof. Since B is a basis, then by Corollary 2.3.17, each $\mathbf{u} \in U$ can be written *uniquely* as a linear combination of the basis vectors

$$\mathbf{u} = \sum_{i=1}^{n} c_i \mathbf{b}_i,$$

where the $c_i \in \mathbb{R}$ are scalars uniquely determined by $\mathbf{u}$. Since we want $F : U \to V$ to be linear and for it to agree with f on the basis B, it must satisfy the following equalities:

$$F(\mathbf{u}) = F\left(\sum_{i=1}^{n} c_i \mathbf{b}_i\right) = \sum_{i=1}^{n} c_i F(\mathbf{b}_i) = \sum_{i=1}^{n} c_i f(\mathbf{b}_i).$$

This tells us that we should define our linear extension $F : U \to V$ by the rule

$$F(\mathbf{u}) := \sum_{i=1}^{n} c_i f(\mathbf{b}_i).$$

Now that we have a candidate F for the linear extension of f, we should check that it is indeed linear. Given another vector $\mathbf{u}' \in U$, we can express it *uniquely* as a linear combination of the basis B by Corollary 2.3.17:

$$\mathbf{u}' = \sum_{i=1}^{n} c_i' \mathbf{b}_i.$$

We can see that F is additive:

$$\begin{aligned} F(\mathbf{u} + \mathbf{u}') &= F\left(\sum_{i=1}^{n} c_i \mathbf{b}_i + \sum_{i=1}^{n} c_i' \mathbf{b}_i\right) \\ &= F\left(\sum_{i=1}^{n} (c_i + c_i')\mathbf{b}_i\right) \\ &= \sum_{i=1}^{n} (c_i + c_i') f(\mathbf{b}_i) \\ &= \sum_{i=1}^{n} c_i f(\mathbf{b}_i) + \sum_{i=1}^{n} c_i' f(\mathbf{b}_i) \\ &= F(\mathbf{u}) + F(\mathbf{u}'). \end{aligned}$$

We leave it as an exercise to check that F is homogeneous.

To finish the proof, we apply Lemma 2.5.15 to conclude that the function $F : U \to V$ we have constructed is indeed the unique linear extension of the given function $f : B \to V$. □

Theorem 2.5.17 is one of the most useful results in MATHS 120. Let's demonstrate this by finding a formula for any rotation (about the origin) in the plane $\mathbb{R}^2$. To help us with this, we need the Mazur-Ulam Theorem. You do *not* need to memorize this Theorem for the exam—it is only stated here to help us with the subsequent example.

Theorem 2.5.18: Mazur-Ulam

Let $f : \mathbb{R}^n \to \mathbb{R}^n$ be a function such that

$$\operatorname{dist}(f(\mathbf{x}), f(\mathbf{y})) = \operatorname{dist}(\mathbf{x}, \mathbf{y}) \qquad \text{for all } \mathbf{x}, \mathbf{y} \in \mathbb{R}^n.$$

Then there exists a linear function $L : \mathbb{R}^n \to \mathbb{R}^n$ such that

$$f(\mathbf{x}) = L(\mathbf{x}) + f(\mathbf{0}) \qquad \text{for all } \mathbf{x} \in \mathbb{R}^n.$$

Moreover, L has the property

$$\langle L\mathbf{x}, L\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle \qquad \text{for all } \mathbf{x}, \mathbf{y} \in \mathbb{R}^n,$$

Proof. Given such a distance-preserving function f, just define

$$L(\mathbf{x}) := f(\mathbf{x}) - f(\mathbf{0}).$$

We still need to verify that L is linear and that L preserves the Euclidean scalar product—you'll see the rest of the proof in MATHS 254. □

Example 2.5.19

Let $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ be the function which rotates the plane counterclockwise about the origin through an angle θ. Find an explicit formula for $R_\theta\left(\begin{bmatrix} x \\ y \end{bmatrix}\right)$, where $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$ is arbitrary.

Solution.

The origin is fixed by this rotation, and rotating a vector does not change its length. In other words,

$$\begin{aligned} R_\theta(\mathbf{0}) &= \mathbf{0}, \\ \operatorname{dist}(R_\theta\mathbf{u}, R_\theta\mathbf{v}) &= \operatorname{dist}(\mathbf{u}, \mathbf{v}). \end{aligned}$$

Thus, the Mazur-Ulam Theorem 2.5.18 tells us that R_θ must be a linear function! In order to apply Theorem 2.5.17, we first need to describe how the standard ordered basis $(\mathbf{e}_1, \mathbf{e}_2)$ of $\mathbb{R}^2$ is transformed by R_θ. With some straightforward secondary school trigonometry, we see that

$$R_\theta(\mathbf{e}_1) = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}.$$

Similarly,

$$R_\theta(\mathbf{e}_2) = \begin{bmatrix} \cos(\theta + \frac{\pi}{2}) \\ \sin(\theta + \frac{\pi}{2}) \end{bmatrix} = \begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix}.$$

Thus, we get the desired formula:

$$\begin{aligned} R_\theta\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) &= R_\theta\left(x\mathbf{e}_1 + y\mathbf{e}_2\right) \\ &= xR_\theta(\mathbf{e}_1) + yR_\theta(\mathbf{e}_2) \\ &= x\begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix} + y\begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix} \\ &= \begin{bmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{bmatrix}. \end{aligned}$$

2.6 Matrices

2.6.1 Basic definitions

Definition 2.6.1

Let $m, n \in \mathbb{N}$. A ***matrix*** *of* ***shape*** *$m \times n$ is an array with m rows and n columns*

$$A := \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

where the $a_{ij} \in \mathbb{R}$ are the entries of the matrix.

- *The ith row of A is*

$$\operatorname{row}_i(A) := \begin{bmatrix} a_{i1} & \cdots & a_{in} \end{bmatrix}$$

- *The jth column of A is*

$$\operatorname{col}_j(A) := \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix}$$

- *We sometimes write $\mathrm{Mat}_{m\times n}(\mathbb{R})$ for the set of all $m \times n$ matrices with entries from $\mathbb{R}$.*

More generally, the entries of a matrix can be integers, complex numbers, or more exotic numbers. In MATHS 120, the entries are real, unless otherwise specified. We will occasionally also use complex matrices in examples.

Definition 2.6.2

- *We call a matrix* $\mathbf{v} \in \operatorname{Mat}_{m\times 1}(\mathbb{R}) = \mathbb{R}^m$ *a* ***column vector****, and we write*
$$\mathbf{v} = \begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix}$$
- *We call a matrix* $\varphi \in \operatorname{Mat}_{1\times n}(\mathbb{R})$ *a* ***row vector****, and we write*
$$\varphi = \begin{bmatrix} \varphi_1 & \cdots & \varphi_n \end{bmatrix}.$$

Example 2.6.3

- $\begin{bmatrix} 1 & 0 & 4 \\ 1 & 2 & 0 \\ 3 & 4 & -1 \end{bmatrix}$ *is a* 3×3 *matrix.*
- $\begin{bmatrix} 3 & 1 & -2 \end{bmatrix}$ *is a* 1×3 *matrix—a row vector.*
- $\begin{bmatrix} 2 \\ 1 \\ 0 \\ 3 \end{bmatrix}$ *is a* 4×1 *matrix—a column vector.*

Definition 2.6.4

Two matrices A *and* B *are* ***equal*** *if they have the same shape, say,* $m \times n$ *and each of their corresponding entries are equal, i.e.,* $a_{ij} = b_{ij}$ *for all* $1 \leq i \leq m$ *and all* $1 \leq j \leq n$*.*

2.6.2 The standard matrix of a linear function

By Theorem 2.5.17, we know that a linear function is uniquely determined by what it does to a basis. Thus, given a choice of ordered basis for the domain and codomain we can neatly encode any linear function between finite-dimensional vector spaces by a matrix.

In this course, we will only do this for linear functions $L : \mathbb{R}^n \to \mathbb{R}^m$, and we will only find the corresponding matrix with respect to the standard ordered bases on the domain and codomain. See MATHS 250 and MATHS 253 for the general case.

Definition 2.6.5

*The **standard matrix** of a linear function $L : \mathbb{R}^n \to \mathbb{R}^m$ is defined to be the $m \times n$ matrix*

$$[L] := \big[L(\mathbf{e}_1) \mid L(\mathbf{e}_2) \mid \cdots \mid L(\mathbf{e}_n) \big]$$

where $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ is the standard ordered basis of $\mathbb{R}^n$.

In other words, the jth column of the standard matrix $[L]$ tells us what the linear function $L : \mathbb{R}^n \to \mathbb{R}^m$ does to the jth standard basis vector, i.e.,

$$\mathrm{col}_j[L] = L(\mathbf{e}_j).$$

As we have seen, this data completely determines the linear function L.

Remark 2.6.6

We can think of the standard matrix construction as function

$$\begin{aligned} [\_] : \quad \mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m) &\longrightarrow \mathrm{Mat}_{m\times n}(\mathbb{R}) \\ L &\longmapsto [L] \end{aligned}$$

which accepts a linear function $L : \mathbb{R}^n \to \mathbb{R}^m$ and returns an $m \times n$ matrix $[L]$.

Remark 2.6.7

We can be more general and construct the matrix associated to $L : \mathbb{R}^n \to \mathbb{R}^m$ with respect to an ordered basis B of $\mathbb{R}^n$ and another ordered basis B' of $\mathbb{R}^m$. The entries for the jth column are then coefficients that uniquely determine $F(\mathbf{b}_j)$ with respect to the ordered basis vectors in B'. We will not consider such matrices in MATHS *120.*

Example 2.6.8

Let $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear function which rotates the plane counterclockwise about the origin through an angle θ. Find its standard matrix.

Solution.
From Example 2.5.19, we immediately get the standard rotation matrix

$$[R_\theta] = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

The set of all such rotation matrices

$$\mathrm{SO}(2) := \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \;\middle|\; \theta \in \mathbb{R} \right\}$$

is called the **rotation group** or the **special orthogonal group** in dimension 2. You will encounter this group again in MATHS 254 and in more advanced physics courses.

Example 2.6.9

Find the standard matrix of the linear function

$$\begin{aligned} L : \quad \mathbb{R}^3 &\longrightarrow \mathbb{R}^2 \\ \begin{bmatrix} x \\ y \\ z \end{bmatrix} &\longmapsto \begin{bmatrix} x - 2y + z \\ 2x - 3z \end{bmatrix} \end{aligned}$$

Solution.
Method 1: We just apply Definition 2.6.5 directly:

$$[L] = \begin{bmatrix} L\mathbf{e}_1 & L\mathbf{e}_2 & L\mathbf{e}_3 \end{bmatrix} = \begin{bmatrix} 1 & -2 & 1 \\ 2 & 0 & -3 \end{bmatrix}.$$

Method 2: We can break up the output vector:

$$L\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x - 2y + z \\ 2x - 3z \end{bmatrix} = x\begin{bmatrix} 1 \\ 2 \end{bmatrix} + y\begin{bmatrix} -2 \\ 0 \end{bmatrix} + z\begin{bmatrix} 1 \\ -3 \end{bmatrix}.$$

On the other hand, by linearity we must have

$$L\begin{bmatrix} x \\ y \\ z \end{bmatrix} = L\left(x\mathbf{e}_1 + y\mathbf{e}_2 + z\mathbf{e}_3\right) = xL\mathbf{e}_1 + yL\mathbf{e}_2 + zL\mathbf{e}_3.$$

Comparing these two expressions tells us that the standard matrix must be

$$[L] = \begin{bmatrix} L\mathbf{e}_1 & L\mathbf{e}_2 & L\mathbf{e}_3 \end{bmatrix} = \begin{bmatrix} 1 & -2 & 1 \\ 2 & 0 & -3 \end{bmatrix}.$$

Exercise 2.6.10

In each case, decide whether the function is uniquely defined as a linear transformation on its domain; if so, find the standard matrix of the function.

1. $f : \mathbb{R}^3 \to \mathbb{R}$ *with*
$$f\left(\begin{bmatrix}1\\0\\1\end{bmatrix}\right) = 1,\ f\left(\begin{bmatrix}1\\2\\3\end{bmatrix}\right) = 3, \text{ and } f\left(\begin{bmatrix}2\\2\\4\end{bmatrix}\right) = 4$$
2. $g : \mathbb{R}^3 \to \mathbb{R}$ *with*
$$g\left(\begin{bmatrix}1\\0\\1\end{bmatrix}\right) = 1,\ g\left(\begin{bmatrix}1\\2\\3\end{bmatrix}\right) = 3, \text{ and } g\left(\begin{bmatrix}2\\2\\4\end{bmatrix}\right) = -4$$
3. $h : \mathbb{R}^2 \to \mathbb{R}^2$ *with* $h(\mathbf{e}_1 + \boldsymbol{e_2}) = \mathbf{e}_1$ *and* $h(\mathbf{e}_1 - \boldsymbol{e_2}) = -\mathbf{e}_1$
4. $k : \mathbb{R}^2 \to \mathbb{R}$ *with* $k\left(\begin{bmatrix}17\\1\end{bmatrix}\right) = 17$ *and* $k\left(\begin{bmatrix}16\\2\end{bmatrix}\right) = 16$

Exercise 2.6.11

Let $F : \mathbb{R}^2 \to \mathbb{R}^3$ *be a linear function which has the following standard matrix*
$$\begin{bmatrix}1 & 2\\3 & 4\\5 & 6\end{bmatrix},$$
what is the output vector $F(\mathbf{e}_1 + \mathbf{e}_2)$*?*

2.6.3 The linear function determined by a matrix

We have just seen that we can encode a linear function $L : \mathbb{R}^n \to \mathbb{R}^m$ by its standard $m \times n$ matrix $[F]$. But what if we want to reverse this process? In other words, given a matrix $A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$, we would like to think of it as being the standard matrix of some linear function $T_A : \mathbb{R}^n \to \mathbb{R}^m$. In other words, we want to have the equality

$$\big[T_A(\mathbf{e}_1) \mid T_A(\mathbf{e}_2) \mid \cdots \mid T_A(\mathbf{e}_n)\big] = A.$$

In order to try to find the rule $T_A(\mathbf{x})$ for this desired linear function, we just follow the same reasoning that we previously used to invent the standard matrix. Indeed, since we want T_A to be linear, then for any $\mathbf{x} \in \mathbb{R}^n$ we must have

$$\begin{aligned}T_A(\mathbf{x}) &= T_A(x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n)\\ &= x_1 T_A(\mathbf{e}_1) + \cdots + x_n T_A(\mathbf{e}_n)\\ &= x_1 \operatorname{col}_1(A) + \cdots + x_n \operatorname{col}_n(A).\end{aligned}$$

Thus, we arrive at the following method to obtain a linear function from a matrix:

Definition 2.6.12

Given a matrix $A \in \operatorname{Mat}_{m\times n}(\mathbb{R})$, we define its corresponding linear function by the rule

$$\begin{aligned} T_A : \quad \mathbb{R}^n &\longrightarrow \mathbb{R}^m \\ \mathbf{x} &\longmapsto x_1 \operatorname{col}_1(A) + \cdots + x_n \operatorname{col}_n(A). \end{aligned}$$

See Remark 2.6.26 for a more concise way to write the rule for T_A.

