CHAPTER 0

INTRODUCTION

In this chapter we introduce key concepts that will be used in later chapters. For this reason, unlike other chapters it contains many statements, sometimes given without thorough explanations or reasoning. While all of these statements are grounded in deep ideas and can be formulated in a rigorous manner, it is advised to first get an intuitive understanding of the ideas before diving into their more formal construction.

Note 0.1 In case you are already familiar with the topics

It is recommended for readers who are familiar with the topics to at least gloss over this chapter and make sure they know and understand all the concepts presented here.

0.1 MATHEMATICAL SYMBOLS AND SETS

0.1.1 Logical Statements and their Truth Value

We start our discussion with the simplest mathematical concept: a **proposition**. A proposition is simply a statement that might be either **true** or **false**.

Example 0.1 Truth of propositions

- $3 > 1$ (**true**)
- $-2 = 5 - 7$ (**true**)
- $7 < 5$ (**false**)
- The radius of the earth is bigger than that of the moon. (**true**)
- The word 'House' starts with the letter 'G'. (**false**)

We can group together propositions using **logical operators**. Two of the most common logical operators are **AND** and **OR**.

The **AND** operator returns a **true** statement only if **both** the statements it groups are themselves **true**, otherwise it returns **false**.

Example 0.2 The AND operator

- $2+4=6$ is **true**, $4-2=2$ is **true**. ($2+4=6$ **AND** $4-2=2$) is therefore **true**.
- $2+4=6$ is **true**, $2>6$ is **false**. ($2+4=6$ **AND** $2>6$) is therefore **false**.
- $\frac{10}{2}=1$ is **false**, $2^4=16$ is **true**. $\left(\frac{10}{2}=1\right.$ **AND** $\left.2^4=16\right)$ is therefore **false**.
- $7<5$ is **false**, $10+2=13$ is **false**. ($7<5$ **AND** $10+2=13$) is therefore **false**.

The **OR** operator returns **true** if **at least** one of the statements it groups is true.

Example 0.3 The OR operator

- $2+4=6$ is **true**, $4-2=2$ is **true**. ($2+4=6$ **OR** $4-2=2$) is therefore **true**.
- $2+4=6$ is **true**, $2>6$ is **false**. ($2+4=6$ **OR** $2>6$) is therefore **true**.
- $\frac{10}{2}=1$ is **false**, $2^4=16$ is **true**. $\left(\frac{10}{2}=1\right.$ **OR** $\left.2^4=16\right)$ is therefore **true**.
- $7<5$ is **false**, $10+2=13$ is **false**. ($7<5$ **OR** $10+2=13$) is therefore **false**.

The behaviour of both operators can be summarized using a **truth table** (see Table 0.1 below).

Table 0.1 The truth table for the operators **AND** and **OR**.

A	B	A AND B	A OR B
true	**true**	**true**	**true**
true	**false**	**false**	**true**
false	**true**	**false**	**true**
false	**false**	**false**	**false**

Table 0.2 Common Mathematical NotationsUsed in this Book.

Symbol	In words
$\neg a$	**not** a
$a \wedge b$	a **and** b
$a \vee b$	a **or** b
$a \Rightarrow b$	a **implies** b
$a \Leftrightarrow b$	a **is equivalent to** b
$\forall x$	**For all** x (...)
$\exists x$	**There exists** x **such that** (...)
$a := b$	a **is defined to be** b
$a \equiv b$	a **is equivalent to** b

When writing, it is convenient to use **notations** to represent operators: the **AND** operator is denoted by $\wedge$, while the **OR** operator is denoted by $\vee$.

Example 0.4 Using the notations for AND and OR

$$(\underset{\textbf{false}}{2+2=5}) \wedge (\underset{\textbf{true}}{1-1=0}) \Rightarrow \textbf{false}$$
$$(\underset{\textbf{false}}{2+2=5}) \vee (\underset{\textbf{true}}{1-1=0}) \Rightarrow \textbf{true}$$

0.1.2 Common mathematical notations

Several more common mathematical notations are given in Table 0.2.

The notation $\Rightarrow$ need a bit of clarification: implication means that we can directly derive a proposition from another proposition. For example, if $x = 3$ then $x > 2$. The opposite implication can be a **false** statemt, i.e. for the example above $x > 2$ does not imply $x = 3$ (denoted as $x > 2 \not\Rightarrow x = 3$). Sometimes implication is expressed by using the word *if*: in the above example $x > 2$ if $x = 3$, but the other way around is not **true**.

We say that two propositions are **equivalent** when they imply each other. For example: $x = 2$ implies that $\frac{x}{2} = 1$, while $\frac{x}{2} = 1$ implies that $x = 2$. We can write this as

$$\frac{x}{2} = 1 \Leftrightarrow x = 2.$$

Instead of the word *equivalent*, the phrase *if and only if* (sometimes shortened to **iff**) is commonly used, e.g.

$$x = 2 \text{ iff } \frac{x}{2} = 1.$$

0.1.3 Sets and subsets

The concept of **sets** is perhaps one of the most basic ideas in modern mathematics. Much of the material convered in this book will be built upon sets and their properties. However, as with the rest of the material presented here - our description of sets will not be thorough nor percise.

For our purposes, a set is a collection of **elements**. These elements can be any concept - be it physical (a chair, a bicycle, a tapir) or abstract (a number, an idea). However, we will consider only sets comprised of numbers. Sets can have finite of infinite number of elements in them.

We denote sets by using curly brackets, and if the number of elements in them is not too big - we display the elements, separated by commas, inside the brackets. In other cases we can express the sets as a sentence or a mathematical proposition.

Example 0.5 Simple sets

$$\{1,2,3,4\} \qquad \left\{-4, \frac{3}{7}, 0, \pi, 0.13, -2.5, \frac{e}{3}, 2^{-\pi}\right\} \qquad \{\text{all even numbers}\}$$

Sets have two important properties:

0.1. Elements in a set do not repeat. i.e each element is unique.

0.2. The order of elements in a set does not matter.

Example 0.6 Important set properties

Examples demonstrating the two afforementioned important properties of sets:

0.1. The following is not a proper set:

$$\{1,1,0,1,0,0,-1,0,0,-1,-1,1\}$$

0.2. The following sets are all identical:

$$\{1,2,3,4\} \qquad \{1,3,2,4\} \qquad \{3,4,1,2\} \qquad \{1,3,2,4\} \qquad \{4,3,2,1\}$$

Sets can be denoted using **conditions**, with the symbol | representing the phrase "such that".

Example 0.7 Defining a set using a condition

he following set contains all the odd whole numbers between 0 and 10, including both:

$$\{0 < x < 10 \mid x \text{ is an odd number}\}.$$

The definition of this set can be read as

all numbers x that are bigger than 0 and are smaller than 10, such that x is odd.

(note that the requirement of x to be an odd number means that it is neccessarily a whole number as well)

This set can be written explicitly as

$$\{1, 3, 5, 7, 9\}.$$

Sets are usually denoted with an uppercase latin letter ($A, B, C, \dots$), while their elements are denoted as lowercase letters ($a, b, \alpha, \phi, \dots$). When we want to denote that an element belongs to a set we use the following symbol: $\in$. Conversly, $\notin$ is used to denote that an element *does not* belong to a set.

Example 0.8 Elements in sets

For the two sets

$$A = \{1, 2, 5, 7\}, \quad B = \{\text{even numbers}\},$$

all the following propostions are **true**:

$$1 \in A, \quad 2 \in A, \quad 5 \in A, \quad 7 \in A,$$
$$2 \in B, \quad 1 \notin B, \quad 5 \notin B, \quad 7 \notin B.$$

The number of elements in a set, also called its **cardinality** is denoted using two vertical bars (similar to the way absolute values are denoted).

Example 0.9 Cardinality

For $S = \left\{-3, 0, -2, 7, 1, \frac{1}{2}, 5\right\}$, $|S| = 7$.

An important special set is the **empty set**, which is the set containing no elements. It is denoted by $\emptyset$, and has the unique property that $|\emptyset| = 0$.

0.1.4 Intersection, union, difference and complement sets

Two sets are equal if they both contain the exact same elements and only these elements, i.e.

$$A = B \iff x \in A \Leftrightarrow x \in B. \tag{0.1.1}$$

This proposition reads 'The sets A and B are equal *if and only if* any element x in A is also in B, and any element x in B is also in A'. When all the elements of a set B are also elements of another set A, we say that B is a **subset** of A, and we denote that as $B \subset A$. In mathematical notation, we write

$$B \subset A \Leftrightarrow \forall x \in B, x \in A. \tag{0.1.2}$$

i.e. B is a subset of A **iff** the following is true: any element in B is also an element in A.

Note 0.2 (not so) Surprising properties of subsets

The definion of a subset (Equation 0.1.2) gives rise to two interesting properties:

- The empty set $\emptyset$ is a subset of any set.
- Any set is a subset of itself.

Note 0.3 The uniqeness of $\emptyset$

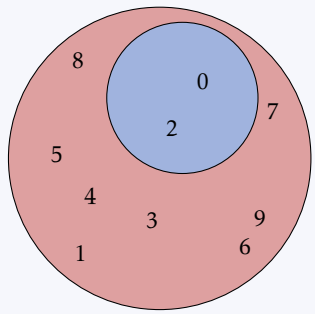
There is only a single empty set, as any set that has no elements is equivalent to any other set with no elements (i.e. they have the same elements). Due to the way subsets are defined, the empty set is a subset of any set (including itself!).

Of course, since we have a definition for a subset, the opposite concept also exists: if B is a subset of A, then we say that A is a **superset** of B.

A very useful way of illustrating the relationship beyween two or more sets is by using **Venn diagrams**, where sets are represented by circles (or other 2D shapes).

Example 0.10 Subsets and Venn diagrams

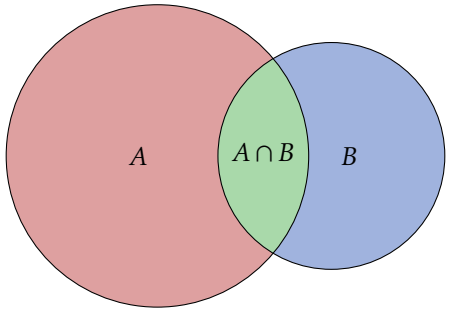
A Venn diagram depicting the set $B = \{0, 2\}$ as a subset of $A = \{0, 1, 2, 3, 4, \ldots, 9\}$:



If for two sets A, B both $A \subset B$ and $B \subset A$, then $A = B$. We can write this fact as a methematical proposition:

$$(A \subset B) \wedge (B \subset A) \Leftrightarrow A = B. \tag{0.1.3}$$

The **intersection** of two sets A and B, denoted $A \cup B$, is the set of all elements x such that



$x \in A$ **AND** $x \in B$:

$$A \cup B = \{x \mid x \in A \wedge x \in B\}. \tag{0.1.4}$$

Example 0.11 Intersection of sets

The intersection of the sets $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6\}$ is the set $A \cup B = \{3, 4\}$.
The intersection of the sets $C = \{0, 1, 2, 6, 7\}$ and $D = \{3, 9, -4, 5\}$ is the empty set $\emptyset$, since no element is in both sets.

The following Venn diagram depicts the intersection of two sets (the green area):

Note 0.4 Disjoint sets

When the intersection of two sets is the empty set, we say that the set is **disjoint**.

The **union** of two sets (denoted using the symbol $\cup$) is the set composed of all the elements that belong to any of the sets, including elements that are in both sets:

$$A \cup B = \{x \mid x \in A \vee x \in B\}. \tag{0.1.5}$$

Example 0.12 Union of sets

The union of the sets $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6\}$ is the set $A \cup B = \{1, 2, 3, 4, 5, 6\}$.
The union of the sets $C = \{0, 1, 2, 6, 7\}$ and $D = \{3, 9, -4, 5\}$ is the set $C \cup D = \{0, 1, 2, 3, -4, 5, 6, 7, 9\}$.

The following Venn diagram depicts the union of two sets (the purple area):

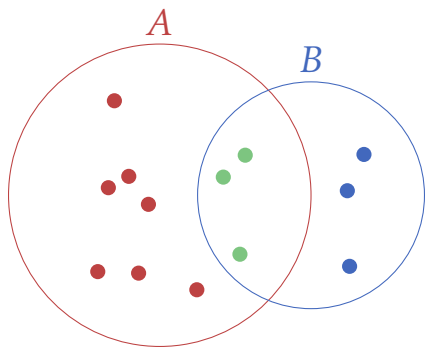
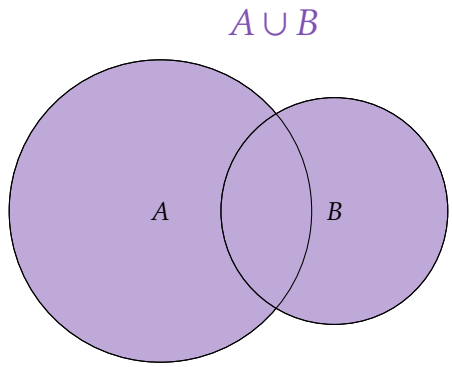


Figure 0.1 Counting the number of elements in the union of two sets: A has 10 elements (red + green dots), while B has 6 elements (blue + green dots). If we count both we get 16 elements, but this counts the joint elements (green dots) twice. Therefore we should subtract the number of joint points, and get that there are only 13 elements in the union.



Naively, the number of elements of a union $A \cup B$ is simply the sum of the number of elements in A and the number of elements in B. However, this naive approach might count the elements in both sets twice: once for A and once for B (see Figure 0.1) - this is exactly the set $A \cap B$. We therefore subtract the number of elements in $A \cap B$ and get

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{0.1.6}$$

When two sets A, B are disjoint, then $|A \cap B| = 0$, and so $|A \cup B| = |A| + |B|$.

The definitions of intersections and unions can be easily extended to any whole number of sets.

Example 0.13 Intersection and union of 3 sets

The intersection of 3 sets $A = \{1, 2, 3, 4, 5\}$, $B = \{-2, -1, 0, 1, 2\}$ and $C = \{2, 3, 4, 5, 6\}$ is the set of all elements that are in A and in B and in C, i.e. the set $A \cap B \cap C = \{2\}$. The union of these sets is the set of all elements that are in either of the sets, i.e. $A \cup B \cup C = \{-2, -1, 0, 1, 2, 3, 4, 5, 6\}$.

The most general definition of an intersection of n sets (where n is a whole number), which we will call $A_1, A_2, A_3, \cdots, A_n$ is

$$A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n = \{x \mid (x \in A_1) \wedge (x \in A_2) \wedge (x \in A_3) \wedge \cdots \wedge (x \in A_n)\}. \tag{0.1.7}$$

the left hand side of Equation 0.1.7 can be written as

$$A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i. \tag{0.1.8}$$

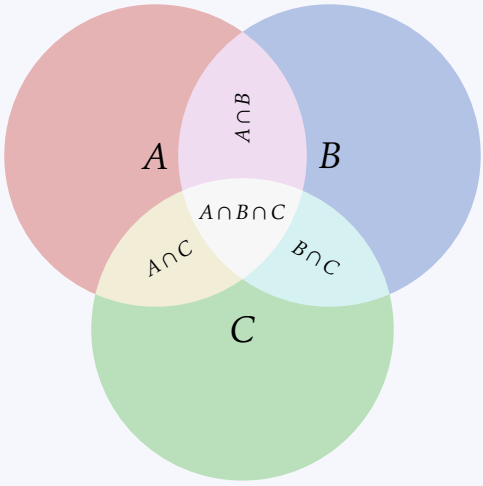
(clarifying the notation? i.e. indexing, etc.)

Similarily, the union of n different sets is defined as

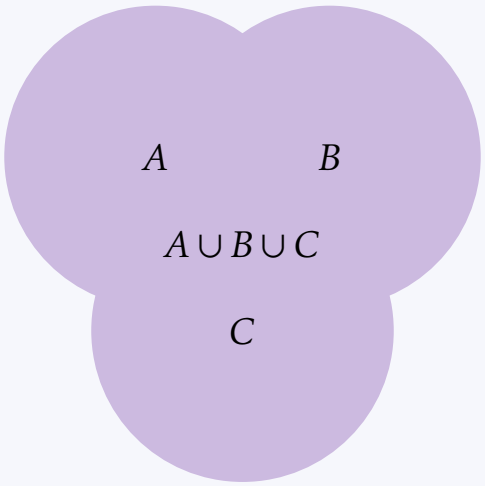
$$\begin{aligned} \bigcup_{i=1}^{n} A_i &= A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n \\ &= \{x \mid (x \in A_1) \vee (x \in A_2) \vee (x \in A_3) \vee \cdots \vee (x \in A_n)\}. \end{aligned} \tag{0.1.9}$$

Example 0.14 Venn diagrams: intersection and union of 3 sets

The following Venn diagram shows all possible intersections between three sets:



...and the following Venn diagram depicts the union of the same three sets:



The **difference** of two sets A and B (written $A - B$ or $A \setminus B$) is, in a sense, the opposite of their intersection: it is the set of all elements in A that are not in B. Note that $A - B$ doesn't necessarily equal $B - A$, i.e. it is not **commutative**.