Exercise 2.6.13

Given a matrix $A \in \operatorname{Mat}_{m\times n}(\mathbb{R})$, prove that the corresponding function $T_A : \mathbb{R}^n \to \mathbb{R}^m$ is indeed linear.

Remark 2.6.14

We have described a process for turning a matrix $A \in \operatorname{Mat}_{m\times n}(\mathbb{R})$ into a linear transformation $T_A : \mathbb{R}^n \to \mathbb{R}^m$. We can think of this process as a function:

$$\begin{aligned} T_{(\_)} : \quad \operatorname{Mat}_{m\times n}(\mathbb{R}) &\longrightarrow \operatorname{Lin}(\mathbb{R}^n, \mathbb{R}^m) \\ A &\longmapsto T_A. \end{aligned}$$

Example 2.6.15

Suppose that $A := \begin{bmatrix} 0 & 1 & 3 \\ 2 & 4 & 4 \end{bmatrix}$ is the standard matrix of a (real) linear transformation T_A.

1. *What are the domain and codomain of T_A?*
2. *Give a formula for $T_A(\mathbf{x})$, where $\mathbf{x}$ is an arbitary vector in the domain.*

Solution. 1. Because A is a 2×3 matrix then we have $T_A : \mathbb{R}^3 \to \mathbb{R}^2$.

2. For any $\mathbf{x} \in \mathbb{R}^n$ we have

$$\begin{aligned} T_A(\mathbf{x}) &= x_1 \operatorname{col}_1(A) + x_2 \operatorname{col}_2(A) + x_3 \operatorname{col}_3(A) \\ &= x_1 \begin{bmatrix} 0 \\ 2 \end{bmatrix} + x_2 \begin{bmatrix} 1 \\ 4 \end{bmatrix} + x_3 \begin{bmatrix} 3 \\ 4 \end{bmatrix} \\ &= \begin{bmatrix} x_2 + 3x_3 \\ 2x_1 + 4x_2 + 4x_3 \end{bmatrix}. \end{aligned}$$

For convenience, we state the following obvious proposition. This makes clear that that the standard matrix construction and the construction of a linear function from a matrix are inverse to one another—we chose our constructions precisely so that this would be the case.

Proposition 2.6.16

Let $L : \mathbb{R}^n \to \mathbb{R}^m$ be a linear function and let $A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$. Then we have

$$[T_A] = A \qquad \textit{and} \qquad T_{[L]} = L.$$

2.6.4 Addition and scaling of matrices

As we have seen in Section 2.6.2, a linear function $F : \mathbb{R}^n \to \mathbb{R}^m$ can be neatly encoded by its $m \times n$ standard matrix $[F]$. Using operations such as addition, scaling, and composition that we already know how to perform on linear functions, we would like to define corresponding operations on matrices.

Let's start by thinking about addition. Given linear functions F, G : $\mathbb{R}^n \to \mathbb{R}^m$, let's apply the standard matrix construction given in Definition 2.6.5 to their sum $F + G : \mathbb{R}^n \to \mathbb{R}^m$.

$$\begin{aligned} \big[F+G\big] &= \big[(F+G)(\mathbf{e}_1) \mid \cdots \mid (F+G)(\mathbf{e}_n)\big] \\ &= \big[F(\mathbf{e}_1) + G(\mathbf{e}_1) \mid \cdots \mid F(\mathbf{e}_n) + G(\mathbf{e}_n)\big] \,. \end{aligned}$$

We want to be able to write

$$[F + G] = [F] + [G]$$

and so our calculation above tells us that we need to make the following definition:

Definition 2.6.17

Given matrices $A, B \in \mathrm{Mat}_{m\times n}(\mathbb{R})$, then their **sum** *$A + B$ is the $m \times n$ matrix defined entrywise by*

$$(A + B)_{ij} := a_{ij} + b_{ij}.$$

In other words, to get the entry in the ith row and jth column of $A + B$, we simply add the corresponding entries from A and B. Warning: as expected from our discussion above, if A and B have different shapes then it is *not possible* to add them!

Example 2.6.18

If possible, calculate the sums of the following matrices.

(i) $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 \\ -3 & 1 & 0 \end{bmatrix}$;

(ii) $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 2 & 1 \\ 4 & 6 \end{bmatrix}$.

Solution. (i) $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 \\ -3 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 2 & 4 \\ 1 & 6 & 6 \end{bmatrix}$.

(ii) These matrices cannot be added as they have different shapes.

Definition 2.6.19

For $m, n \in \mathbb{N}$, the ***zero matrix*** *$O_{m\times n}$ is the $m \times n$ matrix with every entry equal to 0.*

If the dimension is clear from the context, we often simply write O, instead of $O_{m\times n}$.

Let's now turn our attention to defining a scaling operation on matrices. Given a linear function $L : \mathbb{R}^n \to \mathbb{R}^m$ and a scalar $c \in \mathbb{R}$, let's apply the standard matrix construction given in Definition 2.6.5 to the scaled linear function $cL : \mathbb{R}^n \to \mathbb{R}^m$.

$$\begin{aligned} [cL] &= \big[(cL)(\mathbf{e}_1) \bigm| \cdots \bigm| (cL)(\mathbf{e}_n)\big] \\ &= \big[c(L(\mathbf{e}_1)) \bigm| \cdots \bigm| c(L(\mathbf{e}_n))\big] \end{aligned}$$

We want to be able to write

$$[cL] = c[L],$$

and so our calculation above tells us that we need to make the following definition:

Definition 2.6.20

Given an $m \times n$ matrix A and a scalar c, then the scaled matrix $c\,A$ is the $m \times n$ matrix defined entrywise by

$$(c\,A)_{ij} := ca_{ij}.$$

In other words, we simply multiply each entry by c.

Example 2.6.21

Calculate the following.

(i) $5\begin{bmatrix}3 & 2\\ 1 & 0\end{bmatrix}$;

(ii) $-1\begin{bmatrix}3 & 1 & 0\\ 2 & -1 & -2\end{bmatrix}$.

Solution.

(i) $5\begin{bmatrix}3 & 2\\ 1 & 0\end{bmatrix}=\begin{bmatrix}15 & 10\\ 5 & 0\end{bmatrix}$.

(ii) $-1\begin{bmatrix}3 & 1 & 0\\ 2 & -1 & -2\end{bmatrix}=\begin{bmatrix}-3 & -1 & 0\\ -2 & 1 & 2\end{bmatrix}$.

By Proposition 2.5.10, we know that the set $\mathrm{Lin}(\mathbb{R}^n,\mathbb{R}^m)$ of linear functions from $\mathbb{R}^n$ to $\mathbb{R}^m$ is a vector space. Since we have defined addition and scaling of matrices precisely so that these operations would agree with the corresponding operations on linear functions, it should be no surprise that the set $\mathrm{Mat}_{m\times n}(\mathbb{R})$ of all $m\times n$ matrices also satisfies the axioms of a vector space!

Theorem 2.6.22

With addition and scalar multiplication defined as above, and the zero matrix playing the role of the zero vector, the set of all $m\times n$ matrices $\mathrm{Mat}_{m\times n}(\mathbb{R})$ is an $\mathbb{R}$-vector space.

Proof. We need to verify the axioms in Definition 2.2.7. This is easy but repetitive, so we leave most of this to the reader. But for demonstration, let's just check that the zero matrix behaves as required.

Given any $m\times n$ matrix A, then

$$(A+O_{m\times n})_{ij}=a_{ij}+(O_{m\times n})_{ij}=a_{ij}+0=a_{ij},$$

so indeed $A+O_{m\times n}=A=O_{m\times n}+A$. □

The result below immediately follows:

Corollary 2.6.23

For all $m, n \in \mathbb{N}$, the standard matrix construction

$$\begin{aligned} [\_] : \quad \mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m) &\longrightarrow \mathrm{Mat}_{m\times n}(\mathbb{R}) \\ F &\longmapsto [F] \end{aligned} \tag{2.1}$$

is linear. In other words, for all linear functions $F, G : \mathbb{R}^n \to \mathbb{R}^m$ and all scalars $c \in \mathbb{R}$, we have the following equalities:

1. $[F+G] = [F] + [G]$
2. $[cF] = c\,[F]$.

Proof. This follows immediately from Theorem 2.6.22 and the definitions we chose for matrix addition and scalar multiplication. □

Corollary 2.6.24

For any $m, n \in \mathbb{N}$, the construction

$$\begin{aligned} T_{(\_)} : \quad \mathrm{Mat}_{m\times n}(\mathbb{R}) &\longrightarrow \mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m) \\ A &\longmapsto T_A. \end{aligned}$$

is linear. In other words, for all matrices $A, B \in \mathrm{Mat}_{m\times n}(\mathbb{R})$ and all scalars $c \in \mathbb{R}$, we have the following equalities:

1. $T_{A+B} = T_A + T_B$
2. $T_{cA} = cT_A$

Proof. We could check this directly using Definition 2.6.12. Alternatively, we can come back to this once we have proven Theorem 2.7.14. In this case, we apply it together with Proposition 2.6.16 and Corollary 2.6.23. □

2.6.5 Matrix multiplication

It would be nice if we have a rule for multiplying an $m \times n$ matrix A and a column vector $\mathbf{x} \in \mathbb{R}^n$ so that

$$A\mathbf{x} = T_A(\mathbf{x}).$$

Looking at Definition 2.6.12, we see exactly what we need to do:

Definition 2.6.25

let A be an $m \times n$ matrix, and $\mathbf{x} \in \mathbb{R}^n$. We define the product $A\mathbf{x} \in \mathbb{R}^m$ by the rule

$$A\mathbf{x} := \sum_{j=1}^{n} x_j \operatorname{col}_j(A) = x_1 \operatorname{col}_1(A) + \cdots + x_n \operatorname{col}_n(A).$$

Remark 2.6.26

Thanks to this matrix multiplication rule, we can now express the formula appearing in Definition 2.6.12 in a more concise way. Namely, for any $A \in \operatorname{Mat}_{m\times n}(\mathbb{R})$ and $x \in \mathbb{R}^n$ we have

$$T_A(\mathbf{x}) = A\mathbf{x}.$$

Given a pair of matrices $A \in \operatorname{Mat}_{m\times n}(\mathbb{R})$ and $B \in \operatorname{Mat}_{r\times s}(\mathbb{R})$, Definition 2.6.12 allows us to construct the corresponding linear functions $T_A : \mathbb{R}^n \to \mathbb{R}^m$ and $T_B : \mathbb{R}^s \to \mathbb{R}^r$. If $s = m$ then we can construct the composite function

$$\begin{tikzcd}
\mathbb{R}^n \arrow[r, "T_A"'] \arrow[rr, bend left, "T_B \circ T_A"] & \mathbb{R}^m \arrow[r, "T_B"'] & \mathbb{R}^r \\
\mathbf{x} \arrow[r, mapsto] & T_A(\mathbf{x}) \arrow[r, mapsto] \arrow[d, equal] & T_B(T_A(\mathbf{x})) \arrow[d, equal] \\
& A\mathbf{x} & T_B(A\mathbf{x}) \arrow[d, equal] \\
& & B(A\mathbf{x})
\end{tikzcd}$$

The equalities in this diagram just follow from Definition 2.6.25. Since the composite function $T_B \circ T_A : \mathbb{R}^n \to \mathbb{R}^r$ is linear by Proposition 2.5.11, then we can construct its standard $m \times r$ matrix $\left[T_B \circ T_A\right]$. From the diagram above, we see that this standard matrix can be expressed as follows:

$$\begin{aligned}
\left[T_B \circ T_A\right] &= \left[T_B(T_A(\mathbf{e}_1)) \mid T_B(T_A(\mathbf{e}_2)) \mid \cdots \mid T_B(T_A(\mathbf{e}_n))\right] \\
&= \left[B(A(\mathbf{e}_1)) \mid B(A(\mathbf{e}_2)) \mid \cdots \mid B(A(\mathbf{e}_n))\right] \\
&= \left[B \operatorname{col}_1(A) \mid B \operatorname{col}_2(A) \mid \cdots \mid B \operatorname{col}_n(A)\right].
\end{aligned}$$

From this, we can now see how we should define the rule for multiplying matrices so that

$$BA = \left[T_B \circ T_A\right].$$

In other words, we want our to write our rule for matrix multiplication so that the matrix product corresponds to function composition.

Definition 2.6.27

Given matrices $A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$ *and* $B \in \mathrm{Mat}_{r\times m}(\mathbb{R})$, *we define the product*

$$BA := \left[B\,\mathrm{col}_1(A) \;\middle|\; B\,\mathrm{col}_2(A) \;\middle|\; \cdots \;\middle|\; B\,\mathrm{col}_n(A)\right],$$

where $\mathrm{col}_j(A)$ *is the* j*th column of* A. *This matrix multiplication operation can be viewed as a function:*

$$\begin{aligned} \mathrm{Mat}_{r\times m}(\mathbb{R}) \times \mathrm{Mat}_{m\times n}(\mathbb{R}) &\longrightarrow \mathrm{Mat}_{r\times n}(\mathbb{R}) \\ (B, A) &\longmapsto BA \end{aligned}$$

Note that the rule given in the definition above generalizes—and relies upon—the matrix multiplication rule previously given in Definition 2.6.25, since it involves multiplying each of the columns of A on the left by B.

We also emphasize that this matrix multiplication operation is only defined if the matrices involved have the correct shapes. The following memory aid should you remember the correct shape of the product:

$$(m \times \underbrace{n) \cdot (n}_{\text{cancel}} \times r) = (m \times r).$$

Example 2.6.28

(i) $\begin{bmatrix} 1 & -1 & 2 \\ 4 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} = \begin{bmatrix} -1 \\ 5 \end{bmatrix}.$

(ii) $\begin{bmatrix} 1 & -2 & 5 \\ -3 & 6 & -15 \end{bmatrix} \begin{bmatrix} -3 & -1 \\ 1 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$

(iii) $\begin{bmatrix} 1 & 2 & 3 & 4 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 8 \end{bmatrix}.$

(iv) $\begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 2 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix}$ *is* not *defined, because the first matrix is* 2×2 *while the second is* 3×3.