Example 0.15 Difference of two sets

Given the two sets $A = \{1, 2, 3, 4, 5\}$ and $B = \{3, 4, 5, 6, 7, 8, 9\}$,

$$A - B = \{1, 2\},$$
$$B - A = \{6, 7, 8, 9\}.$$

(note how in this case $A - B \neq B - A$)

Given a set A and a subset of A, $B \subset A$, we can define the **complement** of B in relation to A (notation: $B^{\complement}$) as all the elements in A that are not in B. As the name suggest, the elements of $B^{\complement}$ complete B: $B \cup B^{\complement} = A$.

Example 0.16 Complement of a set

Given the set $A = \mathbb{Z}$ and $B = \{x \in \mathbb{Z} \mid x \text{ is odd}\}$, the complement $B^{\complement}$ in relation to A is the set of all even numbers. The reason is that any integer number can be either odd (in which case it belongs in B) or even (in which case it belongs in $B^{\complement}$).

Given a set A with $|A|$ elements - how many different subsets does it have? We'll start by looking at a practical example: $A = \{1, 2, 3\}$. We can immidetly see that any set which contains just one of the elements of A is a subset of A, i.e. $\{1\}, \{2\}, \{3\}$ are all subsets of A. In addition, any set which contains only two elements from A is a subset of A, i.e. $\{1, 2\}, \{1, 3\}, \{2, 3\}$. Of course, we must not forget the empty set and A itself - both subsets of A (see **??**). Thus altogether A has 8 subsets:

$$\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}.$$

Generaly, any set A with $|A|$ elements has $2^{|A|}$ different subsets. The set of all these subsets is called the **power set** of A, and is denoted as $P(A)$.

Example 0.17 Power set

The power set of $A = \{1, 2, 3\}$ is

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

0.1.5 Important number sets

It is now time to introduce some important number sets. We begin with the simplest of these sets: the **natural numbers**, denoted by $\mathbb{N}$. These are the numbers $1, 2, 3, 4, \ldots$. Adding the opposites to the natural numbers and adding 0 to the set yields the **integers**, denoted by $\mathbb{Z}$. Loosley speaking, we can define the integers as

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}. \tag{0.1.10}$$

This makes the integers a superset of the natural numbers, i.e.

$$\mathbb{N} \subset \mathbb{Z}. \tag{0.1.11}$$

One can think of the integers as all the number needed for solving an equation of the form $a + x = b$, where a and b are integers themselves, and x is an unknown. No matter which integer values we put in a and b, the unknown x will always be an integer as well (whether it be positive, negative or zero depends on the values of a and b). However, when one wishes to solve an equation fo the sort $ax = b$, the integers are not longer sufficient: for example, if $a = 2$ and $b = 1$, then x is not an integer.

To solve $ax = b$ (where $a, b \in \mathbb{Z}$) we must introduce the **rational numbers**: numbers with values that are ratios of two integers. We denote the set of rational numbers with the symbol $\mathbb{Q}$, and write

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z} \wedge b \neq 0 \right\}. \tag{0.1.12}$$

(TBW: discuss briefly why $b \neq 0$)

For some combinations of a and b the ratio $\frac{a}{b}$ is an integer. For example: $\frac{3}{1}$, $\frac{8}{4}$, $\frac{-2}{2}$. This makes the integers a subset of the rational numbers, i.e.

$$\mathbb{Z} \subset \mathbb{Q}. \tag{0.1.13}$$

About 2500 years ago it was discovered that some numbers are not rational (and thus also not integers). The most famous example is the number $\sqrt{2}$ - there are not two integers a, b such that $\frac{a}{b} = \sqrt{2}$. We call some of these numbers **algebraic numbers** (denoted by $\mathbb{A}$), and what makes them special is that they are solutions to **polynomial equations**, which we will not define yet (see section xxx). Instead, here is an example for a 2nd order polynomial equation (called a **quadratic equation**):

$$x^2 - 2x - 1 = 0. \tag{0.1.14}$$

Similar to what we saw before, the rational numbers are a subset of the algebraic numbers, i.e.

$$\mathbb{Q} \subset \mathbb{A}. \tag{0.1.15}$$

The algebraic numbers together with other non-rational numbers, such as π and e, form the set of **real numbers**, denoted as $\mathbb{R}$. The definition of real numbers is way beyond the scope of this book, but it is important to understand that the progression we used so far still holds, i.e.

$$\mathbb{A} \subset \mathbb{R}. \tag{0.1.16}$$

The final set of numbers we will touch upon here is the set of **complex numbers**, denoted $\mathbb{C}$, which we can define as

$$\mathbb{C} = \left\{ a + \mathrm{i}b \mid a, b \in \mathbb{R},\ \mathrm{i} = \sqrt{-1} \right\}. \tag{0.1.17}$$

When $b = 0$, Equation 0.1.17 becomes just a single real number - and so

$$\mathbb{R} \subset \mathbb{C}. \tag{0.1.18}$$

(Section 0.6 is dedicated to complex numbers)

Equations 0.1.11-0.1.18 can be merged together to the following single equation:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{A} \subset \mathbb{R} \subset \mathbb{C}. \tag{0.1.19}$$

There are more advanced constructions that generalize the complex numbers (i.e. create supersets of the complex number set). These include **quaternions** and **Clifford algebras**. However, as stated before, we will not consider them in this book.

0.1.6 Intervals on the real number line

An important concept that is easily defined over the set $\mathbb{R}$ is an **interval**. A **closed interval** $[a, b]$ is a subset of $\mathbb{R}$ which is defined as

$$[a, b] = \{ x \in \mathbb{R} \mid a \leq x \leq b \}. \tag{0.1.20}$$

An **open interval** (a, b) is a subset of $\mathbb{R}$ which is defined as

$$(a, b) = \{ x \in \mathbb{R} \mid a < x < b \}. \tag{0.1.21}$$

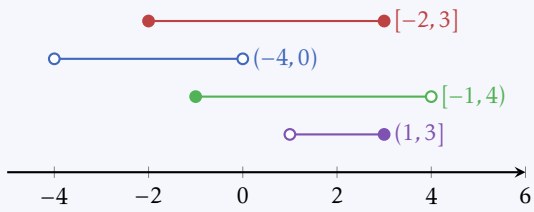
The difference between closed and open intervals is the inclusion and exclusion, respectively, of the edge point: in a closed interval the points a, b are included, while they are not included in an open interval. Of course, we can also create **half open intervals**, i.e.

$$\begin{aligned} [a, b) &= \{ x \in \mathbb{R} \mid a \leq x < b \}, \\ (a, b] &= \{ x \in \mathbb{R} \mid a < x \leq b \}, \end{aligned} \tag{0.1.22}$$

where the first interval includes a but not b, and the second interval includes b but not a.

Example 0.18 Intervals

Intervals can be drawn as colored line segments on top of the real number line:



Note how a full point denotes a closed edge, while an empty point denotes an open edge.

In some cases, it is necessary to use intervals that are infinite in one side, i.e. the left or the right edge are at infinity. In these cases, we use the symbol ∞ to denote infinity, and always keep the interval open at that end:

$$\begin{aligned}(-\infty, b) &= \{x \mid x < b\},\\ (-\infty, b] &= \{x \mid x \le b\},\\ (a, \infty) &= \{x \mid x > a\},\\ [a, \infty) &= \{x \mid x \ge a\}.\end{aligned} \tag{0.1.23}$$

0.1.7 Cartesian Products

The **Cartesian product** of two sets A, B (denoted $A \times B$) is the set of all possible **ordered** pairs, where the first component is an element of A and the second component is an element of B:

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}. \tag{0.1.24}$$

Example 0.19 Cartesian products

Consider $A = \{1, 2, 3\}$, $B = \{x, y\}$. Then

$$A \times B = \{(1, x),\ (1, y),\ (2, x),\ (2, y),\ (3, x),\ (3, y)\}$$

The concept of 'ordered pairs' is paramount: if we reverse the order of the elements in a pair the result might not be in the Cartesian product. We therefore say that the Cartesian product is **not commutative**.

Example 0.20 Non-commutivity of the Cartesian product

The elements $(x, 1)$, $(y, 1)$, $(x, 2)$ and so on **are not** in the Cartesian product $A \times B$ as defined in the previous example, since in each one of the pairs the first element is from B and the second element is from A.

The number of elements in a Cartesian product is the product of the number of elements in each of the sets it is composed of, i.e.

$$|A \times B| = |A| \cdot |B|. \tag{0.1.25}$$

Example 0.21 Number of elements in a Cartesian product

The Cartesian product described in the previous two examples has in total $3 \cdot 2 = 6$ elements, as seen in **??**.

As with intersections and unions, the definition of a Cartesian product can be expanded into any natural number of sets:

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) \mid x_1 \in A_1,\ x_2 \in A_2,\ \ldots, x_n \in A_n\}. \tag{0.1.26}$$

Example 0.22 Cartesian product of three sets

The Cartesian product of the sets $A = \{1, 2, 3\},\ B = \{x, y\},\ C = \{\alpha, \beta\}$ is

$$\begin{aligned} A \times B \times C = \{&(1, x, \alpha),\ (1, x, \beta),\ (1, y, \alpha),\ (1, y, \beta) \\ &(2, x, \alpha),\ (2, x, \beta),\ (2, y, \alpha),\ (2, y, \beta) \\ &(3, x, \alpha),\ (3, x, \beta),\ (3, y, \alpha),\ (3, y, \beta)\}. \end{aligned}$$

A special case of Cartesian products are those products for which all the sets composing them are the same set. We denote these as the respective integer power, for example the Cartesian product $\mathbb{R} \times \mathbb{R}$ is denoted as $\mathbb{R}^2$, the Cartesian product $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ is denoted as $\mathbb{R}^3$, etc.

Specifically, the Cartesian product $\mathbb{R}^2$ can be interpreted as the two-dimensional **Euclidean space**, which is the space used to draw graphs in one-dimensional calculus and shapes in two-dimensional analytican geometry. We will explore this idea (and higher dimensional spaces) in more details in upcoming chapters.

0.2 RELATIONS AND FUNCTIONS

0.2.1 Basics

The Cartesian product of two sets can be viewed as describing all possible connections between the elements of the first set to the elements of the second set, and thus any subset of a Cartesian product forms a specific **relation** between the sets.

Example 0.23 Relations as subsets of Cartesian products

Given the following two sets:

$$A = \{1, 2, 3, 4\},\ B = \{\alpha, \beta, \gamma\},$$

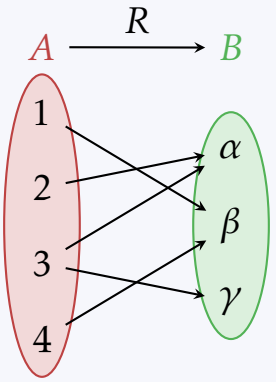
then

$$\begin{aligned} A \times B = \{&(1,\alpha),\ (1,\beta),\ (1,\gamma),\\ &(2,\alpha),\ (2,\beta),\ (2,\gamma),\\ &(3,\alpha),\ (3,\beta),\ (3,\gamma),\\ &(4,\alpha),\ (4,\beta),\ (4,\gamma)\}. \end{aligned}$$

We can choose the following pairs to form a subset of $A \times B$:

$$R = \{(1,\beta),\ (2,\alpha),\ (3,\alpha),\ (3,\beta), (4,\gamma)\}.$$

R is thus a relation between A and B. We can graphically illustrate R as follows:



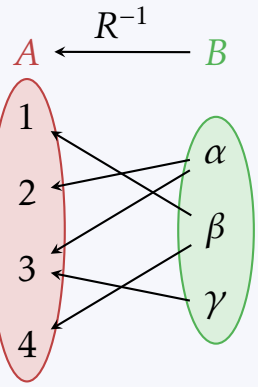
Relations can be inversed by reversing the order of each of its pairs.

Example 0.24 Inverse relation

The inverse relation to the relation in 0.23 is

$$R^{-1} = \{(\beta,1),\ (\alpha,2),\ (\alpha,3),\ (\beta,3), (\gamma,4)\}.$$

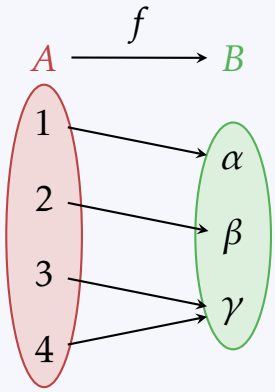
Graphically:

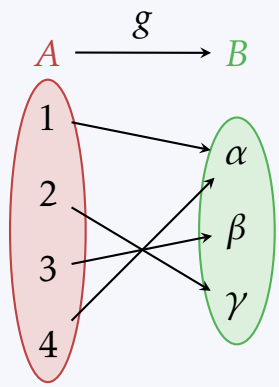


A **function** f from a set A to a set B is a relation for which any element in A is connected to a single element in B.

Example 0.25 Functions

The following are two functions from the set A to the set B defined in 0.23:





The pairs making up f are $(1,\alpha)$, $(2,\beta)$, $(3,\gamma)$ and $(4,\gamma)$, and the pairs making up g are $(1,\alpha)$, $(2,\gamma)$, $(3,\beta)$ and $(4,\alpha)$.

Note 0.5 Relations which are not functions

Note that the relation in 0.23 is **not** a function, since the element $3 \in A$ is connected to more than one element in B, namely α and γ.

Different names are used in some branches of mathematics to describe functions, such as **maps** and **transformations**. Barring context, they all mean the same thing.

A common way to denote that a function f is connecting elements in A to elements in B is

$$f : A \to B. \tag{0.2.1}$$

A is called the **domain** of f, and B its **image**. In this book and many other sources, the following notation is used: $f(x) = y$, which means that when we apply the function f to an element $x \in A$, the result is the element it is connected to, i.e. $y \in B$. We write this as $x \mapsto y$ (the special symbol $\mapsto$ is called a **mapping notation**).

Example 0.26 Value $\mapsto$ value notation for functions

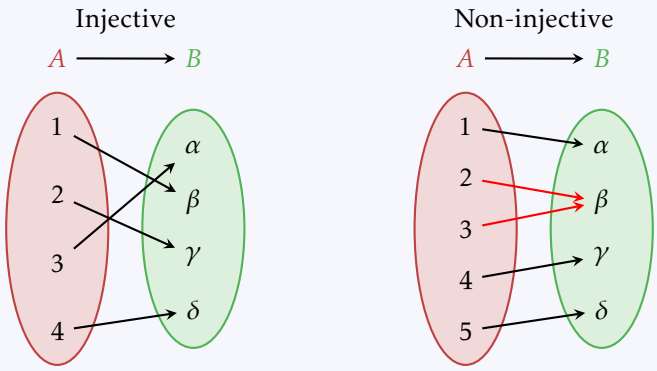
For the functions f, g as defined in 0.25:

$$f(1) = \alpha,\ f(2) = \beta,\ f(3) = f(4) = \gamma.$$
$$g(1) = g(4) = \alpha,\ g(2) = \gamma,\ g(3) = \beta.$$

0.2.2 Injective, surjective and bijective functions

A function is **injective** if each of the elements in its **image** is connected to by at most a single element in its **domain**. An injective function is also known as an **injection**.

Example 0.27 Injective function



The function on the right in non-injective because the element $\beta \in B$ is connected to by two elements in A (2 and 3, red arrows).

A function is **surjective** if every element in its image is connected to by at least a single element in its domain (see 0.28). As with injective functions, a surjective function is also known as a **surjection**. A non surjective function can be made into surjective function by excluding from its image any element that is not connected to by any element from its domain (see 0.29).

A function $f : A \to B$ that is both surjective and bijective is called a **bijective function** (also a **bijection**). All elements in the image of a bijection are connected to by exactly a single element in its domain. This means that the direction of the connections can be flipped, yielding the **inverse** of the original function (denoted f^{-1}).

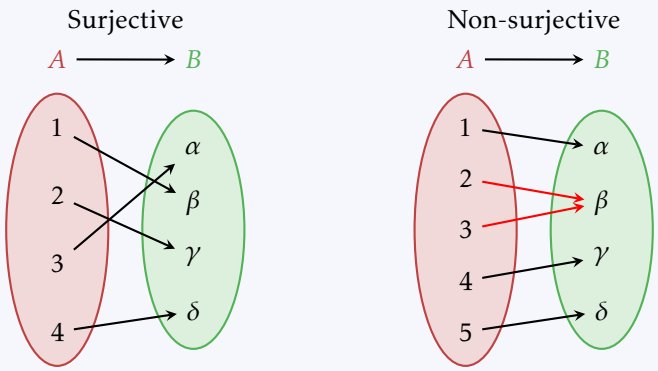
The reason only bijective functions have inverses is as follows: Given a function $f : A \to B$,

- if f is non-injective, then there is at least one element $y_1 \in B$ which is connected to by at least two elements from A. We can name these elements x_1 and x_2. When inverted, $f^{-1} : B \to A$ has an element $y_1 \in B$ (note that for f^{-1}, B is its domain), which is connected to two or more elements in A, the image of f^{-1}. These are of course x_1, x_2. This fact disqualifies f^{-1} from being a function.

- If f is non-surgetive, then there exists at least one element $y_2 \in B$ that is not connected to by any element from A. When inverted, y_2 in the domain B of f^{-1} is not connected to any element in its image A. This fact disqualifies f^{-1} from being a function.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Example 0.28 Surjective function



Example 0.29 Making a non-surjective function into a surjection

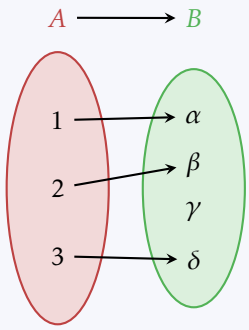
Given the two sets $A = \{1, 2, 3, 4\}$ and $B = \{\alpha, \beta, \gamma, \delta\}$, the following non-surjective function $f : A \to B$ is defined:

$$f = \{(1, \alpha),\ (2, \beta),\ (3, \gamma),\ (4, \gamma)\}.$$

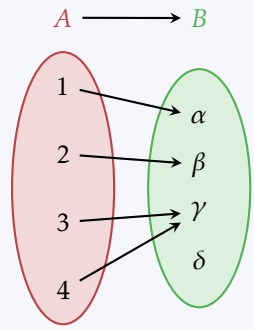
By removing δ from B, the function f becomes surjective (though it remains non-injective).

Example 0.30 Cross examples

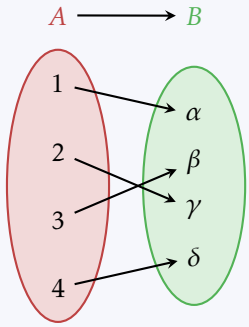
Injective, non surjective



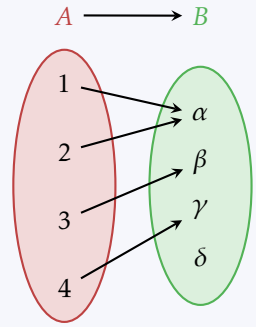
Injective, non surjective



Injective and surjective



Neither injective nor surjective



Note 0.6 Other names for bijections

Bijections are also called **one-to-one correspondences** and **invertible functions**.

0.2.3 Real functions

In suitable cases, a function is defined via a general mapping rule. This should be very familiar to anyone who learned mathematics in highschool, where many times functions are defined this way, e.g.

$$f(x) = x^2 + 3x - 4. \tag{0.2.2}$$

In mapping notation we can write Equation 0.2.2 as $f : x \mapsto x^2 + 3x - 4$. In highschool mathematics, both the domain and image of such functions is $\mathbb{R}$, although it is almost never specified explicitly. Such functions are commonly referred to as **real functions**, a convention used in this book as well.

Example 0.31 Functions defined using a mapping rule

The following are real functions:

$$f_1(x) = 2x^2 - 5, \quad f_2(x) = \sin\left(\frac{x}{3}\right), \quad f_3(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{\sigma^2}}.$$

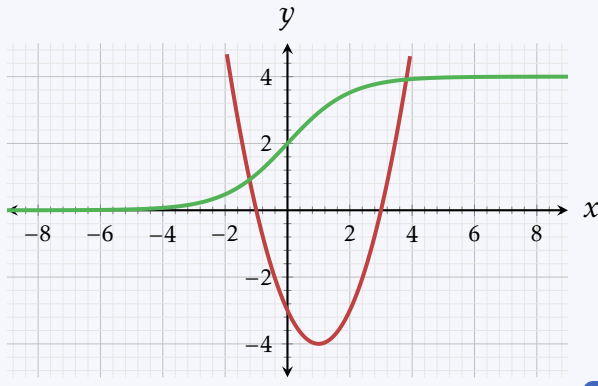
Note that these functions can also be defined using different sets, for example $f_1 : \mathbb{N} \to \mathbb{Z}$, $f_2 : \mathbb{N} \to [-1, 1]$, etc.

Real functions can be easily plotted in a **Cartesian coordinate system** by drawing all the points $(x, f(x))$ (i.e. all the points (x, y), where $x, y \in \mathbb{R}$ and $x \mapsto y$). We call these points the **graph** of f over $\mathbb{R}$.

Example 0.32 Graphs of real functions

The following two functions are plotted on the domain $[-9, 9]$:

- $f(x) = x^2 - 2x - 3$,
- $g(x) = 4e^x/(e^x + 1)$.

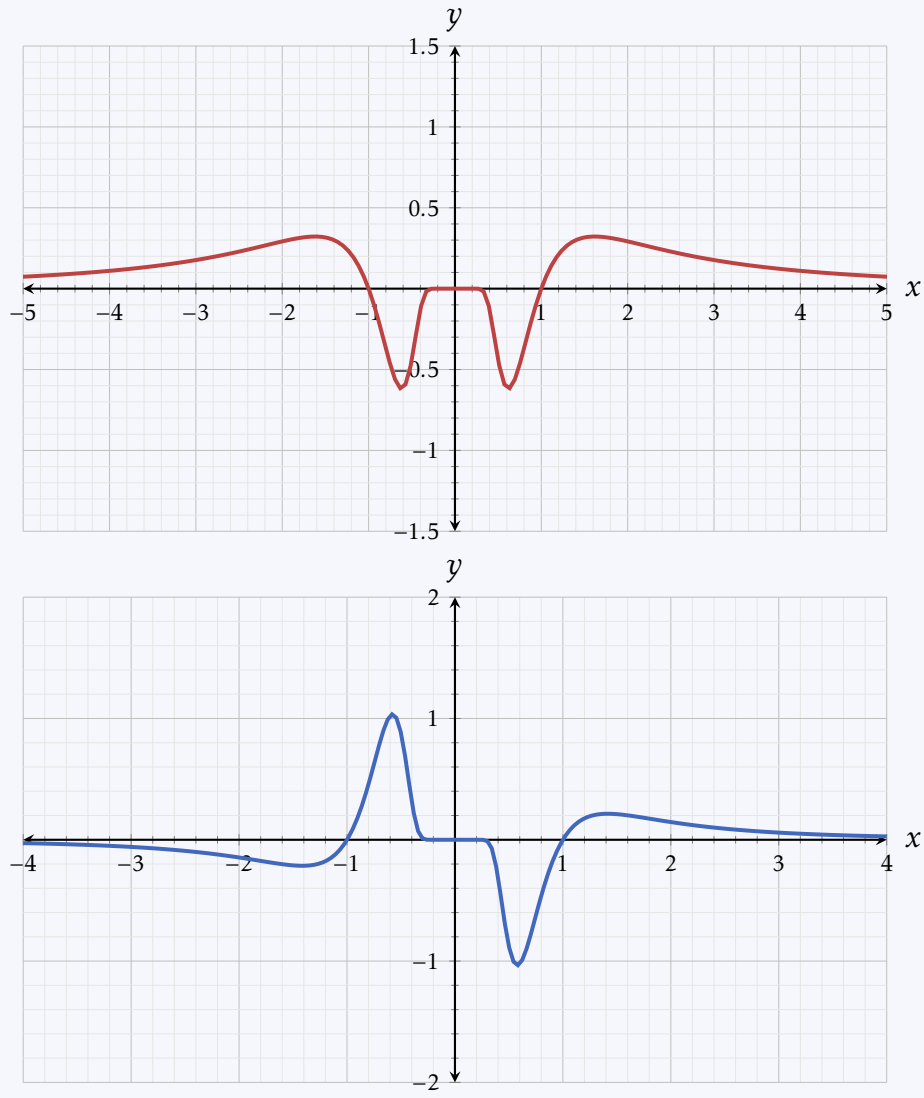


In 0.32, the function $g(x)$ always increases in value from left to right. Let's give this notion a more formal tone: a function f is said to be **increasing** on an interval I if for any $x_1, x_2 \in I$, if $x_2 > x_1$ then $f(x_2) > f(x_1)$. We can similarily define the idea of **decreasing** on an interval.

A property of some functions which is visually easy to depict is symmetry. A real function f is said to be **symmetric** if for any $x \in \mathbb{R}$, $f(-x) = f(x)$. This essentially means that the y-axis mirrors the function's plot. If for any $x \in \mathbb{R}$, $f(-x) = -f(x)$, we say that the function is **anti-symmetric**. A function can be neither, but there's only a single function which is both: the zero function, i.e. $f(x) = 0$.

Example 0.33 Symmetric and anti-symmetric functions

In the following graphs, the function on the top is symmetric, while the function on the bottom is anti-symmetric:



(injections/surjections of real functions?)

A real function is said to be **periodic** if it repeats its values exactly over and over with increasing x. In more precise terms we define a real function f to be periodic if for any integer value k,

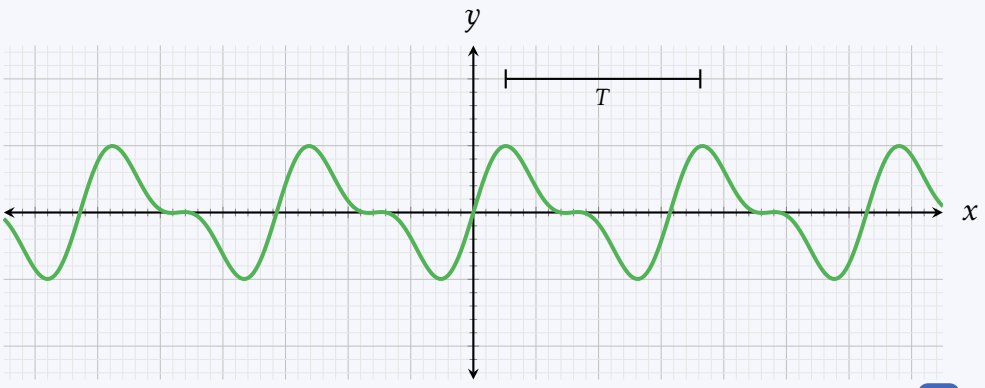
$$f(x+kT) = f(x). \tag{0.2.3}$$

where $T = [a,b]$ is a finite interval of $\mathbb{R}$ which we call the **period** of the function.

Example 0.34 A periodic function

The following graph depicts a periodic function f, with its period T shown. Notice that for any x $f(x+T) = f(x)$, i.e. you can move the period measure left and

right along the x-axis and the values of $f(x)$ in both its edges would always be the equal.



Two additional measures that arise from a period T are the **frequency** $f = \frac{1}{T}$, and the **angular frequency** $\omega = 2\pi f = \frac{2\pi}{T}$. We will use these measures later in the book.

Note 0.7 Units of period and frequency

In a periodic function such as the one in the above example, the units for the period are the same one used for the horizontal axis, while the units of both frequency and angular frequency are both 1 over the unit used for the horizontal axis/period. For example, if the unit of the horizontal axis is that of seconds, then the frequency units are 1/seconds, i.e. Hertz (SI symbol: Hz).

0.2.4 Composition of functions

Functions can be **composed** together, generating new functions. Given two functions $f : A \to B$ and $g : B \to C$, their composition is denoted as $f \circ g$. For the composition to be well defined, the **image** of f must be the same as the **domain** of g, and the resulting composition would have A as its domain and C as its image, i.e. $f \circ g : A \to C$.

Example 0.35 Composition of functions

Consider the functions

$$f(x) = x^2, \quad g(x) = \sin(x).$$

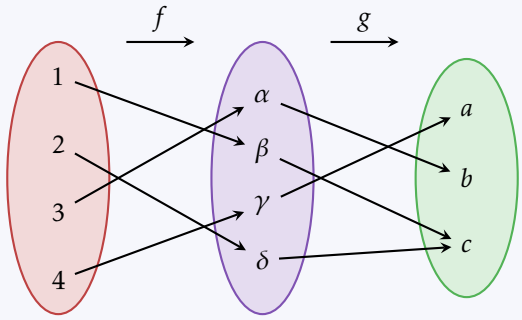
Using these functions, the two possible compositions are

- $f \circ g = f(g(x)) = [\sin(x)]^2$, and
- $g \circ f = g(f(x)) = \sin\left(x^2\right)$.

Example 0.36 Graphical representation of function composition

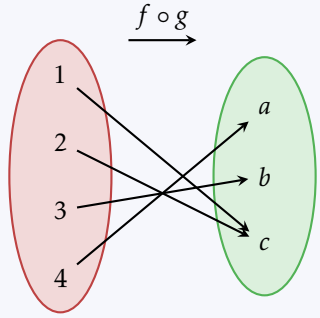
A graphical representation of composing two functions:

$$f : \{1,2,3,4\} \to \{\alpha,\beta,\gamma,\delta\}, \quad g : \{\alpha,\beta,\gamma,\delta\} \to \{a,b,c\}.$$



The composition results in the following function

$$f \circ g : \{1,2,3,4\} \to \{a,b,c,\}.$$



0.3 POLYNOMIAL FUNCTIONS

A very useful family of real functions can be derived using only three fundamental operations: addition, multiplication and exponentiation: the (real) **polynomial functions**. These are functions of the form

$$P_n(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n, \tag{0.3.1}$$

where $a_0, a_1, \ldots, a_n$ are real numbers called the **coefficients** of the polynomial function. Note that $a_n \neq 0$, i.e. the **degree** of the polynomial function is the index of the highest non-zero coefficient (and thus the highest power in the expression). We also call this the **order** of the polynomial function.

Example 0.37 Polynomial

The following is a polynomial function of degree $n = 6$:

$$P(x) = 4 + 2x - 3x^2 + 7x^4 - x^5 + 3x^6.$$

Breaking down this polynomial to its constituent terms:

$$\begin{array}{lcccccc} P(x) = & 4 & +2x & -3x^2 & +7x^4 & -x^5 & +3x^6 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & a_0 = 4 & a_1 = 2 & a_2 = -3 & a_4 = 7 & a_5 = -1 & a_6 = 3 \end{array}$$

Note that a_3 is missing from the polynomial function (i.e. there is no x^3 term). This means that $a_3 = 0$.

A shorthand way to write the general form of a polynomial function is by using the **summation notation**:

$$P(x) = \sum_{k=0}^{n} a_k x^k. \tag{0.3.2}$$

This notation, called the **Capital-sigma notation**, essentially represents addition of n elements (in the case shown here), each with its own **index of summation**, in this case i. The most general form of the summation notation is

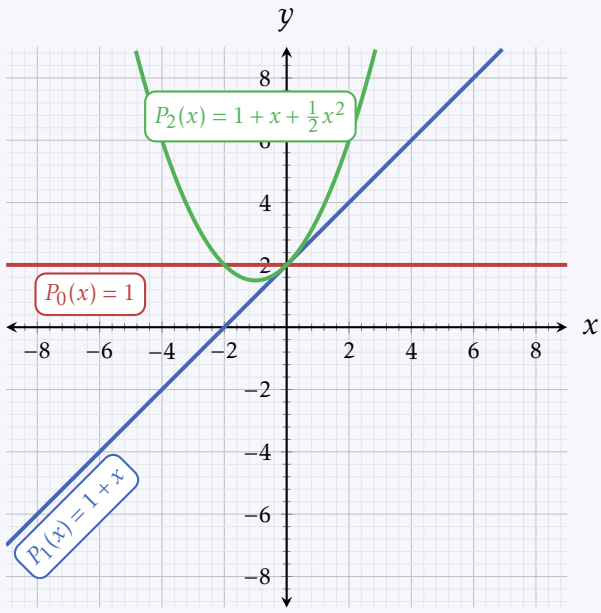
$$\sum_{i=k}^{n} a_i = a_k + a_{k+1} + a_{k+2} + \cdots + a_{n-1} + a_n, \tag{0.3.3}$$

i.e. the notation tells us to add those elements a_i for which $k \geq i \geq n$. Note that in the case of Equation 0.3.2, when $k = 0$, $x^k = x^0 = 1$ and the first term of the polynomial function has no x power (i.e. it is simply a_0), and when $k = 1$, $x^k = x^1 = x$ and thus the second term is $a_1 x$. We will encounter the summation notation in more details later in the book.