In practice one often uses the following formulas to perform matrix multiplication. These are easier to compute with, but don't provide quite the same insight as our definition.

Proposition 2.6.29

Let $B \in \mathrm{Mat}_{r\times m}(\mathbb{R})$, $A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$, $\varphi \in \mathrm{Mat}_{1\times n}(\mathbb{R})$, $\mathbf{x} \in \mathbb{R}^n$. *Then*

1. $\varphi\mathbf{x} = \sum_{k=1}^n \varphi_k x_k = \varphi_1 x_1 + \cdots + \varphi_n x_n$
2. $A\mathbf{x} = \begin{bmatrix} \mathrm{row}_1(A)\mathbf{x} \\ \vdots \\ \mathrm{row}_m(A)\mathbf{x} \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{bmatrix}$
3. $BA = \begin{bmatrix} \mathrm{row}_1(B)\,\mathrm{col}_1(A) & \cdots & \mathrm{row}_1(B)\,\mathrm{col}_n(A) \\ \vdots & \ddots & \vdots \\ \mathrm{row}_r(B)\,\mathrm{col}_1(A) & \cdots & \mathrm{row}_r(B)\,\mathrm{col}_n(A) \end{bmatrix}$

Proof. Exercise. □

Remark 2.6.30

Part 3 of Proposition 2.6.29 gives us a formula for the entries of the product BA*. In particular, for each* $1 \leq i \leq r$, $1 \leq j \leq n$, *we have*

$$(BA)_{ij} = \mathrm{row}_i(B)\,\mathrm{col}_j(A) = \sum_{k=1}^{m} b_{ik}a_{kj}.$$

Another way to look at this formula is that the entry $(BA)_{ij}$ *of the product matrix is just the scalar product of the* i*th row of* B *with the* j*th column of* A.

If you are familiar with MATLAB, we encourage you to try to write your own matrix multiplication function using this formula!

For your convenience, we now summarize the desired relationship between matrix multiplication and composition of linear functions:

Theorem 2.6.31

Let $F : \mathbb{R}^n \to \mathbb{R}^m$ and $G : \mathbb{R}^m \to \mathbb{R}^r$ be linear functions, let $A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$, $B \in \mathrm{Mat}_{r\times m}(\mathbb{R})$, and let $\mathbf{x} \in \mathbb{R}^n$. The following hold:

1. $[F]\mathbf{x} = F(\mathbf{x})$
2. $T_A(\mathbf{x}) = A\mathbf{x}$
3. $\big[G \circ F\big] = \big[G\big]\,\big[F\big]$
4. $T_B \circ T_A = T_{BA}$

Proof. These equalities all hold because we chose the definition of matrix multiplication precisely so that they would! □

Recall that the identity function $\mathrm{id}_{\mathbb{R}^n} : \mathbb{R}^n \to \mathbb{R}^n$ is linear by Proposition 2.5.11, and therefore we can construct its standard matrix as follows:

$$\big[\mathrm{id}_{\mathbb{R}^n}\big] = \big[\mathrm{id}_{\mathbb{R}^n}(\mathbf{e}_1) \mid \cdots \mid \mathrm{id}_{\mathbb{R}^n}(\mathbf{e}_n)\big] = \big[\mathbf{e}_1 \mid \cdots \mid \mathbf{e}_n\big]\,.$$

This matrix has 1's on the diagonal, and 0's everywhere else, and we give it the following special name:

Definition 2.6.32

*For each $n \in \mathbb{N}$, the $n \times n$ **identity matrix** I_n is the $n \times n$ matrix defined by*

$$(I_n)_{ij} := \begin{cases} 1 & \text{if} \quad i = j; \\ 0 & \text{if} \quad i \neq j. \end{cases}$$

For example,

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

If the dimension n is clear from the context, we sometimes simply write I, instead of I_n.

Just as the zero matrix $O_{n,m}$ is called an additive identity, the identity matrix I_n is called a **multiplicative identity**.

Taking advantage of the correspondence we have established between linear functions and matrices, we immediately get the following properties of matrix multiplication:

Corollary 2.6.33

Let $E \in \mathrm{Mat}_{s\times r}(\mathbb{R})$, $C, D \in \mathrm{Mat}_{r\times m}(\mathbb{R})$, $A, B \in \mathrm{Mat}_{m\times n}(\mathbb{R})$, $c \in \mathbb{R}$. *The following hold:*

1. *Distributive law:*
   - $C(A+B) = CA + CB$
   - $(C+D)A = CA + DA$
2. *Homogeneous:* $C(cA) = c(CA) = (cC)A$
3. *Associative law:* $(EC)A = E(CA)$
4. *Existence of multiplicative identities:*
   - $I_m A = A$
   - $A I_n = A$
5. *Products with zero matrices:*
   - $0_{r\times m} A = 0_{r\times n}$
   - $C 0_{m\times n} = 0_{r\times n}$

Proof. We just take advantage of Theorem 2.6.31, which establishes the correspondence between linear function composition and matrix multiplication. Then these properties all follow from the corresponding properties for linear transformations.
Alternatively, we can prove these properties directly using the definition of matrix multiplication or one of the formulas given in Proposition 2.6.29 . □

Warning.
If $a, b \in \mathbb{R}$, then we have the very important property:

$$ab = 0 \iff a = 0 \quad \text{or} \quad b = 0.$$

The analogous property (which would, in some sense, does not hold for matrices. In other words, we may find that $A\,B$ is a zero matrix even if neither A nor B is a zero matrix: for an example, see part (ii) of Example 2.6.28.

We also note that matrix multiplication is not necessarily commutative (that is, the order of operation is important). For example, if $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 \\ 2 & 2 \end{bmatrix}$, then

$$A\,B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix},$$

while

$$B\,A = \begin{bmatrix} 2 & 0 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 4 \end{bmatrix}.$$

Definition 2.6.34: Power of a matrix

Let A be an $n \times n$ matrix. We define the kth power of A^k for $k \in \mathbb{N}$ inductively in the following way:

$$\begin{aligned} A^0 &= I_n, \\ A^1 &= A, \\ A^k &= A(A^{k-1}). \end{aligned}$$

Exercise 2.6.35

For every positive integer n, consider the matrix

$$R_n = \begin{bmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}.$$

Show that $R_n^n = I_2$.

Let us now end this section with the observation that a system of linear equations may be written in matrix form.

Example 2.6.36

The linear system of equations

$$\begin{aligned} x + y + z &= 3 \\ x + z &= 2 \\ 3x + 2y &= 0 \\ x + 2y + z &= 1 \end{aligned}$$

can be written as

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 3 & 2 & 0 \\ 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \\ 0 \\ 1 \end{bmatrix}$$

or, in other words,

$$A\boldsymbol{x} = \boldsymbol{b}$$

where $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 3 & 2 & 0 \\ 1 & 2 & 1 \end{bmatrix}$, $\boldsymbol{x} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ *and* $\boldsymbol{b} = \begin{bmatrix} 3 \\ 2 \\ 0 \\ 1 \end{bmatrix}$.

We will return to this idea later, after learning about matrix inverses.

Exercise 2.6.37

Find all vectors $\boldsymbol{x} \in \mathbb{R}^4$ *such that*

$$\begin{bmatrix} 3 & 4 & 6 & -3 \\ 2 & 1 & 5 & 4 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & -3 & 2 \end{bmatrix} \boldsymbol{x} = -\boldsymbol{x}.$$

Exercise 2.6.38

Let $A\boldsymbol{x} = \boldsymbol{b}$ be a system of linear equations in n variables with $\boldsymbol{b} \neq \boldsymbol{0}$ and $\boldsymbol{x}$ the vector of unknowns; let S be the set of solutions to this system. Suppose $S \neq \emptyset$ and $\boldsymbol{x_0} \in S$ is a solution to the system.

1. *Let $\boldsymbol{v} \in \mathbb{R}^n$ be a solution to the homogeneous system $A\,\boldsymbol{v} = \boldsymbol{0}$. Show that $\boldsymbol{x_0} + \boldsymbol{v} \in S$.*
2. *Suppose that $\boldsymbol{x_1} \in S$. Show that $(\boldsymbol{x_1} - \boldsymbol{x_0})$ is a solution to the homogeneous system $A\boldsymbol{x} = \boldsymbol{0}$.*
3. *Let H be the set of solutions to the homogeneous system $A\,\boldsymbol{x} = \boldsymbol{0}$, and define a set S' by*

   $$S' := \{\, \boldsymbol{x_0} + \boldsymbol{v} \mid \boldsymbol{v} \in H \,\}.$$

   Use part (1) to show that $S' \subseteq S$. Use part (2) to show that $S \subseteq S'$. Conclude that $S' = S$.

We have shown that the set of all solutions to the original system can be found by first finding a single solution $\boldsymbol{x_0}$, then finding all the solutions to the homogeneous system with the same coefficient matrix, and finally taking the sums of $\boldsymbol{x_0}$ with all the homogeneous solutions.

Exercise 2.6.39

It turns out that we can represent a complex number $z = a + b\mathrm{i}$ by the 2×2 real matrix

$$Z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Given another complex number $w = c + d\mathrm{i}$, let's denote its corresponding matrix representation by W. Prove that

(a) The matrix $Z + W$ represents the complex number $z + w$;

(b) The matrix ZW represents the complex number zw.

In maths jargon, we say that the field $\mathbb{C}$ is ***isomorphic*** *to the set of matrices*

$$\left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$$

together with the operations of matrix addition and multiplication.

2.6.6 Transpose of a matrix

Definition 2.6.40

If A is an $m \times n$ matrix then the ***transpose*** *of A, denoted $A^\top$, is the $n \times m$ matrix defined by $(A^\top)_{ij} = a_{ji}$.*

In other words, the rows of $A^\top$ are the columns of A and vice versa.

Example 2.6.41

The transpose of $\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\end{bmatrix}^\top = \begin{bmatrix}1 & 4\\ 2 & 5\\ 3 & 6\end{bmatrix}$, *and* $\begin{bmatrix}1 & 2 & 3\end{bmatrix}^\top = \begin{bmatrix}1\\ 2\\ 3\end{bmatrix}$.

Theorem 2.6.42: Properties of the transpose

Let A and B be $m \times n$ matrices, let C be a $r \times m$ matrix, and k a scalar. Then

(i) $\operatorname{row}_i(A^\top) = \operatorname{col}_i(A)^\top \qquad 1 \le i \le n$

(ii) $\operatorname{col}_j(A^\top) = \operatorname{row}_j(A)^\top \qquad 1 \le j \le m$

(iii) $\left(A^\top\right)^\top = A$.

(iv) Transposing is linear, i.e.,

- $(A+B)^\top = A^\top + B^\top$;
- $(kA)^\top = kA^\top$.

(v) $(CA)^\top = A^\top C^\top$

Proof. (i)

$$\operatorname{row}_i(A^\top) = \begin{bmatrix}(A^\top)_{i1} & \cdots & (A^\top)_{im}\end{bmatrix} = \begin{bmatrix}a_{1i} & \cdots & a_{mi}\end{bmatrix} = \begin{bmatrix}a_{1i}\\ \vdots\\ a_{mi}\end{bmatrix}^\top$$
$$= \operatorname{col}_i(A)^\top.$$

(ii) Same as above, *mutatis mutandis*.

(iii) $\left(\left(A^\top\right)^\top\right)_{ij} = \left(A^\top\right)_{ji} = a_{ij}$.

(iv) Easy exercise.

(v)

$$\begin{aligned}(A^\top C^\top)_{ij} &= \sum_{k=1}^{m} (A^\top)_{ik}(C^\top)_{kj} = \sum_{k=1}^{m} a_{ki}c_{jk} = \sum_{k=1}^{m} c_{jk}a_{ki} \\ &= (CA)_{ji} = \left((CA)^\top\right)_{ij}.\end{aligned}$$

□

Exercise 2.6.43

Let $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^n$, and let A be an $n \times n$ matrix. Show that:

1. $\boldsymbol{u}^\top \boldsymbol{v} = \boldsymbol{u} \cdot \boldsymbol{v}$;
2. $(A\,\boldsymbol{u}) \cdot \boldsymbol{v} = \boldsymbol{u} \cdot (A^\top \boldsymbol{v})$;
3. *Show that every linear transformation $f : \mathbb{R}^n \to \mathbb{R}$ is of the form $f(\boldsymbol{v}) = \boldsymbol{a} \cdot \boldsymbol{v}$ for some $\boldsymbol{a} \in \mathbb{R}^n$.*
   (Hint: write down the matrix for f and use (1).)

The second property is known as the ***adjoint*** *property.*

Exercise 2.6.44

If A is an $n \times n$ matrix, define the ***trace*** *of A, written $\operatorname{tr}(A)$, to be the sum of the diagonal entries of A.*

1. *Show that $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B)$ (if A, B are $n \times n$ matrices), and that $\operatorname{tr}(A^\top) = \operatorname{tr}(A)$.*
2. *Find two matrices A and B such that*
   $\operatorname{tr}(A\,B) \neq \operatorname{tr}(A)\,\operatorname{tr}(B)$.
3. *Find two matrices A and B such that*
   $\operatorname{tr}(A\,B) = \operatorname{tr}(A)\,\operatorname{tr}(B)$.
4. *Show that, if A and B are $n \times n$ matrices, then*

   (a) $\operatorname{tr}(A\,B) = \operatorname{tr}(B\,A)$; *and*
   (b) $\operatorname{tr}(A\,B\,A^{-1}) = \operatorname{tr}(B)$ *(if A is invertible).*

2.7 Inverses in linear algebra

2.7.1 Injective linear functions

Definition 2.7.1

- *The* ***null space*** (or ***kernel***) *of a linear function* $L : U \to V$ *is the solution set of the linear equation* $L(\mathbf{u}) = \mathbf{0}$*, i.e.,*

$$\mathrm{Null}(L) := \{\mathbf{u} \in U \mid L(\mathbf{u}) = \mathbf{0}\}.$$

- *The* ***null space*** *of a matrix* $A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$ *is the solution set of the linear equation* $A\mathbf{u} = \mathbf{0}$*, i.e.,*

$$\mathrm{Null}(A) := \{\mathbf{u} \in \mathbb{R}^n \mid A\mathbf{u} = \mathbf{0}\}.$$

The following exercise is a generalisation of Proposition 2.2.12.