In the special case $n = 0$, i.e. when $P(x) = a_0$, the function is constant. When $n = 1$ the function $P(x) = a_0 + a_1 x$ is a line, and when $n = 2$, $P(x) = a_0 + a_1 x + a_2 x^2$ is a quadratic function.

Example 0.38 Polynomial functions for $n = 0, 1, 2$

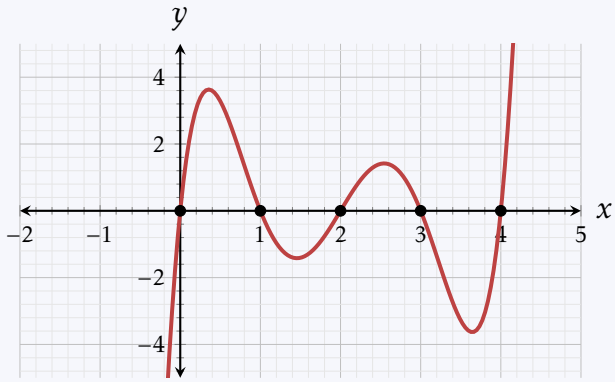
The following graphs represent the polynomial functions of degrees $n = 0, 1, 2$ with coefficients $a_0 = 2$, $a_1 = 1$, $a_2 = \frac{1}{2}$:



The values $x \in \mathbb{R}$ for which $P(x) = 0$ are called the **roots** (also: **zeros**) of the polynomial function.

Example 0.39 Roots of a polynomial function

The polynomial function $P(x) = 24x - 50x^2 + 35x^3 - 10x^4 + x^5$ has the following 5 roots: $x_0 = 0$, $x_1 = 1$, $x_2 = 2$, $x_3 = 3$, $x_4 = 4$. In the following graph of $P(x)$ the roots are shown as black dots.



The maximum number of **real** roots of a polynomial function with degree $n \geq 1$ is n, e.g. a polynomial of degree $n = 4$ has at most 4 real roots. This statement is a consequence of a very important theorem called **the fundamental theorem of algebra**, which due to its importance we will mention here without proof:

Theorem 0.1 The fundamental theorem of algebra

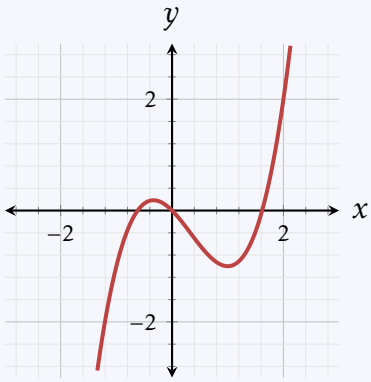
For any $n \geq 1$, the polynomial function $P(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n$, where $a_0, a_1, a_2, \ldots, a_n$ are all **complex numbers** and $a_n \neq 0$, has n complex roots.

Given a polynomial function $P(x)$ with n roots r_1, r_2, $\cdots$, r_n, the function can be written as a product of terms of the form $x - r_i$ (up to a constant), e.g. the polynomial function of degree $n = 3$ with roots $-1, 1, 2$ can be written as

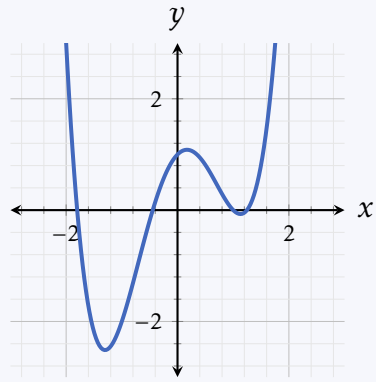
$$P(x) = (x+1)(x-1)(x-2) = x^3 - 2x^2 - x + 2. \tag{0.3.4}$$

Example 0.40 Higher order polynomial functions

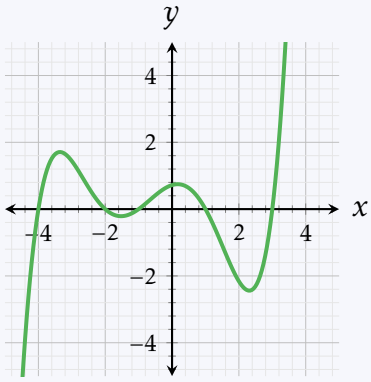
The following are the graphs of high-order polynomial functions ($n = 3, 4, 5, 6$):



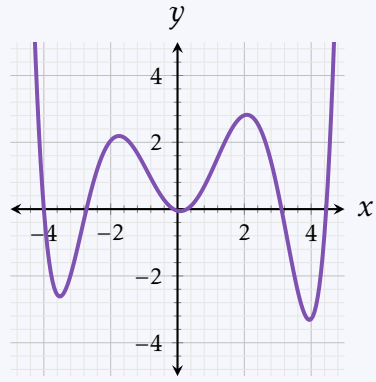
$x^3 - x^2 - x$



$x^4 - 3x^2 + x + 1$



$\frac{3}{100}\left(x^5 + 3x^4 - 11x^3 - 27x^2 + 10x + 24\right)$



$\frac{1}{100}\left(x^6 - x^5 - 26x^4 + 15x^3 + 150x^2 - 25x - 5\right)$

As can be seen in **??**, the maximal number of 'bends' in a polynomial function of order n is $n - 1$ (i.e. one less than the order of the function).

We will continue to explore polynomial functions in more details in future chapters.

0.4 EXPONENTIAL AND LOGARITHMIC FUNCTIONS

In the previous section we dealt with functions composed of integer powers of x. We will now shortly focus on functions where x is in the power itself and their inverse functions.

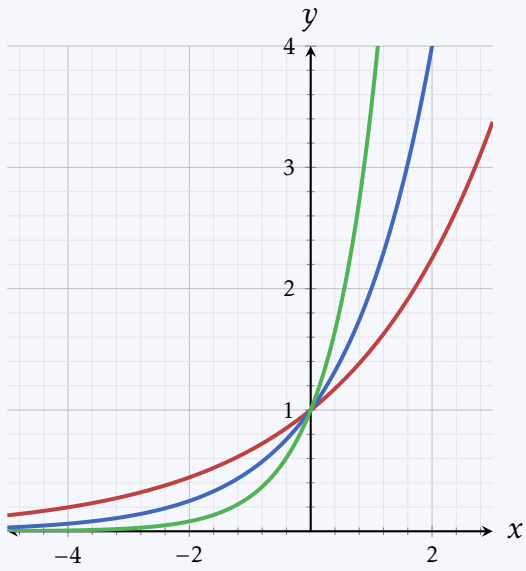
An **exponential function**, or simply an **exponential**, is a real function of the type

$$f(x) = b^x, \tag{0.4.1}$$

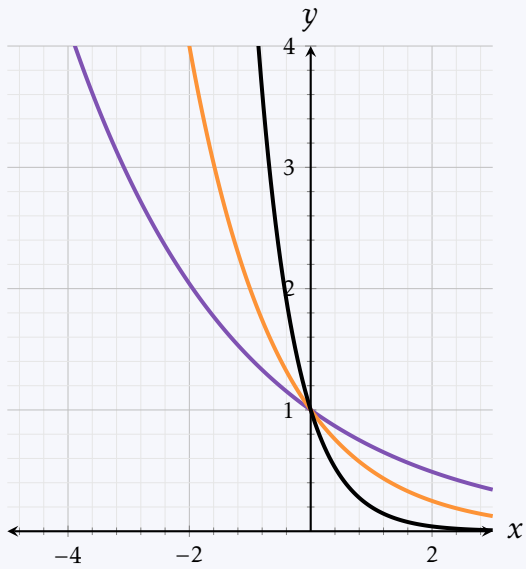
where $b > 0$ is called the **base** of the exponentiation, and x the exponential. All exponents, regardless of base, are always positive. In addition, all exponents pass through the point $(0,1)$ since $b^0 = 1$ for any real positive number, and through the point $(1,b)$ since $b^1 = b$. When $b > 1$ the function is increasing on $\mathbb{R}$, while for $b < 1$ the function is descending on $\mathbb{R}$.

Example 0.41 Exponential functions

The following are graphs of the exponential functions 1.5^x, 2^x and 3.5^x:



And the following are graphs of the exponential functions 0.7^x, 0.5^x and $\mathbf{0.2^x}$:



As a reminder, the following are two well known properties of exponents: given a base $b > 0$,

$$b^{-x} = \frac{1}{b^x}, \tag{0.4.2}$$

$$b^x b^y = b^{x+y}. \tag{0.4.3}$$

A special base for exponential functions is the real, non-algebraic number e. This number has many names, among them is **Euler's number**, but in the constant of exponentials it is known as the **natural base**. Its exact value is not entirely important for the moment: it is about 2.718, and in any case it is not possible to write it as there it has infinitely many digits after the period. It is very common across different fields of mathematics and science to write $\exp(x)$ instead of e^x.

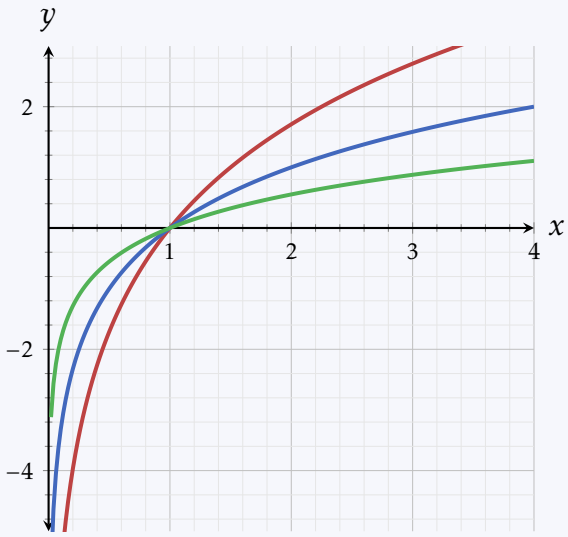
The inverse function to exponentials are the **logarithmic functions** (or simply **logarithms**), i.e. for any real $b > 0$, $b \neq 1$,

$$\log_b(b^x) = b^{\log_b(x)} = x. \tag{0.4.4}$$

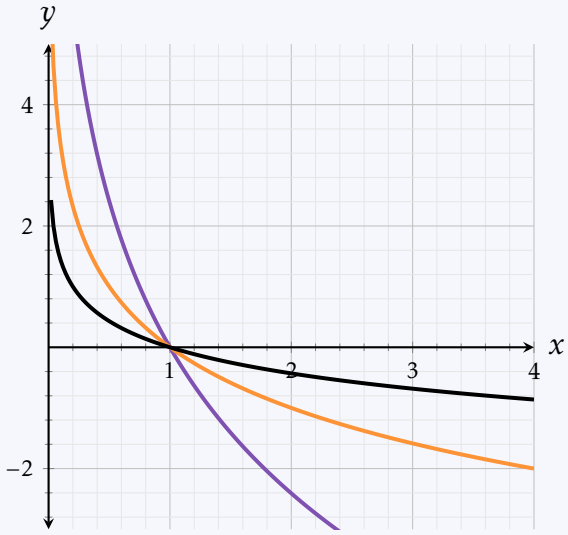
In essence, the logarithm in base b of a number x answers the question *"what is the number a for which $b^a = x$?"*. Being the inverses of exponential functions, all logarithms go through the point $(1, 0)$, and each also passes through its own point $(b, 1)$.

Example 0.42 Logarighmic functions

The following are graphs of the logarithmic functions $\log_{1.5}(x)$, $\log_2(x)$ and $\log_{3.5}(x)$:



...and the following are graphs of the exponential functions $\log_{0.75}(x)$, $\log_{0.5}(x)$ and $\log_{0.2}(x)$:



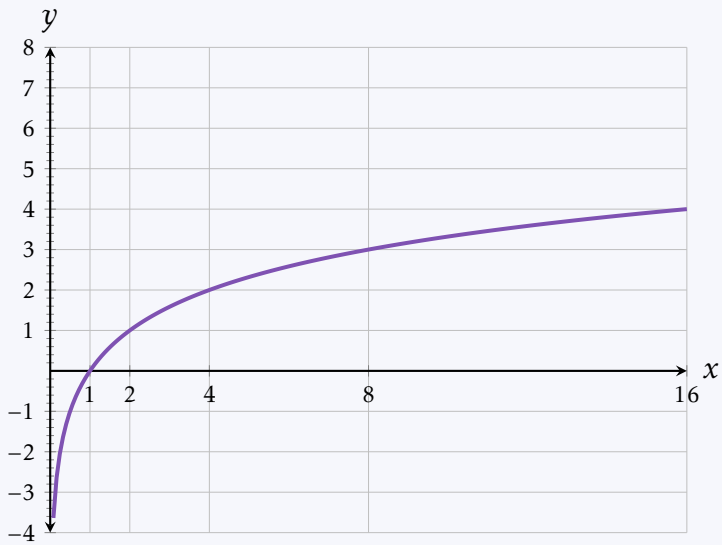
A useful property of logarithms is that they can help reduce ranges spanning several orders of magnitude to numbers humans can deal with. The easiest way to see this is using $b = 10$: $10^1 = 10$, and so $\log_{10}(10) = 1$. $10^2 = 100$, and so $\log_{10}(100) = 2$. $10^3 = 1000$, and so $\log_{10}(1000) = 3$, etc. The value of the logarithm goes by 1 for each raise in order of magnitude of its argument.

Therefore, if we have some measurement x which can hold values spanning several orders of magnitude (say $x \in [3, 1500000000]$), then it can sometimes be useful to use instead the logarithmic value of x (which in our case would span the range $\log_{10}(x) \in$

[0.477, 9.176]). This is done in many fields of science, for example some definitions of entropy[1], acid dissociation constants[2], pH[3] and more.

Example 0.43 Logarithms as evaluating orders of magnitude

In the following graph of $\log_2(x)$, each increase by power of two in x (i.e. $x = 1, 2, 4, 8, 16, \ldots$) yields only a single increase in y (i.e. $y = 0, 1, 2, 3, 4, \ldots$). This shows how logarithms shift our perspective from absolute values to orders of magnitude.



Using the definition of the logarithmic function $\log_b(x)$ (Equation 0.4.4) and the product rule for exponentials (Equation 0.4.3), a similar rule can be derived for logarithms. Let $x, y > 0$ and $b > 0,\ b \neq 1$ all be real numbers. We define

$$\log_b(x) = M,\ \log_b(y) = N, \tag{0.4.5}$$

which means

$$b^M = x,\ b^N = y. \tag{0.4.6}$$

From Equation 0.4.3 we know that

$$xy = b^M b^N = b^{M+N}, \tag{0.4.7}$$

and by re-applying the definition of logarithmic functions we get that

$$\log_b(xy) = M + N = \log_b(x) + \log_b(y). \tag{0.4.8}$$

Simlilarily to Equation 0.4.8, division yields subtraction:

$$\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y). \tag{0.4.9}$$

[1] $S = k_B \log(\Omega)$
[2] $pK_a = -\log(K_{diss})$
[3] $pH = -\log([H^+])$

Equations 0.4.8 and 0.4.9 reveal another valuable property of logarithms: they reduce multiplication to addition (and subsequently division to subtraction). While today this property doesn't seem very impressive, in pre-computers days it helped carrying on complicated calculations, using tables of pre-calculated logarithms (called simply **logarithm tables**) - a sight rarely seen today.

Taking one step forward in regards to reduction of operations, logarithms reduce powers to multiplication:

$$\log_b\left(x^k\right) = k\log_b(x). \tag{0.4.10}$$

for any $k \in \mathbb{R}$.

(TBW: proving this will be in the chapter questions to the reader)

Any logarithm $\log_b(x)$ can be expressed using another base, i.e. $\log_a(x)$ (where $a > 0$, $a \neq 1$) using the following formula:

$$\log_a(x) = \log_b(x) \cdot \log_a(b). \tag{0.4.11}$$

(TBW: proving this too will be a question to the reader)

Example 0.44 Changing logarithm base

Expressing $\log_4(x)$ in terms of $\log_2(x)$:

$$\log_4(x) = \log_2(x) \cdot \underbrace{\log_4(2)}_{=\frac{1}{2}} = \frac{1}{2}\log_2(x).$$

Much like with exponentials, the number e plays an important role when it comes to logarithms, for reasons that are discussed in the calculus chapter (ref). For now, we will just mention that $\log_e(x)$ gets a special notation: $\ln(x)$, which stands for **natural logarithm**. This notation is mainly used in applied mathematics and science, while in pure mathematics the notation is simply $\log(x)$, i.e. without mentioning the base [4].