Exercise 2.7.2

Prove the following:

(i) For any linear map $L : U \to V$*,* $\mathrm{Null}(L)$ *is a linear subspace of* U*.*

(ii) For any $A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$*,* $\mathrm{Null}(A)$ *is a linear subspace of* $\mathbb{R}^n$*.*

For a linear function, the following Lemma gives a very useful way to check if it is injective.

Theorem 2.7.3

Let U *and* V *be* $\mathbb{R}$*-vector spaces, and let* $L : U \to V$ *be a linear function. Then* L *is injective if and only if* $\mathrm{Null}(L) = \{\mathbf{0}\}$*.*

Proof. By definition, if $\mathbf{x} \in \mathrm{Null}(L)$ then

$$L(\mathbf{x}) = \mathbf{0} = L(\mathbf{0}).$$

Thus, if L is injective then $\mathbf{x} = \mathbf{0}$.
For any vectors $\mathbf{u}_1, \mathbf{u}_2 \in U$, notice that

$$\begin{aligned} L(\mathbf{u}_1) = L(\mathbf{u}_2) &\iff L(\mathbf{u}_1) - L(\mathbf{u}_2) = \mathbf{0} \iff L(\mathbf{u}_1 - \mathbf{u}_2) = \mathbf{0} \\ &\iff \mathbf{u}_1 - \mathbf{u}_2 \in \mathrm{Null}(L). \end{aligned}$$

Thus, if $\mathrm{Null}(L) = \{\mathbf{0}\}$ then

$$L(\mathbf{u}_1) = L(\mathbf{u}_2) \implies \mathbf{u}_1 - \mathbf{u}_2 = \mathbf{0} \implies \mathbf{u}_1 = \mathbf{u}_2.$$

□

In other words, we have shown that a linear function $L : U \to V$ is injective if and only if for every $\mathbf{u} \in U$,

$$L(\mathbf{u}) = \mathbf{0} \implies \mathbf{u} = \mathbf{0}.$$

Example 2.7.4

Consider the linear function

$$\begin{array}{rccc} L: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^3 \\ & \begin{bmatrix} x \\ y \end{bmatrix} & \longmapsto & \begin{bmatrix} x \\ y \\ 0 \end{bmatrix} \end{array}$$

Then $L\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ *if and only if* $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, *so*

$$\text{Null}(L) = \{\mathbf{0}\}.$$

Thus, L is injective by Theorem 2.7.3. A left-inverse (which happens to be linear) is

$$\begin{array}{rccc} F: & \mathbb{R}^3 & \longrightarrow & \mathbb{R}^2 \\ & \begin{bmatrix} x \\ y \\ z \end{bmatrix} & \longmapsto & \begin{bmatrix} x \\ y \end{bmatrix} \end{array}$$

Proposition 2.7.5

Let $L : U \to V$ be an injective linear function. If $X \subseteq U$ is a linearly independent subset, then $L(X) \subseteq V$ is a linearly independent subset.

Proof. Consider a list of distinct vectors $(\mathbf{y}_1, \ldots, \mathbf{y}_k)$ from $L(X)$. We want to solve the equation

$$\sum_{i=1}^{k} c_i \mathbf{y}_i = \mathbf{0}$$

for the scalars c_i. By injectivity of L, we know that there exist distinct vectors $\mathbf{x}_i \in X$ such that $L(\mathbf{x}_i) = \mathbf{y}_i$, $1 \leq i \leq k$. Substituting into the equation we wish to solve and using linearity, we get:

$$\mathbf{0} = \sum_{i=1}^{k} c_i L(\mathbf{x}_i) = L\left(\sum_{i=1}^{k} c_i \mathbf{x}_i\right).$$

Since L is injective, then by Theorem 2.7.3 it must be the case that

$$\sum_{i=1}^{k} c_i \mathbf{x}_i = \mathbf{0}.$$

Since the subset X was assumed to be linearly independent, then we must have

$$c_1 = \cdots = c_k = 0.$$

Thus, $L(X)$ is indeed linearly independent. □

This states that injective linear functions preserve linear independence! In other words, given a set of linearly independent inputs, an injective linear function will produce a set of linearly independent outputs.

Corollary 2.7.6

Let $L : U \to V$ be a linear function, and let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be an ordered basis for U. Then

$$L \text{ is injective} \iff (L(\mathbf{b}_1), \ldots, L(\mathbf{b}_n)) \text{ is linearly independent.}$$

Proof.

- $(\implies)$. This is just a special case of Proposition 2.7.5.
- $(\impliedby)$. Suppose that $(L(\mathbf{b}_1), \ldots, L(\mathbf{b}_n))$ is linearly independent. Let $\mathbf{u} \in \mathrm{Null}(L)$ be arbitrary. We can express it as a linear combination of the basis as follows

  $$\mathbf{u} = \sum_{j=1}^{n} c_j \mathbf{b}_j.$$

  Applying L gives us

  $$\mathbf{0} = \sum_{j=1}^{n} c_j L(\mathbf{b}_j)$$

  Because $(L(\mathbf{b}_1), \ldots, L(\mathbf{b}_n))$ is linearly independent then

  $$c_1 = \cdots = c_n = 0,$$

  so $\mathbf{u} = \mathbf{0}$.

□

2.7.2 Surjective linear functions

Remark 2.7.7

Given a linear function $L : U \to V$, by Proposition 2.5.4 its range $L(U)$ is a linear subspace of its codomain V.

Lemma 2.7.8

Let $L : U \to V$ be a linear function, and $X \subseteq U$. Then

$$L(\operatorname{Span} X) = \operatorname{Span} L(X).$$

Proof.

- $(\subseteq)$ Suppose that $\mathbf{v} \in L(\operatorname{Span} X)$. Then there exist some vectors $\mathbf{x}_j \in X$ and scalars $a_j \in \mathbb{R}$ such that

$$\mathbf{v} = L\left(\sum_{j=1}^{k} a_j \mathbf{x}_j\right) = \sum_{j=1}^{k} a_j L(\mathbf{x}_j).$$

  Thus, $\mathbf{v} \in \operatorname{Span} L(X)$.

- $(\supseteq)$ Conversely, suppose that $\mathbf{v} \in \operatorname{Span} L(X)$. Then there exist some vectors $\mathbf{x}_j \in X$ and scalars $b_j \in \mathbb{R}$ such that

$$\mathbf{v} = \sum_{j=1}^{l} b_j L(\mathbf{x}_j) = L\left(\sum_{j=1}^{l} b_j \mathbf{x}_j\right).$$

  Thus, $\mathbf{v} \in F(\operatorname{Span} X)$.

□

Let $L : \mathbb{R}^n \to \mathbb{R}^m$ be a linear function. Given a vector $\mathbf{y} \in \mathbb{R}^m$, we can ask if there exists a solution $\mathbf{x} \in \mathbb{R}^n$ to the linear equation

$$L(\mathbf{x}) = \mathbf{y}.$$

This occurs if and only if

$$\mathbf{y} = L(\mathbf{x}) = L\left(\sum_{j=1}^{n} x_j \mathbf{e}_j\right) = \sum_{j=1}^{n} x_j L(\mathbf{e}_j).$$

Thus,

$$\mathbf{y} \in L(\mathbb{R}^n) \iff \mathbf{y} \in \operatorname{Span}\{L(\mathbf{e}_1), \dots, L(\mathbf{e}_n)\}$$

We can state this more generally as follows:

Proposition 2.7.9

Let U, V be $\mathbb{R}$-vector spaces, and let $L : U \to V$ be a linear function. Let $X \subseteq U$ be a spanning subset, i.e., $\operatorname{Span} X = U$. *Then*

$$L \text{ is surjective} \iff \operatorname{Span}(L(X)) = V.$$

Proof. Since we assumed $U = \operatorname{Span} X$, then we can apply Lemma 2.7.8 to get our desired result:

$$L : U \to V \text{ is surjective} \iff V = L(U) = L(\operatorname{Span} X) = \operatorname{Span}(L(X)).$$

□

The following is merely a special case of Proposition 2.7.9, but we wish to emphasize this result:

Corollary 2.7.10

Let $L : U \to V$ be a linear function, and let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be an ordered basis for U. Then

$$L \text{ is surjective} \iff \operatorname{Span}\{L(\mathbf{b}_1), \ldots, L(\mathbf{b}_n)\} = V.$$

In particular, to determine if a linear function $L : \mathbb{R}^n \to \mathbb{R}^m$ is surjective, we just need to check that the columns of its standard matrix span its codomain!

Example 2.7.11

The function $L : \mathbb{R}^3 \to \mathbb{R}^2$ from Example 2.7.4 is a linear function. Furthermore,

$$\operatorname{Span}\{L(\mathbf{e}_1), L(\mathbf{e}_2), L(\mathbf{e}_3)\} = \operatorname{Span}\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\0\end{bmatrix}\right\} = \mathbb{R}^2,$$

so L is surjective (as expected).

2.7.3 Bijective linear functions

Example 2.7.12

Consider the linear function

$$\begin{aligned} L : \quad \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ \begin{bmatrix}x\\y\end{bmatrix} &\longmapsto x + y \end{aligned}$$

Check that the following functions are right inverses of L:

$$\begin{aligned} \operatorname{ins}_1 : \mathbb{R} &\to \mathbb{R}^2 \\ x &\mapsto \begin{bmatrix}x\\0\end{bmatrix}, \end{aligned} \qquad \begin{aligned} \operatorname{ins}_2 : \mathbb{R} &\to \mathbb{R}^2 \\ x &\mapsto \begin{bmatrix}0\\x\end{bmatrix}, \end{aligned} \qquad \begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R}^2 \\ x &\mapsto \begin{bmatrix}x+1\\-1\end{bmatrix}. \end{aligned}$$

Solution.
Let's calculate the following composite rules:

$$(L \circ \text{ins}_1)(x) = L(\text{ins}_1(x)) = L\left(\begin{bmatrix} x \\ 0 \end{bmatrix}\right) = x + 0 = x = \text{id}_{\mathbb{R}}(x)$$

$$(L \circ \text{ins}_2)(x) = L(\text{ins}_2(x)) = L\left(\begin{bmatrix} 0 \\ x \end{bmatrix}\right) = 0 + x = x = \text{id}_{\mathbb{R}}(x)$$

$$(L \circ f)(x) = L(f(x)) = L\left(\begin{bmatrix} x+1 \\ -1 \end{bmatrix}\right) = (x+1) + (-1) = x = \text{id}_{\mathbb{R}}(x)$$

Thus, ins_1, ins_2, and f are all right inverses of L. We see that L, ins_1 and ins_2 are linear, but f is clearly not linear, so we conclude that a right inverse of a linear function is not necessarily linear!

However, we can say the following. We will not prove this result in the course since it requires some techniques from MATHS 250, but it is not particularly difficult.

Remark 2.7.13

Let $L : \mathbb{R}^n \to \mathbb{R}^m$ be a linear function. Then the following hold:

1. *If L is injective then there exists at least one linear left-inverse to L.*
2. *If L is surjective then there exists at least one linear right-inverse to L.*

Fortunately, a two-sided inverse of a linear function is guaranteed to be linear:

Theorem 2.7.14

Let U, V be $\mathbb{R}$-vector spaces, and suppose that $L : U \to V$ is a bijective linear function. Then its inverse $L^{-1} : V \to U$ is also linear.

Proof. Let $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2 \in V$, and let c be a scalar. Using the fact L is linear and that $LL^{-1} = \text{id}_V$, we get:

$$\begin{aligned} L^{-1}(\mathbf{v}_1 + \mathbf{v}_2) &= L^{-1}(LL^{-1}\mathbf{v}_1 + LL^{-1}\mathbf{v}_2) \\ &= L^{-1}L\left(L^{-1}\mathbf{v}_1 + L^{-1}\mathbf{v}_2\right) \\ &= L^{-1}\mathbf{v}_1 + L^{-1}\mathbf{v}_2. \end{aligned}$$

Again, using the same strategy:

$$\begin{aligned} L^{-1}(c\mathbf{v}) &= L^{-1}(cLL^{-1}\mathbf{v}) \\ &= L^{-1}L(cL^{-1}\mathbf{v}) \end{aligned}$$

$$= cL^{-1}\mathbf{v}.$$

□

Remark 2.7.15

It is quite special that the inverse of a linear function is automatically linear. For comparison, the inverse of a differentiable function is not necessarily differentiable. Indeed, for the MATHS *130 students, you can check that the function $f : \mathbb{R} \to \mathbb{R}$ given by the formula $f(x) := x^3$ is differentiable and bijective, but its inverse fails to be differentiable at the origin.*

We will address the problem of actually computing the inverse of a linear function in Section 2.7.4. Before we do, we want to show two crucial things about invertibility of linear functions:

1. If $L : \mathbb{R}^n \to \mathbb{R}^m$ is an invertible linear function, then $n = m$.
2. If $L : \mathbb{R}^n \to \mathbb{R}^n$ is a linear function (with $\mathbb{R}^n$ as both its domain and codomain), then having *either* a right- or left-inverse is sufficient to be invertible.

Theorem 2.7.16

Let $L : U \to V$ be a linear function, and let $B := (\mathbf{b}_1, \dots, \mathbf{b}_n)$ be an ordered basis for U. Then L is bijective if and only if $(L(\mathbf{b}_1), \dots, L(\mathbf{b}_n))$ is an (ordered) basis for V.

Proof. This is just putting together Corollary 2.7.6 and Corollary 2.7.10. □

Continuing the analogy between finite-dimensional vector spaces and finite sets (pointed out in Remark 2.7.20), notice that the following Corollary is analogous to Exercise 1.4.19.

Corollary 2.7.17

Let $L : \mathbb{R}^n \to \mathbb{R}^m$ be a linear function. If L is bijective, then $n = m$.

Proof. Suppose L is bijective, and consider the standard ordered basis $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ for $\mathbb{R}^n$. Then $(L(\mathbf{e}_1), \dots, L(\mathbf{e}_n))$ is an ordered basis for $\mathbb{R}^m$ by Theorem 2.7.16. But since $\dim(\mathbb{R}^m) = m$, then we apply Theorem 2.3.22 to conclude that $n = m$. □

We now have all the tools to prove the following. Note the very strong resemblance to Proposition 1.4.18!

Proposition 2.7.18

Let $L : \mathbb{R}^n \to \mathbb{R}^m$ be a linear function.