For reason we will see in the calculus chapter, it is relatively simple to calculate both the exponential and logarithm in base e. Therefore, many operations in modern computations are actually done using these functions, for example calculating logarithms in other bases:

$$\log_b(x) = \frac{\ln(x)}{\ln(b)}. \tag{0.4.12}$$

Another operation commonly using both e^x and $\ln(x)$ is raising a real number a to a real power b: using the properties of both exponential and logarithmic functions, any such power can be expressed as

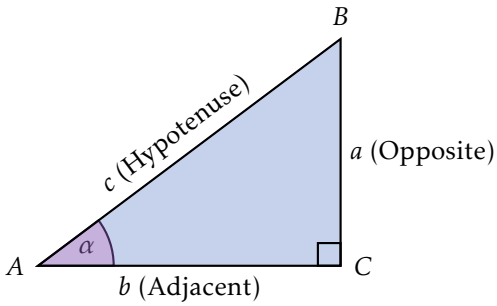
$$a^b = e^{b\ln(a)}. \tag{0.4.13}$$

[4] Depending on convention and context, this notation can refer to logarithm in any other base, most commonly $\log_{10}(x)$ and $\log_2(x)$.

0.5 TRIGONOMETRIC FUNCTIONS

0.5.1 Basic Definitions

Consider a **right triangle** $\triangle ABC$ with sides a, b, and Hypotenuse c, where the angle $\angle ACB$ is 90°, and the angle $\angle BAC$ is denoted as α:



We use the ratios between the three sides of the triangle to define three functions of α:

- The **sine** of the angle α is $\sin(\alpha) = \frac{a}{c}$,
- the **cosine** of the angle α is $\cos(\alpha) = \frac{b}{c}$, and
- the **tangent** of the angle α is $\tan(\alpha) = \frac{a}{b}$, which in turn is equal to $\frac{\sin(\alpha)}{\cos(\alpha)}$.

We can rearrange the above definitions:

$$\begin{aligned} a &= c\sin(\alpha), \\ b &= c\cos(\alpha). \end{aligned} \tag{0.5.1}$$

Normally, the Hypotenuse is the longest side of a right triangle. We will consider here the two edge cases where one of the sides a or b is equal to the Hypotenuse (and the other side is thus 0):

- if $a = c$ then $\alpha = 90°$,
- if $b = c$ then $\alpha = 0°$.

The possible length of a is therefore in the range $0 \le a \le c$, which means that $0 \le \frac{a}{c} \le 1$. Since $\sin(\alpha) = \frac{a}{c}$ this means that the image of $\sin(\alpha)$ is $[0, 1]$. The same idea is also true for b, and therefore $[0, 1]$ is the image of $\cos(\alpha)$ as well.

As a reminder, the **Pythagorean theorem**[5] states that for a right triangle with sides a, b and c,

$$a^2 + b^2 = c^2. \tag{0.5.2}$$

By substituting **Equation** 0.5.1 into the Pythagorean theorem we get

$$\begin{aligned} c^2 &= a^2 + b^2 \\ &= [c\sin(\alpha)]^2 + [c\cos(\alpha)]^2 \\ &= c^2\sin^2(\alpha) + c^2\cos^2(\alpha) \\ &= c^2\left[\sin^2(\alpha) + \cos^2(\alpha)\right], \end{aligned}$$

and therefore

$$\sin^2(x) + \cos^2(x) = 1. \tag{0.5.3}$$

0.5.2 The Unit Circle

We defined $\sin(\alpha)$ and $\cos(\alpha)$ so far in way such that their domains are both $[0°, 90°]$, and their images are both $[0, 1]$. However, there is a simple way to extend these functions such that both their domains are $\mathbb{R}$, and both their images are $[-1, 1]$: by using a **unit circle**.

Figure 0.4 depicts a unit circle: it is simply a circle of radius $R = 1$, which is placed such that its center lies at the origin of a 2-dimensional axis system (i.e. at the point $\boldsymbol{O} = (0, 0)$. We then draw a line from $\boldsymbol{O}$ to a point $\boldsymbol{P} = (x, y)$ on the circumference of the unit circle. We call the angle between the line $\boldsymbol{OP}$ and the x-axis θ. We then draw another line, this time from the point $\boldsymbol{P}$ to a point $\boldsymbol{D}$ on the x-axis, such that $\boldsymbol{PD}$ is perpendicular to the x-axis.

The triangle $\triangle OPD$ is a right triangle. Therefore, we can use the trigonometic functions to calculate the coordinates of the point $\boldsymbol{P} = (x, y)$:

$$\begin{aligned} x &= R\cos(\theta) = \cos(\theta), \\ y &= R\sin(\theta) = \sin(\theta). \end{aligned} \tag{0.5.4}$$

We then define $\cos(\theta)$ and $\sin(\theta)$ as a function of θ:

$$\begin{aligned} \sin(\theta) &= y, \\ \cos(\theta) &= x. \end{aligned} \tag{0.5.5}$$

Using this definition, the angle θ can take any value between 0° and 360°. In fact, the values of θ can be extended to any real number in degrees: any real value of degrees is equivalent to some value in the range $[0°, 360°]$, the first and most obvious example is that 360° is equivalent to 0°. Similarly, $-30° \equiv 330°$, $-180° \equiv 180°$, $-90° \equiv 270°$, etc (see Figure 0.3). In fact, this property makes the trigonometric functions periodic, with a period $T = 360°$.

[5] It's worth mentioning that no three positive integers a, b, and c satisfy the equation $a^n + b^n = c^n$ for any integer value of $n > 2$. This can be proven, however the proof is too large to fit in the footnotes.

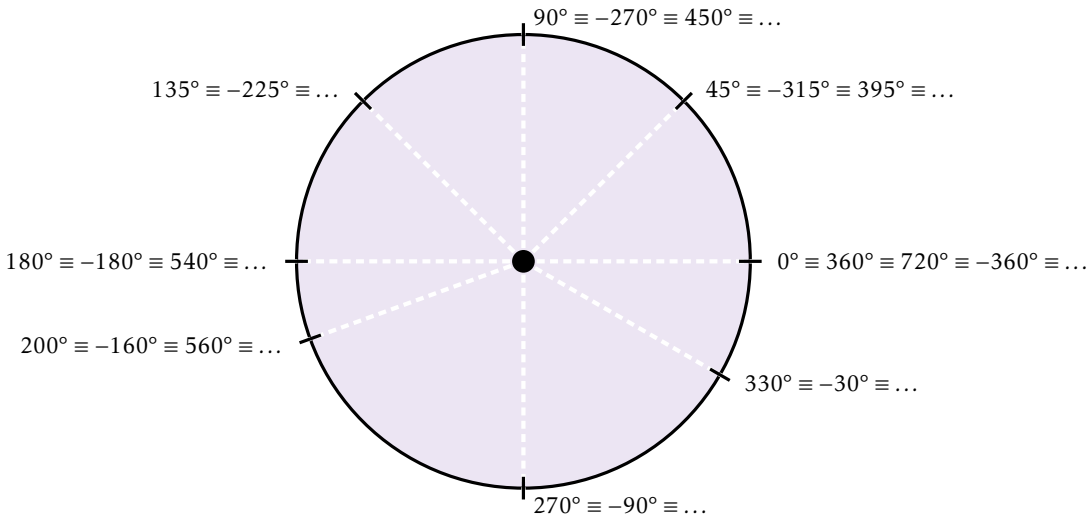


Figure 0.3 Angles equivalency on a circle.

Table 0.3 Common angles in radians, and their respective images for the three main trigonometic functions.

θ		$\sin(\theta)$	$\cos(\theta)$	$\tan(\theta)$
degrees	radians			
0°	0	0	1	0
30°	$\frac{\pi}{6}$	$\frac{1}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{\sqrt{3}}$
45°	$\frac{\pi}{4}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{2}}{2}$	1
60°	$\frac{\pi}{3}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}$	$\sqrt{3}$
90°	$\frac{\pi}{2}$	1	0	undefined
180°	π	0	−1	0
270°	$\frac{3\pi}{2}$	−1	0	undefined
360°	2π	0	1	0

0.5.3 Radians

Using degrees to measure angles in a sphere creates an inconvinience: the domain and image of the trigonometric functions have different units. In order to measure both these magnitudes using the same unit we switch to measuring angles on a circle using **radians** instead of degrees. One radian equals the length of a single radius R of the circle (in the case of the unit circle this is always $R = 1$). We define an inner angle θ to equal one radian if the arc length it represents is equal to R (see Figure 0.5).

How much is a radian in degrees? The full circumference of any circle with radius R equals $2\pi R$, which means that a single radian R is equivalent to $\frac{180°}{\pi} \approx 57.3°$. Table 0.3 shows some common angles and their equivalent value in radians.

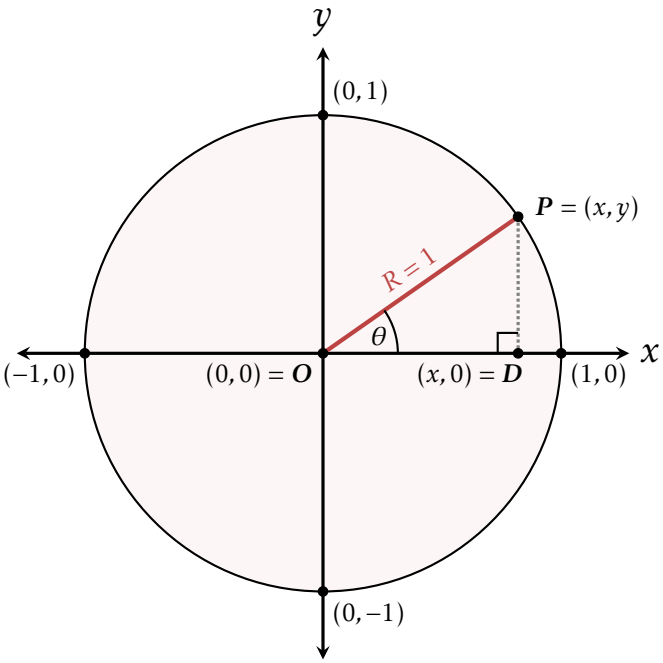


Figure 0.4 A unit circle with a point $\boldsymbol{P} = (x, y)$ on its circumference. The triangle $\triangle \boldsymbol{OPD}$ is a right triangle with sides $\boldsymbol{OD} = x$, $\boldsymbol{OP} = y$ and an angle θ opposing the side $\boldsymbol{DP}$.

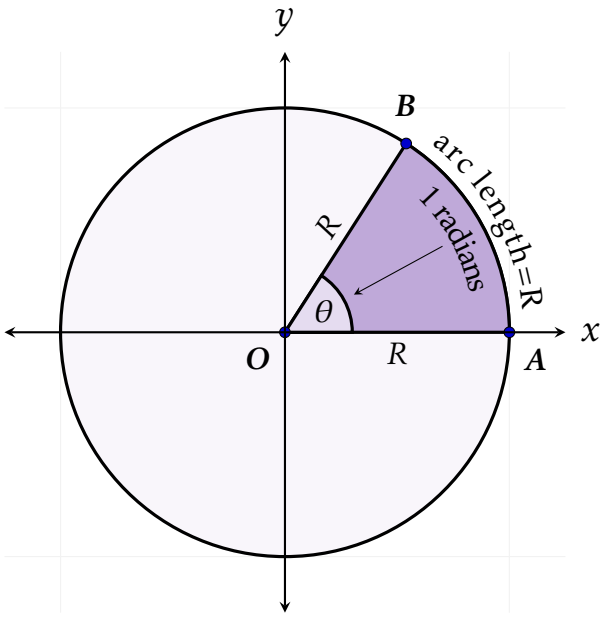


Figure 0.5 In this figure the arc $\boldsymbol{AB}$ has the same length of the radii $\boldsymbol{OA}$ and $\boldsymbol{OB}$ (all are equal to R), and therefore $\theta = 1$ radians.

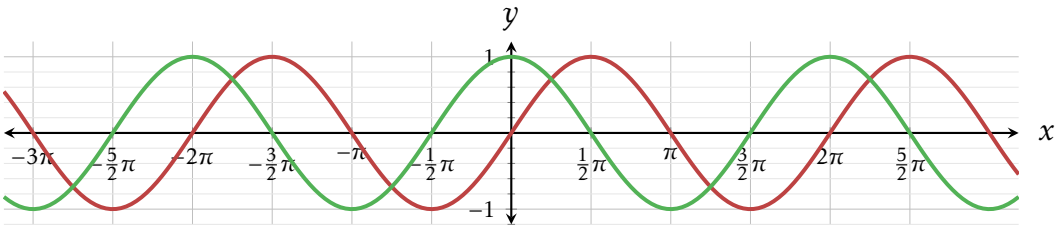


Figure 0.6 The graphs of $\sin(x)$ and $\cos(x)$ for $x \in [-10, 10]$. Note how the graph of $\cos(x)$ is "lagging" behind the graph of $\sin(x)$ by $\pi/2$.

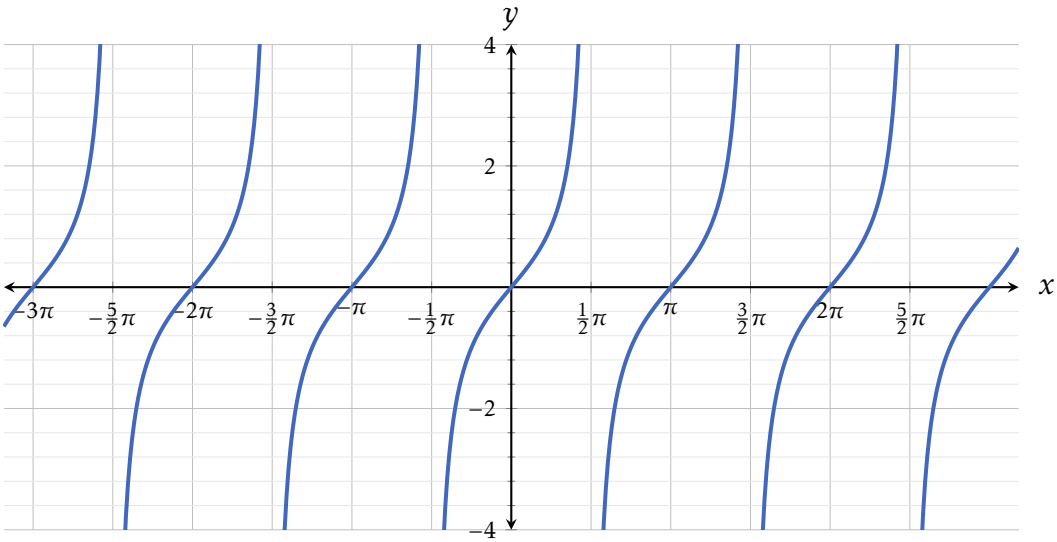


Figure 0.7 The graphs of $\tan(x)$ on the domain $[-3\pi, 3\pi]$.

0.5.4 Graphs

As seen previosuly, the functions $\sin(x)$ and $\cos(x)$ are periodic, having both the period $T = 2\pi$. Their graphs are depicted in Figure 0.7. The value of $\sin(x)$ is always equal to that of $\cos\left(x - \frac{\pi}{2}\right)$: we say that the two functions have a **phase difference** of $\pi/2$. The graph of $\tan(x)$ is depicted in Figure 0.6.