1. *If $n > m$, then L is not injective.*
2. *If $n < m$, then L is not surjective.*
3. *If $n = m$, then L is injective if and only if it is surjective.*

Proof.

1. If L were injective then $(L\mathbf{e}_1, \ldots, L\mathbf{e}_n)$ would be linearly independent. But since $n > m$, this would violate Theorem 2.3.22

2. If L were surjective then we would have
$$\operatorname{Span}\{L\mathbf{e}_1, \ldots, L\mathbf{e}_n\} = \mathbb{R}^m.$$
But since $n < m$, this would violate Theorem 2.3.22

3. Since $n = m$, then by Corollary 2.3.23 the list
$$(L\mathbf{e}_1, \ldots, L\mathbf{e}_n)$$
is linearly independent if and only it spans the codomain $\mathbb{R}^m$. Applying Corollaries 2.7.6 and 2.7.10 gives the desired conclusion.

□

An immediate consequence of Proposition 2.7.18 is that for a linear function between vector spaces of the same dimension, any left inverses are automatically right inverses, and *vice versa*!

Corollary 2.7.19

Let $f : \mathbb{R}^m \to \mathbb{R}^n$ be a function, and let $L : \mathbb{R}^n \to \mathbb{R}^m$ be a linear function. If $n = m$ then

$$F \text{ is a left inverse of } L \iff F \text{ is a right inverse of } L.$$

Remark 2.7.20

Because a linear function $F : \mathbb{R}^n \to \mathbb{R}^m$ is uniquely determined by where it sends the standard basis $(\mathbf{e}_1, \dots, \mathbf{e}_n)$, F behaves a lot like a function between finite sets $f : N \to M$, where $|N| = n$ and $|M| = m$. Indeed, we encourage you to review Section 1.4.2, and to try to notice some similarities between the results here and there.

*For the curious student, it turns out that this similarity can be made precise using an area of "meta-mathematics" called category theory: the collection of finite-dimensional vector spaces is a **categorification** of the natural numbers.*

2.7.4 Matrix inverses

We can define left- and right-inverses of matrices in the same way as we did for functions:

Definition 2.7.21

If A is an $m \times n$ matrix, we say that an $n \times m$ matrix B is

1. *a **left-inverse** of A if $B\,A = I_n$,*
2. *a **right-inverse** of A if $A\,B = I_m$, and*
3. *an **inverse** of A if it is both a left- and right-inverse.*

*If B is an inverse of A, then we say that the matrix A is **invertible** (or **non-singular**), and that B is its **inverse**. Uniqueness of the matrix inverse follows from uniqueness of inverses of functions, and we write $B = A^{-1}$.*

Remark 2.7.22

Since composition of linear functions corresponds to matrix multiplication, we can translate the results from the previous three subsections into matrix language!

Example 2.7.23

If A is an invertible $n \times n$ matrix then $A^\top$ is also invertible and

$$(A^\top)^{-1} = (A^{-1})^\top.$$

Solution.

By Theorem 2.6.42, we have

$$A^\top\,(A^{-1})^\top = (A^{-1}\,A)^\top = I_n^\top = I_n,$$

so $(A^{-1})^\top$ is the inverse of $A^\top$.

Example 2.7.24

Recall from Exercise 2.6.35 that the matrix

$$R_n = \begin{bmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}.$$

satisfies $R_n^n = I_2$.

- *Note that $R_n^n = R_n\,R_n^{n-1}$. Hence, R_n has a right-inverse and it is R_n^{n-1}.*
- *Similarly, we also have $R_n^n = R_n^{n-1}\,R_n$, so R_n^{n-1} is also a left-inverse of R_n.*
- *Therefore, R_n is invertible with inverse $R_n^{-1} = R_n^{n-1}$.*

Proposition 2.7.25: Properties of matrix inverse

Let A and B be invertible $n \times n$ matrices. Then the following hold:

1. $(A^{-1})^{-1} = A$;
2. $(A^k)^{-1} = (A^{-1})^k$ *for all* $k \in \mathbb{N}$;
3. $(A\,B)^{-1} = B^{-1}\,A^{-1}$;
4. $(c\,A)^{-1} = \frac{1}{c}\,A^{-1}$ *for all* $c \in \mathbb{R}\backslash\{0\}$.

Proof.

1. This follows directly from the definition. Alternatively, it follows from the analogous statement for functions.
2. We prove this by induction. Let $P(k)$ be the statement: $(A^k)^{-1} = (A^{-1})^k$.

   Base case.
   The case $k = 0$ is trivial, because I_n is its own inverse.

   Inductive step.
   For the inductive step, let $i \geq 1$ and assume that $P(i)$ is true, that is, $(A^i)^{-1} = (A^{-1})^i$. We will show that $P(i+1)$ holds by showing that $A^{i+1}\,(A^{-1})^{i+1} = I_n$. Note that

   $$A^{i+1}\,(A^{-1})^{i+1} = A\,A^i\,(A^{-1})^i\,A^{-1} = A\,I_n\,A^{-1} = A\,A^{-1} = I_n.$$

Therefore, by the Principle of Mathematical Induction, we conclude that $(A^k)^{-1} = (A^{-1})^k$ for all $k \in \mathbb{N}$.

3.

$$\begin{aligned}(AB)(B^{-1}A^{-1}) &= A(BB^{-1})A^{-1}\\ &= AI_nA^{-1}\\ &= AA^{-1}\\ &= I_n.\end{aligned}$$

4. $(cA)\left(\frac{1}{c}A^{-1}\right) = c\left(\frac{1}{c}\right)AA^{-1} = 1I_n = I_n.$ □

By Corollary 2.7.19, in order to determine whether a particular $n \times n$ matrix A is invertible, it suffices to try to solve the system $AB = I_n$ for an arbitrary $n \times n$ matrix B; this reduces to solving a system of n^2 linear equations.

Example 2.7.26

Show that the matrix $\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$ *is* **not** *invertible.*

Solution.

If $\begin{bmatrix}a & b\\ c & d\end{bmatrix}$ is its inverse, then

$$\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix} = \begin{bmatrix}a+c & b+d\\ a+c & b+d\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}.$$

Equating coefficients yields a system of four linear equations in a, b, c and d. This system is inconsistent (for example, we have $0 = a+c = 1$), so $\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$ is not invertible.

Example 2.7.27

Show that $\begin{bmatrix}1 & 0 & 2\\ 2 & -1 & 3\\ 4 & 1 & 8\end{bmatrix}$ *is invertible and find its inverse.*

Solution.

Let $A = \begin{bmatrix}1 & 0 & 2\\ 2 & -1 & 3\\ 4 & 1 & 8\end{bmatrix}$. We need to find a matrix B such that $A\,B = I_3$.

Let $B = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$. Now $\begin{bmatrix} a \\ d \\ g \end{bmatrix}$ is a solution to the matrix equation

$$\begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

and $\begin{bmatrix} b \\ e \\ h \end{bmatrix}$ is a solution to the matrix equation

$$\begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

and $\begin{bmatrix} c \\ f \\ i \end{bmatrix}$ is a solution to the matrix equation

$$\begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

So we need to solve these 3 systems of linear equations. Note that the left side is the same in all of them, so let us try solving them all at once.

$$\left[\begin{array}{ccc|c|c|c} 1 & 0 & 2 & 1 & 0 & 0 \\ 2 & -1 & 3 & 0 & 1 & 0 \\ 4 & 1 & 8 & 0 & 0 & 1 \end{array}\right] \begin{array}{l} \\ R_2 \leftarrow R_2 - 2R_1 \\ R_3 \leftarrow R_3 - 4R_1 \end{array}$$

$$\left[\begin{array}{ccc|c|c|c} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & -1 & -1 & -2 & 1 & 0 \\ 0 & 1 & 0 & -4 & 0 & 1 \end{array}\right] \begin{array}{l} \\ R_2 \leftarrow R_3 \\ R_3 \leftarrow R_2 \end{array}$$

$$\left[\begin{array}{ccc|c|c|c} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & -4 & 0 & 1 \\ 0 & -1 & -1 & -2 & 1 & 0 \end{array}\right] \begin{array}{l} \\ \\ R_3 \leftarrow R_3 + R_2 \end{array}$$

$$\left[\begin{array}{ccc|c|c|c} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & -4 & 0 & 1 \\ 0 & 0 & -1 & -6 & 1 & 1 \end{array}\right] \begin{array}{l} R_1 \leftarrow R_1 + 2R_3 \\ \\ \quad R_3 \leftarrow -R_3 \end{array}$$

$$\left[\begin{array}{ccc|c|c|c} 1 & 0 & 0 & -11 & 2 & 2 \\ 0 & 1 & 0 & -4 & 0 & 1 \\ 0 & 0 & 1 & 6 & -1 & -1 \end{array}\right]$$

Therefore, $\begin{bmatrix} a \\ d \\ g \end{bmatrix} = \begin{bmatrix} -11 \\ -4 \\ 6 \end{bmatrix}$, $\begin{bmatrix} b \\ e \\ h \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \\ -1 \end{bmatrix}$ and $\begin{bmatrix} c \\ f \\ i \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ -1 \end{bmatrix}$ and so

$$B = \begin{bmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{bmatrix}.$$

For a shorthand version, consider the 3×6 matrix:

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 2 & -1 & 3 & 0 & 1 & 0 \\ 4 & 1 & 8 & 0 & 0 & 1 \end{array}\right] = [A : I_3]$$

and reduce the left hand side to reduced echelon form to get:

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -11 & 2 & 2 \\ 0 & 1 & 0 & -4 & 0 & 1 \\ 0 & 0 & 1 & 6 & -1 & -1 \end{array}\right] = [I_3 : B] = [I_3 : A^{-1}].$$

General procedure to find matrix inverse

We now state and prove a general procedure for computing the inverse of a square matrix without solving a system of n^2 equations.

Algorithm 2.7.28

To find the inverse of a given $n \times n$ matrix A:

1. *Form the $n \times 2n$ augmented matrix $[A \mid I_n]$.*
2. *Row reduce $[A \mid I_n]$ into reduced echelon form.*
3. *If in the left $n \times n$ block, a row of zeros emerges, then stop (A is not invertible in this case). Otherwise, the left $n \times n$ block must reduce to I_n; the right $n \times n$ block of the reduced matrix is then A^{-1}.*

At the end of this procedure, you can check your answer by computing $A\,A^{-1}$, which should be I_n.

Proof of the algorithm.
Recall from Corollary 2.7.19 that it suffices to find a square right-inverse for A: that is, an $n \times n$ matrix B with the property that $A\,B = I_n$. If such a matrix exists, then A is invertible with unique inverse B.

Solving the equation $A\,B = I_n$ is equivalent to solving the n matrix equations $A\,\boldsymbol{b_i} = \boldsymbol{e_i}$ for $1 \leq i \leq n$, where $\boldsymbol{b_i}$ is the ith column of B. Now note that $A\boldsymbol{b_i} = \boldsymbol{e_i}$ can be solved uniquely if and only if A is row-reducible to the identity matrix: indeed, a system of equations is solvable uniquely if and only if it can be reduced by row-reduction to a system without free variables that can be solved by back substitution; and such a system has the identity matrix as its coefficient matrix (compare with Theorem 2.1.21). Further, the coefficients of $\boldsymbol{b_i}$ are the coefficients of the $(n+1)$th column of the matrix resulting from row-reducing the augmented matrix $[A : \boldsymbol{e_i}]$ to some matrix $[I_n \,|\, \boldsymbol{b_i}]$. The algorithm listed above just carries out this procedure for every i at once. □

Most computer codes, such as, for example MATLAB, do not use Gaussian elimination to find the inverse of a matrix; this is because imperfect computer arithmetic can significantly affect the process of Gaussian elimination. You can learn about more accurate and also faster methods to invert a matrix, or solve a system of linear equations, in a course on advanced numerical analysis.

Matrix inverses can sometimes be useful to solve systems of linear equations. Given such a system in the form $A\mathbf{x} = \mathbf{y}$, as in Example 2.6.36, if A is invertible, then the system has a unique solution, namely $A^{-1}\mathbf{y}$. This is particularly useful if one next wants to solve another linear system $A\,\mathbf{x} = \mathbf{z}$, since we have already computed A^{-1}.

Example 2.7.29

If possible, find the inverses of each of the following matrices.

(i) $A = \begin{bmatrix} 1 & 2 & 1 \\ 3 & 1 & 2 \\ 9 & -2 & 5 \end{bmatrix}$;

(ii) $B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$.

Solution.

(i) Not invertible:

(ii) $\begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}$.

The matrix B in Example 2.7.29 is called **lower triangular**, because every non-zero entry appears on or below the diagonal, i.e., if $i < j$ then $B_{ij} = 0$. Similarly, a matrix A is called **upper triangular** if the only non-zero entries of A appear on or above the diagonal; more precisely, if $i > j$ then $A_{ij} = 0$. The following matrix is an example:

$$\begin{bmatrix} 1 & 0 & 13 & 4 \\ 0 & 0 & 4 & -1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{2.2}$$

A matrix is **triangular** if it is either upper or lower triangular. Observe that the result of a row reduction to echelon form will always produce an upper triangular matrix.

We now show how a very similar procedure can be used to find right- and left-inverses of matrices.

Example 2.7.30

Find the right-inverses of each of the following matrices.

1. $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$;

2. $\begin{bmatrix} 1 & 0 \end{bmatrix}$.

Solution.

1. Let $A = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$. A right inverse B of A must be a 1×2 matrix such that $AB = I_2$. Now, writing $B = \begin{bmatrix} a & b \end{bmatrix}$, we have $AB = \begin{bmatrix} a & b \\ 2a & 2b \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ which yields $a = 2b = 1$ and $2a = b = 0$. This system has no solution, so A does not have a right-inverse.
2. Let $A = \begin{bmatrix} 1 & 0 \end{bmatrix}$. A right inverse B of A must be a 2×1 matrix such that $AB = I_1$. Now, writing $B = \begin{bmatrix} a \\ b \end{bmatrix}$, we have $AB = \begin{bmatrix} a \end{bmatrix} = \begin{bmatrix} 1 \end{bmatrix}$ which yields $a = 1$. We can then choose b freely, so A has infinitely many right-inverses.

Finding left-inverses can be done in a similar fashion.

Exercise 2.7.31

Let $a, b, c, d \in \mathbb{R}$, and assume that $ad - bc \neq 0$. Show that the matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is invertible, by computing its inverse. Conversely, show that if $ad - bc = 0$ then the matrix A is not invertible.