0.5.5 Identities

The following are some useful facts and connections between trigonometic functions:

- Pythagorean identity:

$$\sin^2(\theta) + \cos^2(\theta) = 1 \tag{0.5.6}$$

- Symmetry/Antisymmetry:

$$\sin(-\theta) = -\sin(\theta). \tag{0.5.7}$$
$$\cos(-\theta) = \cos(\theta). \tag{0.5.8}$$
$$\tan(-\theta) = -\tan(\theta). \tag{0.5.9}$$

- Tangent from sine and cosine:

$$\tan(\theta) = \frac{\sin(\theta)}{\cos(\theta)} \tag{0.5.10}$$

- Phase between sine and cosine:

$$\sin\left(\theta \pm \frac{\pi}{2}\right) = \pm\cos(\theta). \tag{0.5.11}$$
$$\cos\left(\theta \pm \frac{\pi}{2}\right) = \mp\sin(\theta). \tag{0.5.12}$$

- Half-period shift:

$$\sin(\theta + \pi) = -\sin(\theta). \tag{0.5.13}$$
$$\cos(\theta + \pi) = -\cos(\theta). \tag{0.5.14}$$

- Angle sum:

$$\sin(\alpha \pm \beta) = \sin(\alpha)\cos(\beta) \pm \cos(\alpha)\sin(\beta). \tag{0.5.15}$$
$$\cos(\alpha \pm \beta) = \cos(\alpha)\cos(\beta) \mp \sin(\alpha)\sin(\beta). \tag{0.5.16}$$

- Double angle:

$$\sin(2\theta) = 2\sin(\theta)\cos(\theta). \tag{0.5.17}$$
$$\cos(2\theta) = 1 - 2\sin^2(\theta). \tag{0.5.18}$$

- Half angle:

$$\sin\left(\frac{\theta}{2}\right) = \pm\sqrt{\frac{1-\cos(\theta)}{2}}. \tag{0.5.19}$$
$$\cos\left(\frac{\theta}{2}\right) = \pm\sqrt{\frac{1+\cos(\theta)}{2}}. \tag{0.5.20}$$
$$\tan\left(\frac{\theta}{2}\right) = \frac{\sin(\theta)}{1+\cos(\theta)}. \tag{0.5.21}$$

- Product to sum:

$$\sin(\theta)\sin(\varphi) = \frac{1}{2}\left[\cos(\theta-\varphi) - \cos(\theta+\varphi)\right]. \tag{0.5.22}$$
$$\cos(\theta)\cos(\varphi) = \frac{1}{2}\left[\cos(\theta-\varphi) + \cos(\theta+\varphi)\right]. \tag{0.5.23}$$
$$\sin(\theta)\cos(\varphi) = \frac{1}{2}\left[\sin(\theta+\varphi) + \sin(\theta-\varphi)\right]. \tag{0.5.24}$$
$$\tan(\theta)\tan(\varphi) = \frac{\cos(\theta-\varphi) - \cos(\theta+\varphi)}{\cos(\theta-\varphi) + \cos(\theta+\varphi)}. \tag{0.5.25}$$

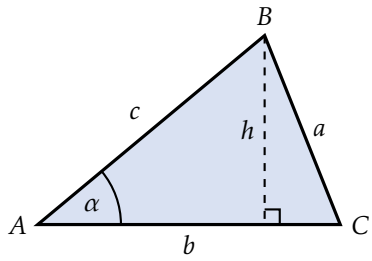


Figure 0.8 The area of a triangle using the side b as a base, and its corresponding height to the point B. The angle opposing the side A is marked as α.

- Sum to product:

$$\sin(\theta) \pm \sin(\varphi) = 2\sin\left(\frac{\theta \pm \varphi}{2}\right)\cos\left(\frac{\theta \mp \varphi}{2}\right). \tag{0.5.26}$$

$$\cos(\theta) + \cos(\varphi) = 2\cos\left(\frac{\theta + \varphi}{2}\right)\cos\left(\frac{\theta - \varphi}{2}\right). \tag{0.5.27}$$

$$\cos(\theta) - \cos(\varphi) = -2\cos\left(\frac{\theta + \varphi}{2}\right)\cos\left(\frac{\theta - \varphi}{2}\right). \tag{0.5.28}$$

$$\tan(\theta) \pm \tan(\varphi) = \frac{\sin(\theta \pm \varphi)}{\cos(\theta)\cos(\varphi)}. \tag{0.5.29}$$

0.5.6 Useful theorems

The area S of a triangle $\triangle ABC$ can be calculated using the length L any side of the triangle (in this context called a **base**) and the height h to its opposing vertex (see Figure 0.8):

$$S = \frac{1}{2}Lh. \tag{0.5.30}$$

The triangle with sides cbh is a right triangle, c being its hypotenuse. We can therefore infer the size of h using α:

$$h = c\sin(\alpha). \tag{0.5.31}$$

Subtituting this back to Equation 0.5.30 yields that the area of the triangle is

$$S = \frac{1}{2}bc\sin(\alpha). \tag{0.5.32}$$

There is nothing special about choosing the side b as a base: we can also use a or c for the calculation. This will yield, repspectively,

$$S = \frac{1}{2}ac\sin(\gamma), \tag{0.5.33}$$

$$S = \frac{1}{2}ac\sin(\beta), \tag{0.5.34}$$

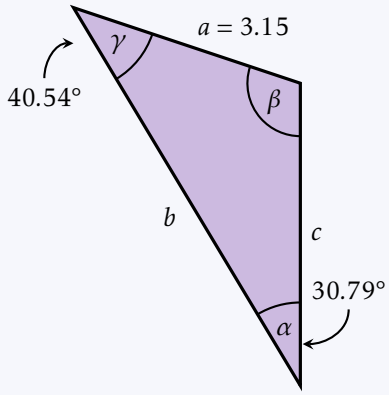
where β is the angle opposing b and γ is the angle opposing c. Since S is the same in all cases, we simply multiply each of the area equations by 2 and divide by abc, which yields

$$\frac{\sin(\alpha)}{a} = \frac{\sin(\beta)}{b} = \frac{\sin(\gamma)}{c}, \tag{0.5.35}$$

i.e. in a triangle, the ratio between any side and the sine of its opposing angle is always the same no matter which side we choose. This theorem is called the **law of sines**.

Example 0.45 Law of sines

Given the triangle $\triangle ABC$ below, what are β and b?



Since all angles in a triangle must add up to 180°,

$$\beta = 180° - 30.79° - 40.54° = 108.67°.$$

Using the law of sines,

$$b = \frac{a}{\sin(\alpha)} \cdot \sin(\beta) = \frac{3.15}{\sin(30.79°)} \cdot \sin(108.67°) \approx 5.83,$$

and

$$c = \frac{a}{\sin(\alpha)} \cdot \sin(\gamma) = \frac{3.15}{\sin(30.79°)} \cdot \sin(40.54°) \approx 4.$$

Note 0.8 Ambiguity of solutions

The above example reveals an issue that might arise due to the symmetrical nature of $\sin(x)$ around $x = \pi$ (180°): say we wanted to calculate β using the law of sines instead of by using $\beta = 180° - \alpha - \gamma$. In this case we would solve the equation

$$\frac{\sin(\alpha)}{a} = \frac{\sin(\beta)}{b},$$

which would result in $\beta = \arcsin\left(\frac{b\sin(\alpha)}{a}\right) = \arcsin(0.95)$. However, two angles can fit this requirement: the sines of 71.34° and 108.67° are both equal to 0.95!

Therefore, we must be careful when using the law of sine and make sure we always choose values that make sense (e.g. such that all angles add up to 180°).

Of course, the sine function is not unique in having its own named "Law": another useful theorem is the so-called **law of cosines** (also **al-Kashi's theorem**). This theorem states that given a triangle with sides a, b, c and an angle γ opposing c,

$$c^2 = a^2 + b^2 - 2ab\cos(\gamma). \tag{0.5.36}$$

Much like the law of sines, the choice of angle does not matter, as long as we plug the correct sides to the equation: for α and β being the angles opposing to a and b respectively,

$$\begin{aligned} a^2 &= b^2 + c^2 - 2bc\cos(\alpha), \\ b^2 &= a^2 + c^2 - 2ac\cos(\beta). \end{aligned} \tag{0.5.37}$$

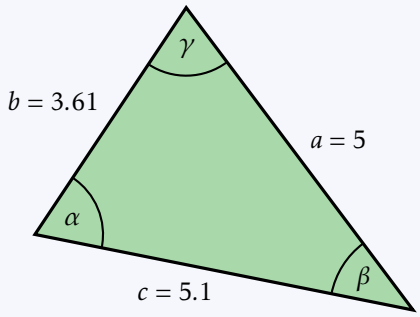
If the triangle in question is a right triangle then one of the angles is equal to 90°. Without loss of generality, let us assume that this is γ. Since $\cos(90°) = 0$ we get that in the case of a right triangle

$$c^2 = a^2 + b^2, \tag{0.5.38}$$

i.e. we retrieve back the Pythagorean theorem.

Example 0.46 Law of cosines

Calculate all angles in the following triangle:



Using the law of cosines:

$$\begin{aligned} \cos(\gamma) &= \frac{c^2 - b^2 - a^2}{-2ab} = \frac{5.1^2 - 3.61^2 - 5^2}{-2 \cdot 5 \cdot 3.61} \approx 0.33302 \Rightarrow \gamma = 70.54°, \\ \cos(\beta) &= \frac{b^2 - a^2 - c^2}{-2ac} = \frac{3.61^2 - 5^2 - 5.1^2}{-2 \cdot 5 \cdot 5.1} \approx 0.74466 \Rightarrow \beta = 41.87°, \\ \cos(\alpha) &= \frac{a^2 - b^2 - c^2}{-2cb} = \frac{5^2 - 3.61^2 - 5.1^2}{-2 \cdot 5.1 \cdot 3.61} \approx 0.38135 \Rightarrow \alpha = 67.58°. \end{aligned}$$

0.6 COMPLEX NUMBERS

0.6.1 Algebraic approach

Real numbers, while being extremely useful, are not complete - they can't solve all equations involving numbers. For example, the equation

$$x^2 + 1 = 0 \tag{0.6.1}$$

has no real solutions, since there can be no real number x such that $x^2 = -1$. However, we can choose to define a new number, $\mathrm{i} = \sqrt{-1}$ and using it to build a new number system. This system is of course the set of complex numbers, $\mathbb{C}$. It is defined as the set of all z such that

$$z = a + \mathrm{i}b, \tag{0.6.2}$$

where $a, b \in \mathbb{R}$ and $\mathrm{i} = \sqrt{-1}$. We call a the **real component** of z or $\mathfrak{Re}(z)$, and b its **imaginary component** or $\mathfrak{Im}(z)$[6]. These numbers appear a lot all throughout the exact sciences (but especially in physics and engineering), so we must at the very least learn their basic properties.

It is not so obvious that we can add two different kinds of numbers together, but it works (the linear algebra chapter sheds more light on this idea). What is important is that we always keep these two parts separated. We see this when we add together two complex numbers z_1, z_2:

$$z = z_1 + z_2 = (a_1 + b_1\mathrm{i}) + (a_2 + b_2\mathrm{i}) = (a_1 + a_2) + (b_1 + b_2)\mathrm{i}. \tag{0.6.3}$$

The real part of z is therefore $a_1 + b_1$, and its imaginary part is $b_1 + b_2$.

What happens when we multiply two complex numbers? Let's check:

$$\begin{aligned} z = z_1 z_2 &= (a_1 + b_1\mathrm{i})(a_2 + b_2\mathrm{i}) \\ &= a_1 a_2 + \mathrm{i}a_1 b_2 + \mathrm{i}a_2 b_1 + \mathrm{i}^2 b_1 b_2 \\ &= a_1 a_2 + \mathrm{i}a_1 b_2 + \mathrm{i}a_2 b_1 - b_1 b_2 \\ &= (a_1 a_2 - b_1 b_2) + \mathrm{i}\,(a_1 b_2 + a_2 b_1). \end{aligned} \tag{0.6.4}$$

We see that we can still separate the real part and imaginary part of the result. What happens in the case of two real numbers? For real numbers $b = 0$, and thus Equation 0.6.4 devolves to $z = a_1 a_2 \in \mathbb{R}$, which is exactly what we expect: multiplying two real numbers yields their product, which is a real number. Notice that this doesn't happen with purely imaginary numbers: multiplying together two imaginary numbers (i.e. numbers for which $a = 0$) results in a real number. Will get to understand why this happens very soon.

When discussing real numbers sometimes we like to refer to their *magnitude*, i.e. their absolute value. With complex numbers this is defined as

$$|z| = \sqrt{a^2 + b^2}, \tag{0.6.5}$$

[6] There is nothing more "real" about real numbers than imaginary numbers, but unfortunately that's the terminology we're stuck with ¯_(ツ)_/¯

i.e. in a sense, to get the magnitude of a complex number we imagine its two components as being perpendicular and calculate the length of the resulting hypotenous (cf. the Pythagorean theorem). In fact, this is one very useful interpertation of complex numbers, which we will explore in depth in the next subsection.

A very important operation that can be applied to complex numbers is **conjugation**. The conjugate of a complex number $z = a + \mathrm{i}b$ is defined as

$$\overline{z} = a - \mathrm{i}b, \tag{0.6.6}$$

i.e. conjugating a number is simply negating its imaginary part. When we multiply a complex number by its own complex conjugate we get

$$z\overline{z} = (a + \mathrm{i}b)(a - \mathrm{i}b) = a^2 + \cancel{ab\mathrm{i}} - \cancel{ab\mathrm{i}} - b^2\mathrm{i}^2 = a^2 + b^2, \tag{0.6.7}$$

i.e. $z\overline{z} = |z|^2$. The inverse of a complex number can be expressed as

$$z^{-1} = \frac{\overline{z}}{|z|^2}. \tag{0.6.8}$$

0.6.2 Geometric approach

As alluded to in the previous subsection, we can interpret a complex number $z = a + \mathrm{i}b$ as two components in a 2-dimensional space (called the **complex plane**), in which the horizontal axis represents real components, and the vertical access represents imaginary components:

Drawing a line from z to a (on the real axis) creates a right triangle. We can then define θ to be the angle near the origin and r the length of the hypotenous: We call r the **magnitude** of z, and θ its **argument**. The ranges for r and θ are, respetively, $[0, \infty)$ and $[0, 2\pi)$.

Using Equation 0.5.4 the real and imaginary components of z are

$$\begin{aligned} a &= r\cos(\theta), \\ b &= r\sin(\theta), \end{aligned} \tag{0.6.9}$$

and z can be re-written as

$$z = r(\cos(\theta) + \mathrm{i}\sin(\theta)). \tag{0.6.10}$$

Which we call the **polar form** of z (contrasted with $z = a + \mathrm{i}b$ being the **Cartesian form** of z).

Inverting the relations in Equation 0.6.9 yields the relations

$$\begin{aligned} r &= a^2 + b^2, \\ \theta &= \arctan\left(\frac{b}{a}\right). \end{aligned} \tag{0.6.11}$$

Let's examine the same properties of complex numbers shown in Equations 0.6.3, 0.6.4 and 0.6.6, and verify that they work in the polar form of complex numbers. We start

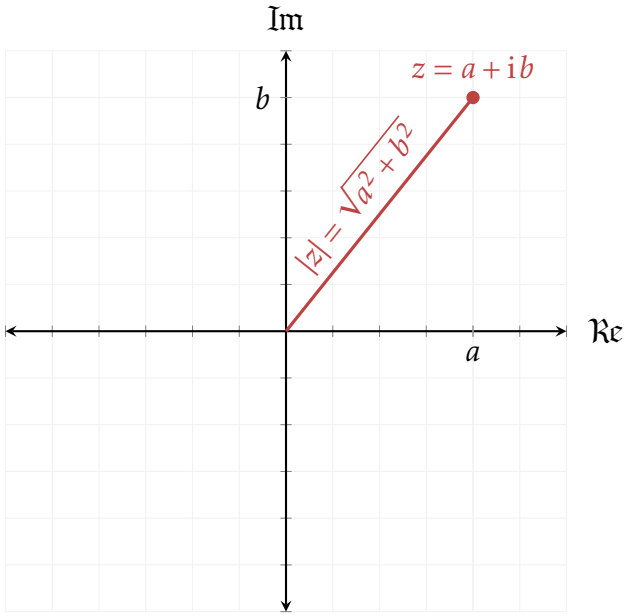


Figure 0.9 A complex number $z = a + \mathrm{i}b$ shown on the complex plane: the horizontal and vertical axes represent the real and imaginary components, respectively.

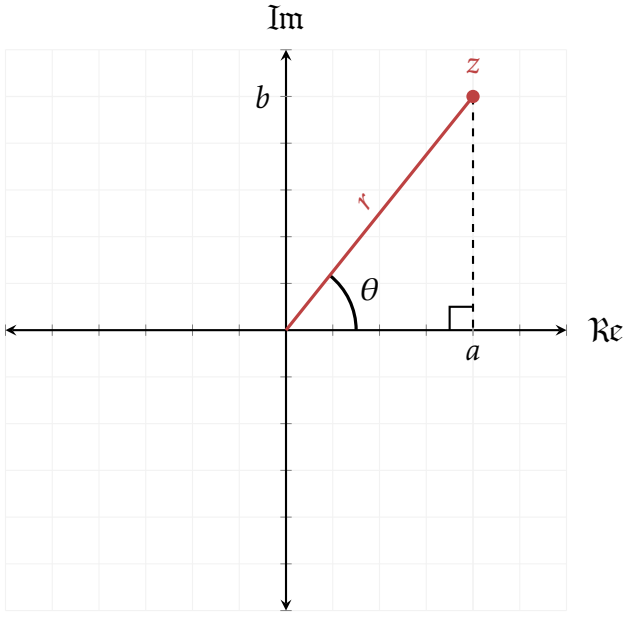


Figure 0.10 The same complex number z from Figure 0.9 shown with its polar components $r = |z| = \sqrt{a^2 + b^2}$ and $\theta = \arctan\left(\frac{b}{a}\right)$.

with addition (Equation 0.6.3):

$$\begin{aligned} z_1 + z_2 &= r_1\left[\cos(\theta_1) + \mathrm{i}\sin(\theta_1)\right] + r_2\left[\cos(\theta_2) + \mathrm{i}\sin(\theta_2)\right] \\ &= \underbrace{r_1\cos(\theta_1)}_{a_1} + \underbrace{r_2\cos(\theta_2)}_{a_2} + \mathrm{i}\underbrace{r_1\sin(\theta_1)}_{b_1} + \mathrm{i}\underbrace{r_2\sin(\theta_2)}_{b_2} \\ &= (a_1 + a_2) + \mathrm{i}(b_1 + b_2). \end{aligned} \tag{0.6.12}$$

We see that indeed, the polar form of complex numbers adheres to the addition rule in Equation 0.6.3. Next is the product rule:

$$\begin{aligned} z_1 z_2 &= r_1\left[\cos(\theta_1) + \mathrm{i}\sin(\theta_1)\right] \cdot r_2\left[\cos(\theta_2) + \mathrm{i}\sin(\theta_2)\right] \\ &= r_1 r_2\left[\cos(\theta_1)\cos(\theta_2) + \mathrm{i}\cos(\theta_1)\sin(\theta_2) + \mathrm{i}\sin(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)\right] \\ &= r_1\cos(\theta_1) r_2\cos(\theta_2) - r_1\sin(\theta_1) r_2\sin(\theta_2) + \mathrm{i}\left[r_1\cos(\theta_1) r_2\sin(\theta_2) + r_1\sin(\theta_1) r_2\cos(\theta_2)\right] \\ &= (a_1 a_2 - b_1 b_2) + \mathrm{i}(a_1 b_2 + a_2 b_1), \end{aligned} \tag{0.6.13}$$

which is indeed the result seen in Equation 0.6.4. We can also develope further the second row of Equation 0.6.13 using some trigonometry (specifically the trigonometric identities in Equation 0.5.25):

$$\begin{aligned} z_1 z_2 &= r_1 r_2\left[\cos(\theta_1)\cos(\theta_2) + \mathrm{i}\cos(\theta_1)\sin(\theta_2) + \mathrm{i}\sin(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)\right] \\ &= r_1 r_2\left[\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2) + i\left[\cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2)\right]\right] \\ &= r_1 r_2\left[\cos(\theta_1 + \theta_2) + \mathrm{i}\sin(\theta_1 + \theta_2)\right]. \end{aligned} \tag{0.6.14}$$

This is a very important result: it shows that multiplying a complex number z_1 by another complex number z_2 gives a complex number with magnitude $r_1 r_2$, i.e. the product of the magnitudes of the two complex numbers, and argument $\theta_1 + \theta_2$, i.e. the argument of z_1 rotated by the argument of z_2 (or vice-versa). We will consider this result in more detail soon.

In the polar form the complex conjugate of a number $z = r\left[\cos(\theta) + \mathrm{i}\sin(\theta)\right]$ can be brought about by substituting $-\theta$ into the arguments of the trigonometric functions:

$$\begin{aligned} \overline{z} &= r\left[\cos(-\theta) + \mathrm{i}\sin(-\theta)\right] \\ &= r\left[\cos(\theta) - \mathrm{i}\sin(\theta)\right] \\ &= r\cos(\theta) - \mathrm{i}r\sin(\theta) \\ &= a - \mathrm{i}b. \end{aligned} \tag{0.6.15}$$

Lastly, let's show that Equation 0.6.7 can be derived in the polar form:

$$\begin{aligned} z\overline{z} &= r\left[\cos(\theta) + \mathrm{i}\sin(\theta)\right] \cdot r\left[\cos(\theta) - \mathrm{i}\sin(\theta)\right] \\ &= r^2\left[\cos^2(\theta) - \cancel{\mathrm{i}\cos(\theta)\sin(\theta)} + \cancel{\mathrm{i}\sin(\theta)\cos(\theta)} + \sin^2(\theta)\right] \\ &= r^2\left[\sin^2(\theta) + \cos^2(\theta)\right] \\ &= r^2 = a^2 + b^2. \end{aligned} \tag{0.6.16}$$

In 1748 Leonhard Euler published his famous work *Introductio in analysin infinitorum*[7]. In it he introduced the following relation, called **Euler's formula**:

$$\mathrm{e}^{\mathrm{i}x} = \sin(x) + \mathrm{i}\cos(x). \tag{0.6.17}$$

[7] Latin for **Introduction to the Analysis of the Infinite**.

Table 0.4 Values of e^{ix} for some useful values of x (cf. Table 0.3 for the values of $\sin(\theta)$ and $\cos(\theta)$).

x	$\cos(x)$	$\sin(x)$	$z = e^{ix}$
$\frac{\pi}{2}$	0	1	i
π	-1	0	-1
$\frac{3\pi}{2}$	0	-1	$-i$
$\frac{\pi}{3}$	$\frac{1}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}\left(1+i\sqrt{3}\right)$
$\frac{\pi}{4}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{2}}{2}(1+i)$
$\frac{\pi}{6}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}$	$\frac{1}{2}\left(\sqrt{3}+i\right)$

Using Euler's formula a complex number z can be written as

$$z = re^{i\theta}. \tag{0.6.18}$$

In Table 0.4 we can see some usefull complex exponentials e^{ix}. Specifically, setting $x = \pi$ yields the famous **Eurler's identity**, considered by many to be one of the most beautiful equations in mathematics, as it binds together five important numbers, namely $0, 1, \pi, e$ and i:

$$e^{i\pi} + 1 = 0. \tag{0.6.19}$$

Table 0.4 also shows us the integer behaviours of i:

$$i^2 = -1,\ i^3 = -i, i^4 = 1,\ i^5 = i,\ i^6 = -1,\ i^7 = -i,\ \ldots \tag{0.6.20}$$

0.6.3 Roots of complex numbers

What is the n-th order roots of a complex number z, i.e. $\sqrt[n]{z}$? An illuminating way to approach this problem is by looking at the polar form of z. As an example, we start with the number $z = 1$ and find its 3rd order roots, i.e. all number w such that $w^3 = 1$ (spoiler alert: there are three such numbers).

Equation 0.6.14 taught us that complex numbers not only scale other numbers, but also rotate them: with real numbers the product $x \cdot y$ is equivalent to a scaling of x by y. With complex numbers the product has two components: its magnitude is the scale of x by y, and its argument is the argument of x rotated by the argument of y[8].

Example 0.47 Rotation using complex numbers

Let $z = 2 + 2i$ and $w = 3i$. Their polar forms are $z = 2\sqrt{2}\,[\cos(\pi/4) + i\sin(\pi/4)]$ and $w = 3\,[\cos(\pi/2) + i\sin(\pi/2)]$. Their product is

$$z \cdot w = (2 + 2i) \cdot 3i = 6i + 6i^2 = -6 + 6i,$$

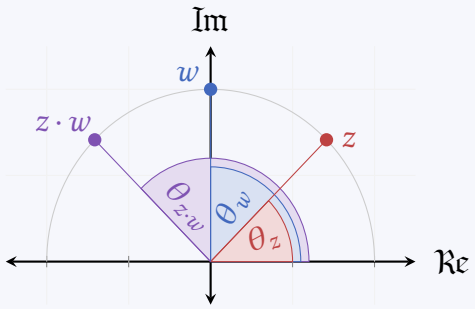
[8] Due to the commutativity of the complex product we can switch the order of z and w and get the same result.

which in polar form is $6\sqrt{2}\,[\cos(3\pi/4)+\mathrm{i}\sin(3\pi/4)]$. Note that

$$2\sqrt{2}\cdot 3 = 6\sqrt{2}, \text{ and}$$
$$\frac{\pi}{4}+\frac{\pi}{2}=\frac{3\pi}{4},$$

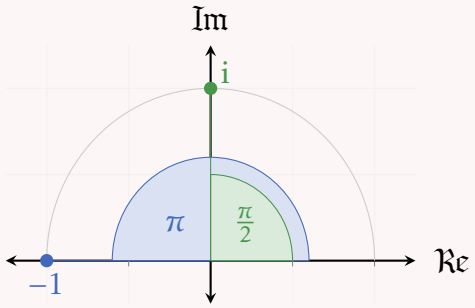
i.e. $z\cdot w$ has magnitude which is the **product** of the magnitudes of z and w, and an argument which is the **sum** of the arguments of z and w.

The figure below depict the arguments of the three numbers $z, w, z\cdot w$. Note that $\theta_{z\cdot w}=\theta_z+\theta_w$.



Note 0.9 $\mathrm{i}^2=-1$ from a geometric (polar) viewpoint

In polar coordinates i has magnitude 1 and argument $\frac{\pi}{2}$, i.e. multiplying by i is equivalent to rotation by $\frac{\pi}{2}$ (90°) counter clockwise. Therefore, multiplying i by itself, i.e. i^2, rotates i itself by $\frac{\pi}{2}$ counter clockwise, bringing it to -1.



In polar form $1=\cos(0)+\mathrm{i}\sin(0)$. Finding the arguments of the cube roots of 1 is therefore done by answering the following question: what angles θ will equal 0 (or its equivalent angles $2\pi, 4\pi, 6\pi, \ldots$) when multiplied by 3? The answer is very simple: the only possible solutions are

$$\begin{aligned}\theta_1 &= 0,\\ \theta_2 &= \frac{2\pi}{3},\\ \theta_3 &= \frac{4\pi}{3}.\end{aligned} \tag{0.6.21}$$

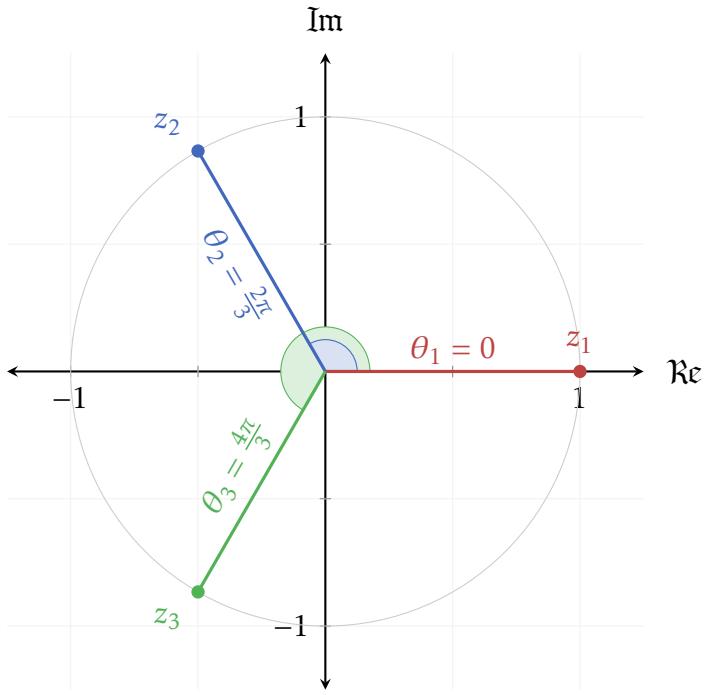


Figure 0.11 The three cube roots of $z = 1$.

(any other number in the range $[0, 2\pi)$ will give the same angles)

Therefore, the three cube roots of 1 are [9] (Figure 0.11)

$$\begin{aligned} z_1 &= \cos(\theta_1) + \mathrm{i}\sin(\theta_1) = \cos(0) + \mathrm{i}\sin(0) = 1, \\ z_2 &= \cos(\theta_2) + \mathrm{i}\sin(\theta_2) = \cos\left(\frac{2\pi}{3}\right) + \mathrm{i}\sin\left(\frac{2\pi}{3}\right) = -0.5 + \frac{\sqrt{3}}{2}\mathrm{i}, \\ z_3 &= \cos(\theta_3) + \mathrm{i}\sin(\theta_1) = \cos\left(\frac{4\pi}{3}\right) + \mathrm{i}\sin\left(\frac{4\pi}{3}\right) = -0.5 - \frac{\sqrt{3}}{2}\mathrm{i}. \end{aligned} \tag{0.6.22}$$

The n-th degree roots of 1 will follow the same pattern for $n \in \mathbb{N}$ (see Figure 0.12): their magnitude is always 1, and the argument of the k-th root is

$$\theta_k = \frac{2\pi}{n}k. \tag{0.6.23}$$

Finding the n-th degree roots of a general complex number $z = r[\cos(\theta) + \mathrm{i}\sin(\theta)]$ can be done in a similar fashion: all roots will have the magnitude $\sqrt[n]{r}$, and their argument θ_k will be such that multiplying it by n gives $\theta + 2\pi m$ for some integer value m, i.e.

$$\theta_k = \frac{\theta + 2\pi m}{n}. \tag{0.6.24}$$

[9] recall that $\sqrt[3]{1} = 1$, and therefore all roots have magnitude 1.

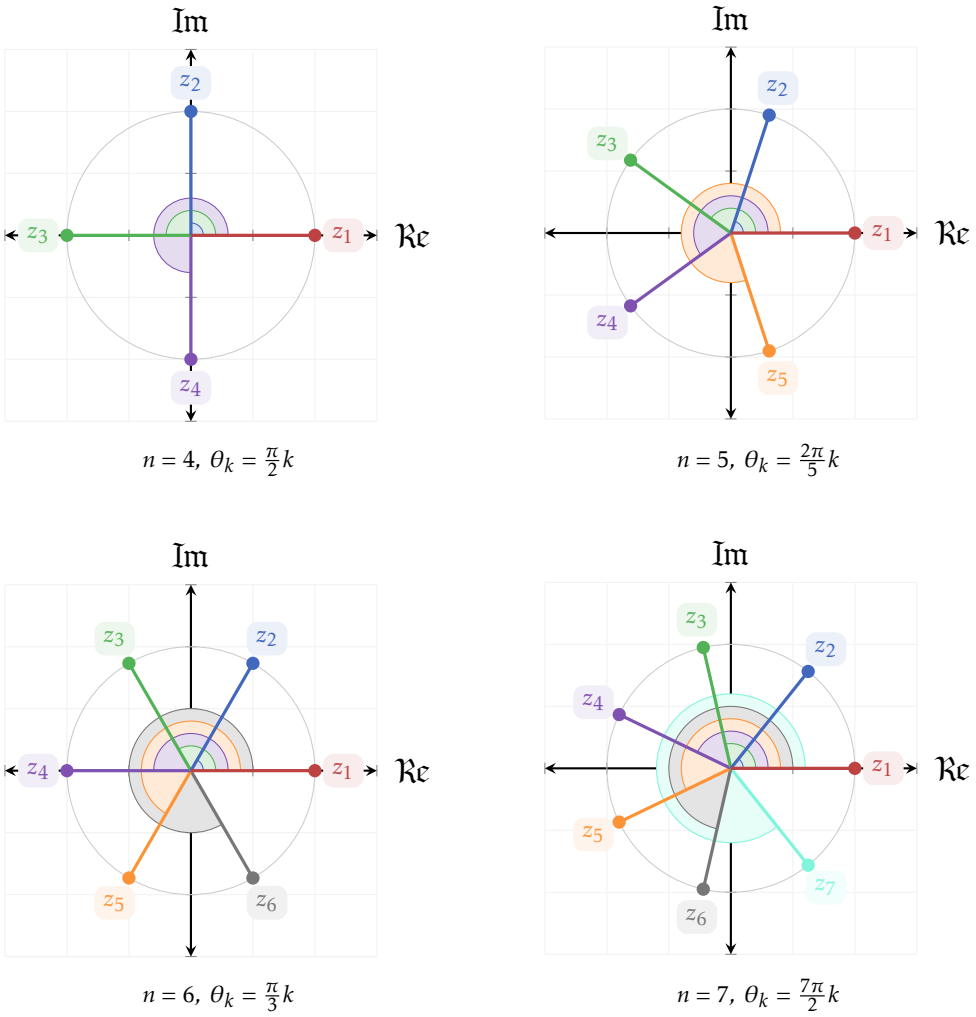


Figure 0.12 Complex n-th roots of $z = 1$ for $n = 4, 5, 6, 7$. Note that for all circles $r = 1$.

0.7 EXERCISES

0.1. Write the following sets explicitly:

(i) $\{x \in \mathbb{N} \mid 1 < x \leq 7\}$

(ii) $\{x \in \mathbb{Z} \mid x < 5\}$

(iii) $\left\{x \in \mathbb{R} \mid x^2 = -1\right\}$

(iv) $\{x \in \mathbb{N} \wedge x \in \mathbb{Q}\}$

(v) $\left\{x \in \mathbb{R} \mid x^2 - 3x - 4 = 0\right\}$

(vi) $\{x \in \mathbb{R} \mid x < 5 \wedge x \geq 2\}$

0.2. Determine the relation between the sets:

(i) $A = \{1,\ 2,\ 3\},\ B = \{1,\ 2\}$

(ii) $A = \varnothing,\ B = \{2,\ -5,\ \pi\}$

(iii) $A = \mathbb{Z},\ B = \{\pm x \mid x \in \mathbb{N} \cup \{0\}\}$

(iv) $A = \left\{\pi, \mathrm{e}, \sqrt{2}\right\},\ B = \mathbb{Q}$

0.3. Write all elements in $S^2 \times W$, where $S = \{\alpha, \beta, \gamma\}$ and $W = \{x, y, z\}$. Find a condition that guarantees $S^2 \times W = W \times S^2$.