2.7.5 Elementary matrices

Definition 2.7.32

An ***elementary matrix*** *is a matrix obtained by applying a single elementary row operation to the identity matrix.*

Since there are three kinds of elementary row operations (recall Section 2.1.3), there are three types of elementary matrices.

Example 2.7.33

Starting with I_4, we apply the following elementary row operations to get an elementary matrix.

1. *Multiplying the second row by 2:*

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

2. *Adding three times the second row to the fourth row:*

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 \end{bmatrix}$$

3. *Swapping rows 1 and 3:*

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Exercise 2.7.34

Let R be an elementary row operation and let E be the corresponding elementary matrix. Verify that the matrix $E\,A$ is equal to the matrix obtained by applying the elementary row operation R to A.

Exercise 2.7.35

Show that the three types of elementary matrices are invertible, and that the inverse of an elementary matrix is also an elementary matrix.

Theorem 2.7.36: Invertible matrix vs elementary matrices

A matrix is invertible if and only if it is a product of elementary matrices.

Proof. By Exercise 2.7.35 and Proposition 2.7.25 a product of elementary matrices is invertible. The converse follows immediately from similar methods to the proof of Algorithm 2.7.28: if A is invertible, then A is row-reducible to I_n; that is, $E_m \cdots E_1 A = I_n$, where $E_1, \ldots, E_m$ are the elementary matrices corresponding to the row-reduction steps; it follows immediately that $A = E_1^{-1} \cdots E_m^{-1}$, so by Exercise 2.7.35 A is a product of elementary matrices. □

2.8 Determinants

Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear transformation given by

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} 2x \\ 2y \end{bmatrix}.$$

Note that the matrix associated to f is $2\,I_2$. Now, if we start with the unit square (of area 1) and apply f, we end up with a square that has sides of length 2 and area 4; the area of the image under f is, therefore, 4 times the area of the original square. In fact, it is not hard to see that the image under f of *any* shape in the plane will have 4 times the area of the original shape. The number 4 is therefore a fundamental invariant of f and its associated matrix $2\,I_2$ (with respect to the standard basis). We will say that 4 is the **determinant** of this matrix.

More generally, the determinant of a square matrix is a scalar invariant that encodes the "scaling factor" of the linear transformation described by the matrix.

As we will see, the determinant also comes equipped with a sign, which determines whether the linear transformation is *orientation-preserving* or not. For example, the linear transformation pictured in Figure 2.11 consists of a reflection in the vertical axis combined with scaling. It does not preserve the "clockwise orientation" of the plane, so it is not orientation-preserving, it is *orientation reversing*. Its determinant will then be negative.

2.8.1 The 2-dimensional case

The unit square is the square in $\mathbb{R}^2$ with vertices $(0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$. What happens when we apply the linear transformation corresponding to the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ to this unit square? As shown in Fig-

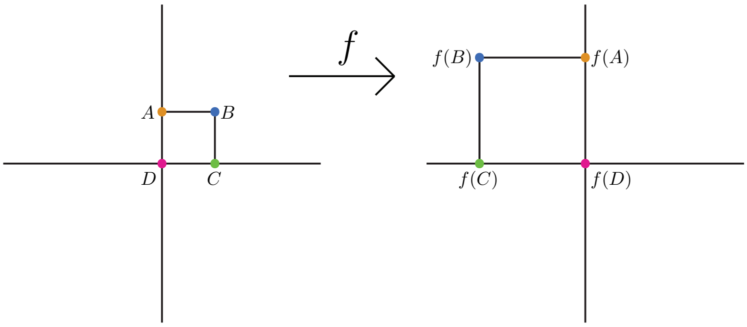


Figure 2.11: A reflection followed by scaling.

ure 2.12, it gets mapped to the parallelogram with vertices $(0, 0)$, (b, d), (a, c) and $(a + b, c + d)$. The unit square has area 1 while the image

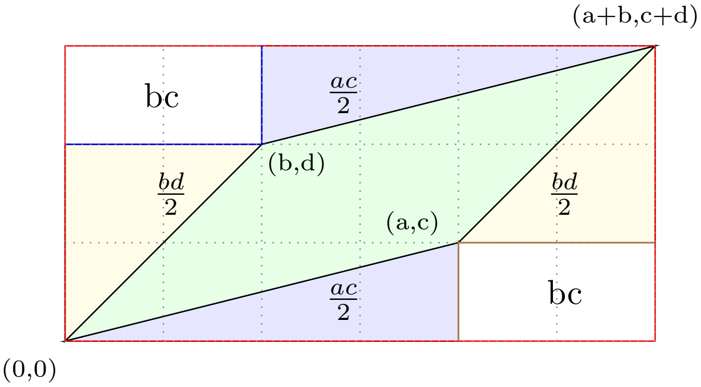


Figure 2.12: The action of a 2×2 matrix.

parallelogram has area

$$(a + b)\,(c + d) - 2\,b\,c - a\,c - b\,d = a\,d - b\,c.$$

We will therefore say that $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ has **determinant** $a\,d - b\,c$ and write this as

$$\det\left(\begin{bmatrix} a & c \\ b & d \end{bmatrix}\right) = a\,d - b\,c.$$

Exercise 2.8.1

Explain the connection to Exercise 2.7.31.

How do we establish a general formula in dimension greater than two? The next section shows that a few simple criteria completely determine the formula.

2.8.2 The general case

Definition 2.8.2: Determinant

*A **determinant** is a function, denoted* $\det$*, from the set of square matrices to* $\mathbb{R}$ *satisfying the following four properties:*

Normalisation. $\det(I_n) = 1$.

Zeroness. *If two columns of* A *are equal then* $\det(A) = 0$.

Homogeneity. *If one column is multiplied by a scalar then the determinant is multiplied by that scalar (Figure 2.13a).*

Additivity. *The function is "additive in each column"; more precisely, if we consider 3 matrices* A, A', A'' *with the properties: (a) that all but the* i*th columns agree; and (b) that the* i*th column of* A *is the sum of the* i*th columns of* A' *and* A''*, then* $\det(A) = \det(A') + \det(A'')$ *(Figure 2.13b).*

*The conditions of homogeneity and additivity are often listed together as **multilinearity**.*

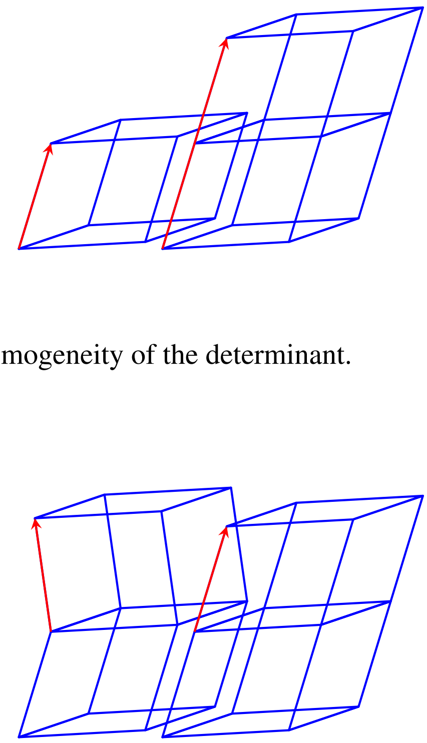
Remark 2.8.3: Origins of the concept of determinant

*The oldest documents about determinants are known as the Fukudai and dated 1683. They have been written Seki Takakazu, also known as Seki Kōwa, who was a leading mathematician in Japan. You can find out more online; see also the academic paper "On the Japanese Theory of Determinants" by Yoshio Mikami [Isis **2**(1): 9-36 (1914)].*

The result below is crucial, however its proof is outside of the scope of the course.

Theorem 2.8.4: Uniqueness of the determinant

The determinant is unique, i.e., there is exactly one function from the set of square matrices to $\mathbb{R}$ *satisfying the four properties from Definition 2.8.2.*



(a) Homogeneity of the determinant.

(b) Multilinearity of the determinant.

Figure 2.13: Geometric properties of the determinant.

Example 2.8.5: Determinant properties

We give a respective example of each of zeroness, homogeneity, and additivity:

$$\det \begin{bmatrix} 1 & 2 & 2 \\ 4 & 5 & 5 \\ 7 & 8 & 8 \end{bmatrix} = 0;$$

$$\det \begin{bmatrix} 1 & 2 & 30 \\ 4 & 5 & 60 \\ 7 & 8 & 90 \end{bmatrix} = 10 \det \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} = \det \begin{bmatrix} 10 & 2 & 3 \\ 40 & 5 & 6 \\ 70 & 8 & 9 \end{bmatrix};$$

$$\det \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} + \det \begin{bmatrix} 1 & 2 & 10 \\ 4 & 5 & 11 \\ 7 & 8 & 12 \end{bmatrix} = \det \begin{bmatrix} 1 & 2 & 3+10 \\ 4 & 5 & 6+11 \\ 7 & 8 & 9+12 \end{bmatrix}.$$

Remark 2.8.6: Geometric interpretation of the determinant

There is a geometric interpretation of the determinant, generalising that of the 2×2 case. In $\mathbb{R}^2$, the standard basis vectors $\{\boldsymbol{e_1}, \boldsymbol{e_2}\}$ define a square; in $\mathbb{R}^3$, the standard basis vectors $\{\boldsymbol{e_1}, \boldsymbol{e_2}, \boldsymbol{e_3}\}$ define a cube; and generally in $\mathbb{R}^n$, the standard basis vectors define what is known as a ***parallelopiped****. The determinant of a linear transformation $f : \mathbb{R}^n \to \mathbb{R}^n$ then measures the volume of the image of this parallelopiped under the transformation: that is, $\det(A)$ is the (signed) volume of the n-dimensional parallelopiped determined by the n image vectors $A\,\boldsymbol{e_1}, \ldots, A\,\boldsymbol{e_n}$. The case $n = 3$ is illustrated in Figure 2.13.*

Lemma 2.8.7

The determinant of a square matrix does not change when you add a multiple of one column to another.

Proof. For a matrix X, let X_i denote the ith column of X. Let $r \in \mathbb{R}$, let A be an $n \times n$ matrix and let B be the matrix obtained from A by adding r times the jth column of A to its ith column. (So $B = A$, except for the ith column, which is equal to $B_i = A_i + r\,A_j$.) We now construct the $n \times n$ matrix C that is also equal to A, except for its ith column, which is just $C_i = r\,A_j$. Hence, the ith columns of these matrices satisfy $B_i = A_i + C_i$ and the three matrices agree in all the other columns. It follows by additivity of the determinant that $\det(B) = \det(A) + \det(C)$. On the other hand, the ith column of C is a multiple of the jth column. Combining zeroness and homogeneity, we find that $\det(C) = 0$. Hence $\det(A) = \det(B)$, as required. □

Lemma 2.8.8

If two columns of a square matrix are interchanged, the determinant is multiplied by -1.

Proof. Let A be an $n \times n$ matrix and let $i, j \in \{1, \dots, n\}$. Consider the following sequence of column operations, where at each step, the operation is applied to the result of the preceding one.

1. Start with A; suppose A_i is the ith column of A;
2. Set $A_j \leftarrow A_i + A_j$;
3. Set $A_i \leftarrow A_i - A_j$ (so A_i is now $A_i - (A_i + A_j) = -A_j$);
4. Set $A_j \leftarrow A_i + A_j$ (so A_j is now the original A_i);
5. Set $A_i \leftarrow -A_i$ (so A_i is now the original A_j).

Hence the resulting matrix is A with its ith and jth column interchanged. Note also, by Lemma 2.8.7, that all these operations leave the determinant unchanged, except the last operation, which multiplies it by -1, by homogeneity. □

Lemma 2.8.9

If a column of a square matrix is zero, the determinant is 0.

Proof. Let the matrix be A and let the column of zeros by the i-th column. Let $k \in \mathbb{R}$ with $k \neq 0$ and $k \neq 1$, then by homogeneity, $\det A = k \det A'$ where A' is the matrix obtained by multiplying the ith column of A by $\frac{1}{k}$. But since that column is all zeros we have $A' = A$. Thus $\det A = k \det A$. Since $k \neq 1$ we obtain that $\det A = 0$. □

Exercise 2.8.10

Prove the above lemma using zeroness instead of homogeneity.

Note that a column of a square matrix is zero if and only if it maps one of the standard basis vectors to $\mathbf{0}$: that is, if the parallelopiped spanned by the images of the basis vectors is 'flat'. (It is best to visualise this in $\mathbb{R}^3$: see Figure 2.14, where it is the vertical direction that is sent to $\mathbf{0}$.) We will not prove the following very useful result:

Theorem 2.8.11

If A is a square matrix, then $\det(A) = \det(A^\top)$.

Theorem 2.8.11 is very useful, because it implies that, in every statement regarding the determinant, we can replace columns by rows. For example, together with Lemma 2.8.8, it implies that if two *rows* of a matrix are interchanged then the determinant is multiplied by -1.

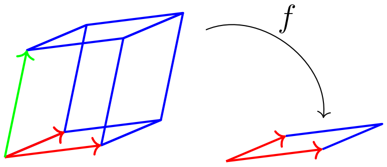


Figure 2.14: The action of a linear transformation $f : \mathbb{R}^3 \to \mathbb{R}^3$ associated with a matrix that has a zero column.

We now know enough about the determinant to calculate it for every square matrix. Indeed, given a square matrix A, we can use row operations to reduce it to row reduced echelon form, as in Section 2.1.3. We know the effect of each row operation on the determinant of A:

1. If B is obtained from A by interchanging two of its rows, then $\det(B) = -\det(A)$.
2. If B is obtained from A by multiplying a row of A by $r \in \mathbb{R}$, then $\det(B) = r\ \det(A)$.
3. If B is obtained from A by adding a multiple of a row of A to another row of A, then $\det(B) = \det(A)$.

We can apply these operations to the matrix, until we either get a zero row (in which case the determinant is 0), or we reach the identity matrix. We must keep track of the effect of the row operations on the determinant.

Example 2.8.12

Evaluate the determinant of $\begin{bmatrix} 0 & 1 \\ 2 & 4 \end{bmatrix}$.

Solution.
Let

$$A_1 = \begin{bmatrix} 0 & 1 \\ 2 & 4 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} 2 & 4 \\ 0 & 1 \end{bmatrix} \; R_2 \leftrightarrow R_1$$

$$A_3 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} R_1 \leftarrow (1/2)R_1$$

$$A_4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} R_1 \leftarrow R_1 - 2R_2$$

Using the rules above, we have

$$\begin{aligned} \det(A_2) &= -\det(A_1), \\ \det(A_3) &= (1/2)\det(A_2), \\ \det(A_4) &= \det(A_3), \\ \det(A_4) &= 1. \end{aligned}$$

Combining all of these, we get

$$\det(A_1) = -\det(A_2) = -2\ \det(A_3) = -2\ \det(A_4) = -2.$$

There is a potential problem with this approach: how do we know that a different choice of row operations will give the same answer? This is guaranteed by Theorem 2.8.4.

Proposition 2.8.13

Let A be an $n \times n$ matrix and let $r \in \mathbb{R}$. Show that

$$\det(r\,A) = r^n\ \det(A).$$

Proof. Multiplying one row of A by r multiplies the determinant by r. Since there are n rows, multiplying all the rows of A by r multiplies the determinant by r^n. □

Definition 2.8.14

A square matrix is ***diagonal*** *if its only non-zero entries are on the main diagonal.*

Example 2.8.15

$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{bmatrix}$ *is a diagonal matrix.*

Lemma 2.8.16

The determinant of a diagonal matrix is the product of the elements on the main diagonal.

Proof. Start with the identity matrix, and multiply each row by the appropriate scalar. □

Corollary 2.8.17

The determinant of either an upper or a lower triangular matrix is the product of the elements on the main diagonal.

Proof. Suppose first that the matrix is upper triangular. If the last row is zero, then the determinant is zero and there is a zero on the diagonal, so the result holds. Otherwise, it has a pivot in the last column, and we can add multiples of this row to other rows to get zeros above the pivot. We then move on to the next to last row. If it is not zero, then it has a pivot, and add multiples of the row to get zeros in that column. We repeat this process for each row, either getting a row of 0, or a diagonal matrix, with the same entries on the diagonal as the original matrix. By Lemma 2.8.17, the determinant of this diagonal matrix is the product of the diagonal entries, but our row operations have not changed the determinant, so this is also the determinant of our original matrix.

If our matrix is lower triangular, we can simply take the transpose and apply the previous paragraph. □

Theorem 2.8.18

If A is an $n \times n$ matrix, then A is invertible if and only if $\det(A) \neq 0$.

Proof. We know from earlier that A is invertible if and only if it may be row reduced to I_n. (Recall the algorithm for calculating A^{-1}.) Note that, in that process, the row operations involved do not affect the zeroness of the determinant. Therefore, if it can be reduced to I_n, then it has non-zero determinant. The only obstruction is getting a row of zero at some point, in which case $\det(A) = 0$. □

Remark 2.8.19: Geometric interpretation of $\det A = 0$

Recall that the geometric meaning of the determinant of a matrix A is as a measure of how the linear transformation determined by A changes volumes. Theorem 2.8.18 says that a linear transformation is invertible if and only if it takes shapes of positive volume and maps them into shapes of zero volume: more precisely, a linear transformation is not invertible if and only if it maps the basis vectors of $\mathbb{R}^n$ to a set that does not span $\mathbb{R}^n$.

Exercise 2.8.20: Determinant of a product with an elementary matrix

If E is an $n \times n$ elementary matrix (see Definition 2.7.32) and A is an $n \times n$ matrix, then $\det(E\,A) = \det(E)\,\det(A)$.

Theorem 2.8.21: Determinant is multiplicative

If A and B are $n \times n$ matrices, then $\det(A\,B) = \det(A)\det(B)$.

Proof. If A is not invertible, then neither is $A\,B$, by Theorem 2.7.19. In this case, by Theorem 2.8.18, we have both $\det(A\,B) = 0$ and $\det(A)\,\det(B) = 0$; in particular, both sides of the equality are zero.

We can thus assume that A is invertible. By Theorem 2.7.36, A is the product of elementary matrices, say $A = E_1 \cdots E_k$. Using Exercise 2.8.20, it follows that

$$\begin{aligned}
\det(A\,B) &= \det(E_1 \cdots E_k\,B) \\
&= \det(E_1) \cdots \det(E_k)\,\det(B) \\
&= \det(E_1 \cdots E_k)\,\det(B) \\
&= \det(A)\,\det(B).
\end{aligned}$$

□

Corollary 2.8.22

If A is an $n \times n$ invertible matrix, then $\det(A^{-1}) = \det(A)^{-1}$.

Proof. By Theorem 2.8.21, we obtain $\det(A)\,\det(A^{-1}) = \det(A\,A^{-1}) = \det(I_n) = 1$. Therefore, $\det(A^{-1}) = \det(A)^{-1}$. □

Exercise 2.8.23: Idempotency

*Let A be a square matrix such that $A^2 = A$ (such matrices are called **idempotent**).*
What are the possibilities for $\det A$*?*

Exercise 2.8.24: Nilpotency

*Let A be an $n \times n$ matrix such that $A^k = O_{n,n}$ for some integer $k > 0$ (such matrices are called **nilpotent**).*
What are the possibilities for $\det A$*?*

Exercise 2.8.25

Find an invertible matrix A, other than the identity, such that both A and A^{-1} have all integer entries. Can you find infinitely many?

Exercise 2.8.26

Show that it is not true, in general, that $\det(A+B) = \det A + \det B$. Find all pairs of 2×2 matrices such that $\det(A+B) = \det A + \det B$. (Note: for every $n \times n$ matrix A, there are infinitely many matrices B that work.)

2.8.3 Cofactors

In this section, we will give another way to compute the determinant of a matrix, called cofactor expansion.

Definition 2.8.27

*Let A be an $n \times n$ matrix. Let $A_{(i,j)}$ be the $(n-1) \times (n-1)$ matrix obtained from A by deleting its ith row and jth column. The (i,j)-**cofactor** of A is*

$$C_{(i,j)} = (-1)^{i+j} \det(A_{(i,j)}).$$

Example 2.8.28

The $(2,3)$-cofactor of $\begin{bmatrix} 2 & 0 & 1 \\ 1 & 0 & 1 \\ -1 & 1 & 0 \end{bmatrix}$ is

$$C_{(2,3)} = (-1)^{2+3} \det\left(\begin{bmatrix} 2 & 0 \\ -1 & 1 \end{bmatrix}\right) = -1\,(2) = -2.$$

Theorem 2.8.29: Cofactor expansion/Laplace expansion

If A is an $n \times n$ matrix and $1 \le i \le n$, then

$$\det(A) = C_{(i,1)}\,[A]_{i,1} + C_{(i,2)}\,[A]_{i,2} + \cdots + C_{(i,n)}\,[A]_{i,n}.$$

This is called the **cofactor expansion** or the **Laplace expansion** of A along the i^{th} row. Note that, by Theorem 2.8.11, we can also expand along a column of A.

We will not prove that this is equivalent to our previous definition of the determinant.

Example 2.8.30

Use cofactor expansion to compute the determinant of

$$A = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

Solution.

$$\begin{aligned} \det(A) &= 0 \det\left(\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}\right) - 1 \det\left(\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}\right) + 2 \det\left(\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}\right) \\ &= 0\,(-1) - 1\,(-1) + 2\,(0) \\ &= 1. \end{aligned}$$

Note that, in general, it is preferable to expand along a row or a column containing many zero entries, as this simplifies computations.

Exercise 2.8.31

We have already seen that

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = a\,d - b\,c.$$

Find a similar formula for

$$\det \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}.$$

2.8.4 The cross product in $\mathbb{R}^3$

We now consider a very special operation that is only valid in $\mathbb{R}^3$.

Theorem 2.8.32: Cross product

Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be vectors in $\mathbb{R}^3$. Then there is a unique vector $(\boldsymbol{u} \times \boldsymbol{v}) \in \mathbb{R}^3$ such that

$$(\boldsymbol{u} \times \boldsymbol{v}) \cdot \boldsymbol{w} = \det\left([\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{w}\,]\right)$$

for all $\boldsymbol{w} \in \mathbb{R}^3$. (Here, $[\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{w}\,]$ denotes the matrix with the three columns $\boldsymbol{u}$, $\boldsymbol{v}$, and $\boldsymbol{w}$.)

The vector $\boldsymbol{u} \times \boldsymbol{v}$ is called the **cross product** or the **vector product** of $\boldsymbol{u}$ and $\boldsymbol{v}$. The name “cross product” comes from the notation, whereas the name “vector product” comes from the fact that the output is a vector (as opposed to the scalar product).

Proof. Suppose there exists a vector $\boldsymbol{a} := \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}$ such that $\boldsymbol{a} \cdot \boldsymbol{w} = \det[\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}]$ for all $\boldsymbol{w} \in \mathbb{R}^3$. In particular, this should then hold for the three standard basis vectors $\{ \boldsymbol{e_1}, \boldsymbol{e_2}, \boldsymbol{e_3} \}$ for $\mathbb{R}^3$, that is:

$$\boldsymbol{a} \cdot \boldsymbol{e_1} = \det \begin{bmatrix} u_1 & v_1 & 1 \\ u_2 & v_2 & 0 \\ u_3 & v_3 & 0 \end{bmatrix}$$

$$\boldsymbol{a} \cdot \boldsymbol{e_2} = \det \begin{bmatrix} u_1 & v_1 & 0 \\ u_2 & v_2 & 1 \\ u_3 & v_3 & 0 \end{bmatrix}$$

$$\boldsymbol{a} \cdot \boldsymbol{e_3} = \det \begin{bmatrix} u_1 & v_1 & 0 \\ u_2 & v_2 & 0 \\ u_3 & v_3 & 1 \end{bmatrix};$$

now note that $\boldsymbol{a} \cdot \boldsymbol{e_1} = a_1$, $\boldsymbol{a} \cdot \boldsymbol{e_2} = a_2$, and $\boldsymbol{a} \cdot \boldsymbol{e_3} = a_3$. Furthermore, computing each of the determinants with Laplace expansion down the final column, we find

$$\boldsymbol{a} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} u_2\, v_3 - u_3\, v_2 \\ u_3\, v_1 - u_1\, v_3 \\ u_1\, v_2 - u_2\, v_1 \end{bmatrix}.$$

Thus, if a vector with the property stated exists, it must be of this vector $\boldsymbol{a}$. It remains to show that $\boldsymbol{a}$ has the property stated in the theorem. Let $\boldsymbol{w} = w_1\, \boldsymbol{e_1} + w_2\, \boldsymbol{e_2} + w_3\, \boldsymbol{e_3}$ be an arbitrary vector in $\mathbb{R}^3$. Then:

$$\begin{aligned} \boldsymbol{a} \cdot \boldsymbol{w} &= \boldsymbol{a} \cdot (w_1\, \boldsymbol{e_1} + w_2\, \boldsymbol{e_2} + w_3\, \boldsymbol{e_3}) \\ &= w_1\, (\boldsymbol{a} \cdot \boldsymbol{e_1}) + w_2\, (\boldsymbol{a} \cdot \boldsymbol{e_2}) + w_3\, (\boldsymbol{a} \cdot \boldsymbol{e_3}) \\ &= w_1\, \det[\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{e_1}] + w_2\, \det[\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{e_2}] + w_3\, \det[\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{e_3}] \\ &= \det[\boldsymbol{u} \mid \boldsymbol{v} \mid w_1\, \boldsymbol{e_1}] + \det[\boldsymbol{u} \mid \boldsymbol{v} \mid w_2\, \boldsymbol{e_2}] + \det[\boldsymbol{u} \mid \boldsymbol{v} \mid w_3\, \boldsymbol{e_3}] \\ &= \det[\boldsymbol{u} \mid \boldsymbol{v} \mid w_1\, \boldsymbol{e_1} + w_2\, \boldsymbol{e_2} + w_3\, \boldsymbol{e_3}] \\ &= \det[\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{w}], \end{aligned}$$

as expected. Thus the vector $\boldsymbol{a}$ satisfies the required properties and it is uniquely determined, which completes the proof. □

Remark 2.8.33: Generalisations to higher dimensions

The definition of the cross product in Theorem 2.8.32 generalises to $\mathbb{R}^n$ for n other than 3; indeed, one can define a 'cross product' of $n-1$ vectors $\boldsymbol{v_1}, \dots, \boldsymbol{v_{n-1}} \in \mathbb{R}^n$ to be a vector $\boldsymbol{a}$ such that $\boldsymbol{a} \cdot \boldsymbol{w} = \det[\boldsymbol{v_1}, \dots, \boldsymbol{v_{n-1}}, \boldsymbol{w}]$ for all $\boldsymbol{w} \in \mathbb{R}^n$. The properties of this generalisation (called the ***wedge product****) are far beyond the scope of this course, but appear very naturally when doing calculus and geometry in higher dimensions.*

The proof of Theorem 2.8.32 above suggests an informal "determinant-type" notation for the cross product, namely, we often write:

$$\boldsymbol{u} \times \boldsymbol{v} = \det\left(\begin{bmatrix} u_1 & v_1 & \boldsymbol{e_1} \\ u_2 & v_2 & \boldsymbol{e_2} \\ u_3 & v_3 & \boldsymbol{e_3} \end{bmatrix}\right) = \det\left(\begin{bmatrix} \boldsymbol{e_1} & \boldsymbol{e_2} & \boldsymbol{e_3} \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{bmatrix}\right).$$

Indeed, a cofactor expansion along the third column for the former and first line for the latter "determinant" gives

$$\begin{aligned} &\boldsymbol{u} \times \boldsymbol{v} \\ &= \boldsymbol{e_1} \det\left(\begin{bmatrix} u_2 & u_3 \\ v_2 & v_3 \end{bmatrix}\right) - \boldsymbol{e_2} \det\left(\begin{bmatrix} u_1 & u_3 \\ v_1 & v_3 \end{bmatrix}\right) + \boldsymbol{e_3} \det\left(\begin{bmatrix} u_1 & u_2 \\ v_1 & v_2 \end{bmatrix}\right), \end{aligned}$$

as in the proof above.

Example 2.8.34

Calculate the cross product between the vectors $\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$ *and* $\begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix}$.

Solution.
Using informal row expansion, the cross product is given by:

$$\begin{aligned} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix} &= \det\left(\begin{bmatrix} \boldsymbol{e_1} & \boldsymbol{e_2} & \boldsymbol{e_3} \\ 1 & 0 & 1 \\ 0 & 2 & 2 \end{bmatrix}\right) \\ &= \boldsymbol{e_1} \det\left(\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}\right) - \boldsymbol{e_2} \det\left(\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}\right) \\ &\quad + \boldsymbol{e_3} \det\left(\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\right) \\ &= \boldsymbol{e_1}\,(-1) - \boldsymbol{e_2}\,(2) + \boldsymbol{e_3}\,(2) = \begin{bmatrix} -1 \\ -2 \\ 2 \end{bmatrix}. \end{aligned}$$

Proposition 2.8.35: Properties of the cross product

For $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^3$ and $c \in \mathbb{R}$, we have:

1. $(c\,\boldsymbol{u}) \times \boldsymbol{v} = c\,(\boldsymbol{u} \times \boldsymbol{v}) = \boldsymbol{u} \times (c\,\boldsymbol{v})$;
2. $\boldsymbol{u} \times \boldsymbol{v} = -(\boldsymbol{v} \times \boldsymbol{u})$; *(Anticommutativity)*
3. $\boldsymbol{u} \times \boldsymbol{u} = \mathbf{0}$;
4. $\mathbf{0} \times \boldsymbol{u} = \boldsymbol{u} \times \mathbf{0} = \mathbf{0}$;
5. $\boldsymbol{u} \times (\boldsymbol{v} + \boldsymbol{w}) = \boldsymbol{u} \times \boldsymbol{v} + \boldsymbol{u} \times \boldsymbol{w}$. *(Distributivity)*

Proof. We only prove (1) and (2) and leave the others as exercises.

1. Observe that $(c\,\boldsymbol{u}) \times \boldsymbol{v}$ is the unique vector with the property $(c\,\boldsymbol{u} \times \boldsymbol{v}) \cdot \boldsymbol{w} = \det([\,c\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{w}\,])$ for all $\boldsymbol{w} \in \mathbb{R}^3$; by homogeneity of the determinant, we know that $\det([\,c\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{w}\,]) = c\det([\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{w}\,])$ and so $(c\,\boldsymbol{u}) \times \boldsymbol{v}$ is the unique vector with the property $(c\,\boldsymbol{u} \times \boldsymbol{v}) \cdot \boldsymbol{w} = c\det([\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{w}\,])$ for all $\boldsymbol{w} \in \mathbb{R}^3$. However, $\boldsymbol{u} \times \boldsymbol{v}$ is the unique vector with the property that $(\boldsymbol{u} \times \boldsymbol{v}) \cdot \boldsymbol{w} = \det([\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{w}\,])$ for all $\boldsymbol{w} \in \mathbb{R}^3$; by uniqueness, we must have that $(c\,\boldsymbol{u}) \times \boldsymbol{v} = c\,(\boldsymbol{u} \times \boldsymbol{v})$.
   The second equality in part (1) is similar.
2. Observe that $\boldsymbol{u} \times \boldsymbol{v}$ is the unique vector with the property $(\boldsymbol{u} \times \boldsymbol{v}) \cdot \boldsymbol{w} = \det([\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{w}\,])$ for all $\boldsymbol{w} \in \mathbb{R}^3$; by Lemma 2.8.8, $\det([\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{w}\,]) = -\det([\,\boldsymbol{v} \mid \boldsymbol{u} \mid \boldsymbol{w}\,])$; hence $\boldsymbol{u} \times \boldsymbol{v}$ is the unique vector with the property that $\boldsymbol{u} \times \boldsymbol{v} = -\det[\boldsymbol{v}, \boldsymbol{u}, \boldsymbol{w}]$ for all $\boldsymbol{w} \in \mathbb{R}^3$, which is exactly the defining property of $-(\boldsymbol{v} \times \boldsymbol{u})$.

□

Alternatively, one may prove the properties of Proposition 2.8.35 by expanding the sides of each equality out in terms of the vector components and checking equality componentwise.

Example 2.8.36

Verify that $\boldsymbol{e_1} \times \boldsymbol{e_2} = \boldsymbol{e_3}$ and $\boldsymbol{e_2} \times \boldsymbol{e_3} = \boldsymbol{e_1}$, while $\boldsymbol{e_1} \times \boldsymbol{e_3} = -\boldsymbol{e_2}$. Then

$$\boldsymbol{e_1} \times (\boldsymbol{e_1} \times \boldsymbol{e_2}) = \boldsymbol{e_1} \times \boldsymbol{e_3} = -\boldsymbol{e_2},$$

while

$$(\boldsymbol{e_1} \times \boldsymbol{e_1}) \times \boldsymbol{e_2} = \mathbf{0} \times \boldsymbol{e_2} = \mathbf{0}.$$

This example illustrates the following

Warning.
In general, $\boldsymbol{u} \times (\boldsymbol{v} \times \boldsymbol{w}) \neq (\boldsymbol{u} \times \boldsymbol{v}) \times \boldsymbol{w}$, that is, the cross product is *not* associative.

Exercise 2.8.37

Check that $\|\boldsymbol{u} \times \boldsymbol{v}\|^2 = \|\boldsymbol{u}\|^2 \|\boldsymbol{v}\|^2 - (\boldsymbol{u} \cdot \boldsymbol{v})^2$.

Theorem 2.8.38

If $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^3$*, then*

1. $\boldsymbol{u} \times \boldsymbol{v}$ *is perpendicular to both* $\boldsymbol{u}$ *and* $\boldsymbol{v}$*, and*
2. $\|\boldsymbol{u} \times \boldsymbol{v}\|$ *is the area of the parallelogram generated by* $\boldsymbol{u}$ *and* $\boldsymbol{v}$*.*

Proof.

1. Note that $(\boldsymbol{u} \times \boldsymbol{v}) \cdot \boldsymbol{u} = \det([\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{u}\,])$ by definition; since the first and third columns are both $\boldsymbol{u}$, the zeroness property of the determinant implies that $\det([\,\boldsymbol{u} \mid \boldsymbol{v} \mid \boldsymbol{u}\,]) = 0$. Similarly, $(\boldsymbol{u} \times \boldsymbol{v}) \cdot \boldsymbol{v} = 0$. (See Figure 2.15a.)
2. Consider the parallelogram with sides $\boldsymbol{u}$ and $\boldsymbol{v}$, as in Figure 2.15b. The area of P is $\|\boldsymbol{u}\|\, h = \|\boldsymbol{u}\|\, \|\boldsymbol{v}\|\, |\sin(\alpha)|$. Now,

$$\begin{aligned}
\|\boldsymbol{u}\|^2 \|\boldsymbol{v}\|^2 |\sin(\alpha)|^2 &= \|\boldsymbol{u}\|^2 \|\boldsymbol{v}\|^2 \sin^2(\alpha) \\
&= \|\boldsymbol{u}\|^2 \|\boldsymbol{v}\|^2 (1 - \cos^2(\alpha)) \\
&= \|\boldsymbol{u}\|^2 \|\boldsymbol{v}\|^2 \left(1 - \left(\frac{\boldsymbol{u} \cdot \boldsymbol{v}}{\|\boldsymbol{u}\|\, \|\boldsymbol{v}\|}\right)^2\right) \\
&= \|\boldsymbol{u}\|^2 \|\boldsymbol{v}\|^2 - (\boldsymbol{u} \cdot \boldsymbol{v})^2 \\
&= \|\boldsymbol{u} \times \boldsymbol{v}\|^2,
\end{aligned}$$

where the last equality comes from Exercise 2.8.37. Taking square roots on both sides, we find $\|\boldsymbol{u}\|\, \|\boldsymbol{v}\| |\sin(\alpha)| = \|\boldsymbol{u} \times \boldsymbol{v}\|$. □

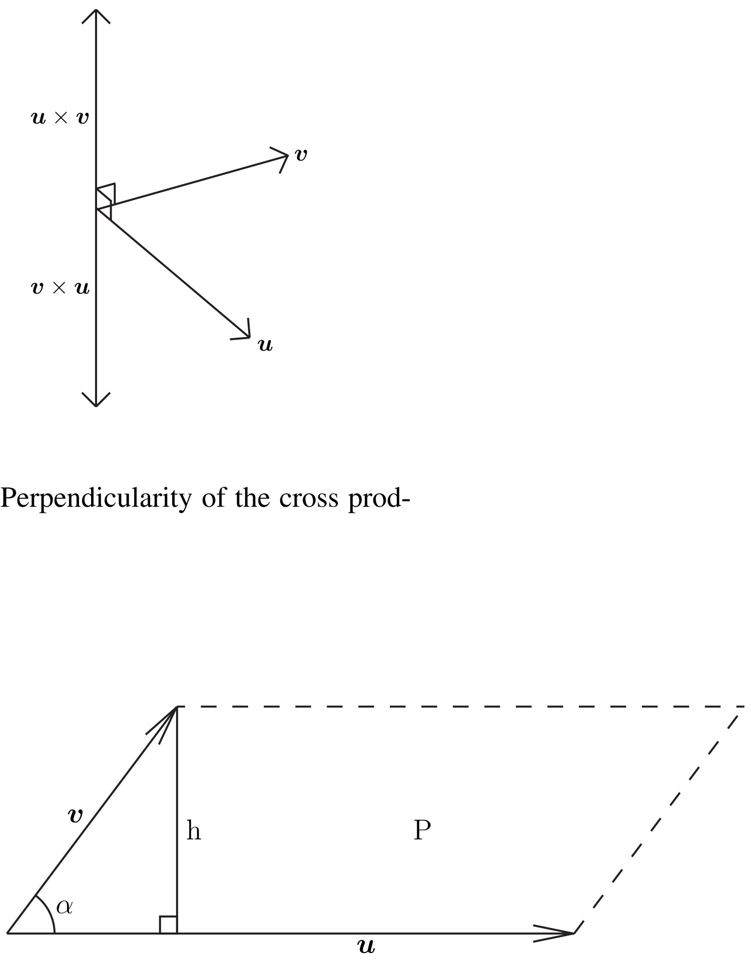
Example 2.8.39

Find a normal vector to the plane through $\begin{bmatrix}1\\1\\1\end{bmatrix}, \begin{bmatrix}1\\2\\3\end{bmatrix}$ *and* $\begin{bmatrix}3\\2\\1\end{bmatrix}$.

Solution.

A normal vector is perpendicular to every direction vector of this plane. Hence, we first find two linearly independent direction vectors:

$$\begin{bmatrix}1\\2\\3\end{bmatrix} - \begin{bmatrix}1\\1\\1\end{bmatrix} = \begin{bmatrix}0\\1\\2\end{bmatrix} \quad \text{and} \quad \begin{bmatrix}3\\2\\1\end{bmatrix} - \begin{bmatrix}1\\1\\1\end{bmatrix} = \begin{bmatrix}2\\1\\0\end{bmatrix}.$$


$\boldsymbol{u} \times \boldsymbol{v}$
$\boldsymbol{v}$
$\boldsymbol{v} \times \boldsymbol{u}$
$\boldsymbol{u}$
$\boldsymbol{v}$
h
P
α
$\boldsymbol{u}$

(a) Perpendicularity of the cross product.

(b) Parallelogram property of the cross product.

Figure 2.15: Geometric properties of the cross product.

We can now choose their cross product as a normal vector, because the cross product will be perpendicular to both of these direction vectors.

Hence, $\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} \times \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -2 \\ 4 \\ -2 \end{bmatrix}$ is a normal vector to the plane through $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ and $\begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}$.

Example 2.8.40

Find the area of the triangle with vertices

$$\boldsymbol{u} = \begin{bmatrix}1\\2\\1\end{bmatrix}, \boldsymbol{v} = \begin{bmatrix}2\\1\\2\end{bmatrix} \text{ and } \boldsymbol{w} = \begin{bmatrix}3\\3\\3\end{bmatrix}.$$

Solution.
The area of this triangle is half the area of the parallelogram generated by two sides of this triangle, say, those given by the vectors $\boldsymbol{v}-\boldsymbol{u}$ and $\boldsymbol{w}-\boldsymbol{u}$; see Figure 2.16. Since the area of the parallelogram is the length of the cross product between these two vectors, we have:

$$\begin{aligned} A &= \frac{1}{2}\|(\boldsymbol{v}-\boldsymbol{u})\times(\boldsymbol{w}-\boldsymbol{u})\| \\ &= \frac{1}{2}\left\|\begin{bmatrix}1\\-1\\1\end{bmatrix}\times\begin{bmatrix}2\\1\\2\end{bmatrix}\right\| \\ &= \frac{1}{2}\left\|\begin{bmatrix}-3\\0\\3\end{bmatrix}\right\| = \frac{1}{2}\sqrt{9+9} = \frac{3}{2}\sqrt{2}. \end{aligned}$$

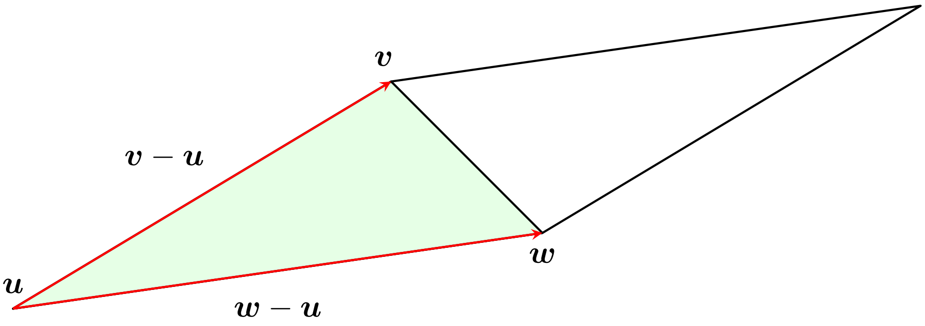

$\boldsymbol{v}$
$\boldsymbol{v}-\boldsymbol{u}$
$\boldsymbol{w}$
$\boldsymbol{u}$
$\boldsymbol{w}-\boldsymbol{u}$

Figure 2.16: The triangle of Example 2.8.40.

For the next two exercises, recall that the trace $\mathrm{tr}(A)$ of a matrix A is the sum of the diagonal entries of A; see Exercise 2.6.44.

Exercise 2.8.41

Let $\boldsymbol{a} \in \mathbb{R}^3$. Define a function $f : \mathbb{R}^3 \to \mathbb{R}^3$ by $f(\boldsymbol{v}) = \boldsymbol{v} \times \boldsymbol{a}$.

1. *Show that f is a linear transformation.*
2. *Find the matrix A associated with f (with respect to the standard basis).*
3. *Is f invertible?*
4. *What are $\det(A)$ and $\mathrm{tr}(A)$?*

Exercise 2.8.42

Repeat Exercise 2.8.41 for the function $g : \mathbb{R}^3 \to \mathbb{R}^3$ given by $g(\boldsymbol{v}) = \boldsymbol{a} \times \boldsymbol{v}$.
Are your results as expected?