0.4. How many different injective functions $f : \{1, 2\} \to \{1, 2\}$ exist? How many injective functions $f : \{1, 2, 3\} \to \{1, 2, 3\}$ exist? How many inject functions $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ exist for a given $n \in \mathbb{N}$?

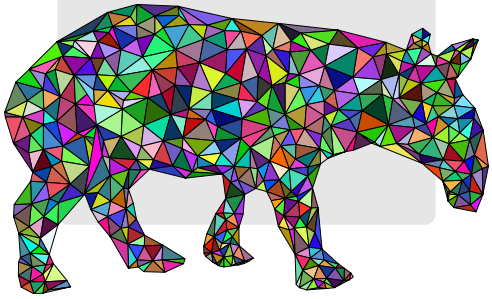
0.5. For each of the real functions below, find a set on which it is surjective (use a graphing calculator if you are not familiar with the shape of a function):

$$x^2,\ x^3 - 5,\ \mathrm{e}^{-x^2/2},\ \sin(x),\ \sin(x) + \cos(x),\ x\mathrm{e}^x.$$

0.6. Given two sets A, B such that $|B| = |A| - 1$, can a bijective function $f : A \to B$ exist? Explain your answer.

0.7. MORE EXERCISES TO BE WRITTEN...

CHAPTER 1



LINEAR ALGEBRA
(INTUITIVE APPROACH)

Linear algebra is one of the most important and often used fields, both in theoretical and applied mathematics. It brings together the analysis of systems of linear equations and the analysis of linear functions (in this context usually called linear transformations), and is employed extensively in almost any modern mathematical field, e.g. approximation theory, vector analysis, signal analsys, error correction, 3-dimensional computer graphics and many, many more.

In this book, we divide our discussion of linear algebra into to chapters: the first (this chapter) deals with a wider, birds-eye view of the topic: it aims to give an intuitive understanding of the major ideas of the topic. For this reason, in this chapter we limit ourselves almost exclusively to discussing linear algebra using 2- and 3-dimensional analysis (and higher dimensions when relevant) using real numbers only. This allows us to first create an intuitive picture of what is linear algebra all about, and how to use correctly the tools it provides us with.

The next chapter takes the opposite approach: it builds all concepts from the ground-up, defining precisely (almost) all basic concepts and proving them rigorously,

and only then using them to build the next steps. This approach has two major advantages: it guarntees that what we build has firm foundations and does not fall apart at any future point, and it also allows us to generalize the ideas constructed during the process to such extent that they can be used as foundation to build ever newer tools we can apply in a wide range of cases.

Note 1.1 Why present rigorous mathematics in this book?

Rigorous mathematics is rarely neccessary for those who are interested of the tools mathematics provides us, rather than the full and deep understanding of the concepts these tools are based on. However, it can be useful to students of scientific fields to experience rigorous mathematics at least once in their course of study. Usually, the choice for the topic to be analyzed rigorously is between linear algebra and calculus - for this book the latter was chosen.

!

1.1 VECTORS

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent

blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

1.2 LINEAR TRANSFORMATIONS

1.3 MATRICES

1.4 SYSTEMS OF LINEAR EQUATIONS

1.5 EIGENVECTORS AND EIGENVALUES

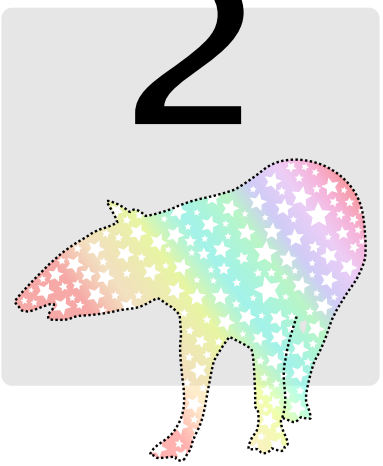
1.6 DECOMPOSITIONS

1.7 SOME REAL LIFE USES OF LINEAR ALGEBRA

1.8 EXERCISES

CHAPTER

2



LINEAR ALGEBRA

(RIGOROUS APPROACH)

Something about formalism, theorems, proofs, etc.

2.1 FIELDS

We begin our dive into the rigorous analysis of linear algebra by defining an algebraic construction call a **field**. In essence, a field has most of the important properties of the real numbers, namely the closure, commutativity, associativity, identity and inverse of addition and multiplication of any two elements in the field (except the product inverse of the field equivalent object for the number 0). In a later section we will use fields to construct the general notion of **vector spaces**.

Definition 2.1 Field

A field $\mathbb{F}$ is a set of objects together with two operations called **addition** and **multiplication** (denoted + and ·, respectively), for which the following axioms hold:

- **Closure of under addition and multiplication**: for any $a, b \in \mathbb{F}$,
  1. $(a + b) \in \mathbb{F}$,
  2. $(a \cdot b) \in \mathbb{F}$.

- **Commutativity under addition multiplication**: for any $a, b \in \mathbb{F}$,
  1. $a + b = b + a$,
  2. $a \cdot b = b \cdot a$.

- **Associativity under addition and multiplication**: for any $a, b, c \in \mathbb{F}$,
  1. $a + (b + c) = (a + b) + c$,
  2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

- **Additive and multiplicative identity**: there exist an element in $\mathbb{F}$ called the *additive identity* and denoted by 0, for which $a + 0 = a$ for any $a \in \mathbb{F}$.

  Similarily, there exists an element in $\mathbb{F}$ called the *multiplicative identity* and denoted by 1, for which $a \cdot 1 = a$ for any $a \in \mathbb{F}$.

- **Additive and multiplicative inverses**: for any element $a \in \mathbb{F}$ (except the additive identity) there exists:
  1. $b \in \mathbb{F}$ such that $a + b = 0$, and
  2. $c \in \mathbb{F}$ such that $a \cdot c = 1$.

  (usualy b is denoted as $-a$, while c is denoted as a^{-1})

- **Distributivity of multiplication over addition**: for any $a, b, c \in \mathbb{F}$,

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

π

2.1.1 Infinite fields

We start with one of the most obvious examples of a field: the real numbers together with the standard addition and product.

Theorem 2.1 $\mathbb{R}$ as a field

The set of real numbers $\mathbb{R}$ forms a field together with the standard addition and product.

We leave the proof of 2.1 to the reader, as it is pretty straight forward using the known properties of the standard addition and product over $\mathbb{R}$ (and rather uninteresting). Instead, we jump forward to using 2.1 for proving the same idea about the complex numbers:

Theorem 2.2 $\mathbb{C}$ as a field and more more more

The set of complex numbers $\mathbb{C}$ forms a field together with the addition and product operations as defined in Section 0.6 (namely Equation 0.6.3, Equation 0.6.4 and Equation 0.6.13).

Proof 2.1 $\mathbb{C}$ as a field

(note: in the following proof, equalities marked with ! use the respective propery of the real numbers)

- **Closure under both operations**: For any two complex numbers $z_1 = a + \mathrm{i}b$ and $z_2 = c + \mathrm{i}d$,

  - Addition: Since addition in $\mathbb{R}$ is closed, $(a+c) \in \mathbb{R}$ and $(b+d) \in \mathbb{R}$. Therefore
  $$z = z_1 + z_2 = a + c + (b+d)\mathrm{i}$$
  is also a complex number with $\mathfrak{Re}(z) = a + c$ and $\mathfrak{Im}(z) = b + d$.

  - Multiplication: Since multiplication in $\mathbb{R}$ is also closed, $(ac - bd) \in \mathbb{R}$ and $(ad + bc) \in \mathbb{R}$. Therefore
  $$z = z_1 \cdot z_2 = ac - bd + (ad + bc)\mathrm{i}$$
  is a complex number with $\mathfrak{Re}(z) = ac - bdc$ and $\mathfrak{Im}(z) = ad + bc$.

- **Commutativity of both operation**: For any two complex numbers $z_1 = a + \mathrm{i}b$ and $z_2 = c + \mathrm{i}d$,

  - Addition: Since addition in $\mathbb{R}$ is commutative, $a+c = c+a$ and $b+d = d+b$. Therefore
  $$z_1 + z_2 = a + c + (b+d)\mathrm{i} \overset{!}{=} c + a + (d+b)\mathrm{i} = z_2 + z_2.$$

  - Multiplication: Since multiplication in $\mathbb{R}$ is also commutative, $ac - bd = ca - db$ and $ad + bc = da + cb$. Therefore
  $$z_1 \cdot z_2 = ac - bd + (ad + bc)\mathrm{i} \overset{!}{=} ca - db + (da + cb)\mathrm{i} = z_2 \cdot z_1.$$

- **Associativity of both operation**: For any three complex numbers $z_1 = a + \mathrm{i}b$, $z_2 = c + \mathrm{i}d$ and $z_3 = g + \mathrm{i}h$ (where $a, b, c, d, g, h \in \mathbb{R}$[a]),

• Addition: Since addition in $\mathbb{R}$ is associative, $a+(c+g)=(a+c)+g$ and $b+(d+h)=(b+d)+h$. Therefore

$$z_1+(z_2+z_3)=a+(c+g)+[b+(d+h)]\mathrm{i}\overset{!}{=}(a+c)+g+[(b+d)+h]\mathrm{i}=(z_1+z_2)+z_3.$$

• Multiplication: Since multiplication in $\mathbb{R}$ is also associative, the following equalities apply:

$$\begin{aligned}
a\cdot(c\cdot g)&=(a\cdot c)\cdot g,\\
b\cdot(c\cdot h)&=(b\cdot c)\cdot h,\\
a\cdot(d\cdot h)&=(a\cdot d)\cdot h,\\
b\cdot(d\cdot g)&=(b\cdot d)\cdot g,\\
a\cdot(c\cdot h)&=(a\cdot c)\cdot h,\\
a\cdot(d\cdot g)&=(a\cdot d)\cdot g,\\
b\cdot(c\cdot g)&=(b\cdot c)\cdot g,\\
b\cdot(d\cdot h)&=(b\cdot d)\cdot h.
\end{aligned}$$

Therefore,

$$\begin{aligned}
z_1\cdot(z_2\cdot z_3)&=a\cdot(c\cdot g)-a\cdot(d\cdot h)-b\cdot(c\cdot h)-b\cdot(d\cdot g)\\
&\quad+[a\cdot(c\cdot h)+a\cdot(d\cdot g)+b\cdot(c\cdot g)-b\cdot(d\cdot h)]\mathrm{i}\\
&\overset{!}{=}(a\cdot c)\cdot g-(a\cdot d)\cdot h-(b\cdot c)\cdot h-(b\cdot d)\cdot g\\
&\quad+[(a\cdot c)\cdot h+(a\cdot d)\cdot g+(b\cdot c)\cdot g-(b\cdot d)\cdot h]\mathrm{i}\\
&=(z_1\cdot z_2)\cdot z_3.
\end{aligned}$$

• **Identity for both operations**:

• Addition: The complex number $0=0+0i$ is the complex addition identity: for any real number $x\in\mathbb{R}$, $x+0=x$. Therefore, for any complex number $z=a+\mathrm{i}b$,

$$z+0=a+\mathrm{i}b+0+0i=a+0+(b+0)\mathrm{i}\overset{!}{=}a+\mathrm{i}b.$$

• Multiplication: The complex number $1=1+0\mathrm{i}$ is the complex multiplication identity: for any real number $x\in\mathbb{R}$, $x\cdot 1=x$ and $x\cdot 0=0$. Therefore, for any complex number $z=a+\mathrm{i}b$,

$$z\cdot 1=(a+\mathrm{i}b)\cdot(1+0\mathrm{i})\overset{!}{=}a\cdot 1-\cancel{b\cdot 0\mathrm{i}^2}+(\cancel{a\cdot 0\mathrm{i}}+b\cdot 1)\mathrm{i}=a+\mathrm{i}b.$$

• **Inverse for both operations**:

• Addition: For any complex number $z_1 = a + \mathrm{i}b$, the number $z_2 = -a - \mathrm{i}b$ is also a complex number for which

$$z_1 + z_2 = a + \mathrm{i}b + -a - \mathrm{i}b \overset{!}{=} a - a + (b - b)\mathrm{i} = 0 + 0\mathrm{i} = 0.$$

• Multiplication: For any complex number $z = re^{\theta i}$ where $r \neq 0$, the number $z^{-1} = \frac{1}{r}e^{-\mathrm{i}\theta}$ is also a complex number for which

$$z \cdot z^{-1} = re^{\mathrm{i}\theta} \cdot \frac{1}{r}e^{-\mathrm{i}\theta} \overset{!}{=} \frac{r}{r}e^{\mathrm{i}\theta - \mathrm{i}\theta} = 1 \cdot 1 = 1.$$

Note: for $z = a + \mathrm{i}b$,

$$z^{-1} = \frac{1}{r}e^{-\mathrm{i}\theta} = \frac{1}{|z|} \cdot \frac{a - \mathrm{i}b}{|z|} = \frac{1}{|z|} \cdot \frac{\overline{z}}{|z|} = \frac{\overline{z}}{|z|^2}.$$

Therefore, for any $z \neq 0$, $z^{-1} = \frac{\overline{z}}{|z|^2}$.

• **Distributivity of of multiplication over addition**: For any $z_1 = a + \mathrm{i}b$, $z_2 = c + \mathrm{i}d$ and $z_3 = g + \mathrm{i}h$,

$$\begin{aligned} z_1 \cdot (z_2 + z_3) &= (a + \mathrm{i}b) \cdot (c + \mathrm{i}d + g + \mathrm{i}h) = (a + \mathrm{i}b) \cdot (c + g + [d + h]\mathrm{i}) \\ &= ac + ag + (bd)\mathrm{i}^2 + (bh)\mathrm{i}^2 \\ &+ (ad)\mathrm{i} + (ah)\mathrm{i} + (bc)\mathrm{i} + (bg)\mathrm{i} \\ &= ac + ag - bd - bh + (ad + ah + bc + bg)\mathrm{i} \\ &= ac - bd + (ad + bc)\mathrm{i} + ag - bh + (ah + bg)\mathrm{i} \\ &= (z_1 \cdot z_2) + (z_1 \cdot z_3). \end{aligned}$$

[a] The letters g and h are used instead of e and f to avoid confusion with Eurler's constant and the common notation for real functions, respectively.

QED

The sets $\mathbb{R}$ and $\mathbb{C}$ are examples of **infinite fields**, since they each have infinite number of elements. The set $\mathbb{Q}$ (rational numbers) can be shown to also be an infinite field, however unlike $\mathbb{R}$ and $\mathbb{C}$ it has **countable** number of elements, i.e. each number in $\mathbb{Q}$ can be assigned an index $1, 2, 3, \ldots$ [1].

Challange 2.1 $\mathbb{Q}$ as a field

Prove that $\mathbb{Q}$ (together with the usual addition and product operation) is indeed a field.

?

[1] For proof, see ...

2.1.2 Finite fields

While all three examples of fields we encountered so far have each an infinite number of elements, some fields only have a finite number of elements (called their **order**). For example, consider the set $S = \{0, 1, a, b\}$ and the addition and product operations described using the following tables (left table describes addition, right table describes multiplication):

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

By examining the tables above, several points become clear:

- all the possible combinations of operands in both addition and multiplication give elements from S itself, meaning that the set is closed under both these operations.
- both tables are symmetric around their main diagonal, meaning that both addition and multiplication are commutative operations.
- in the addition table, the first row and first column both show that $x + 0 = x$ for any $x \in S$, meaning that 0 is the additive identity in S.
- in the product table, the second row and second column both show that $x \cdot 1 = x$ for any $x \in S$, meaning that 1 is the multiplicative identity in S.
- in the addition table, the element 0 appears in each row and each column exactly once. This means that every element x has a single additive inverse $y \in S$.
- in the product table, the element 1 appears in each row and each column exactly once, except for the first row and first column. This means that every element $x \neq 0$ has a single multiplicative inverse $z \in S$.

We therefore only need to prove two points to show that S is a field together with the operations described by the above tables: associativity of both operations and distributivity of multiplication over addition. We leave these proofs as a challange to the reader. Such a field is sometime denoted as $\mathbb{F}_4$. There are, of course, infinitely many finite fields.

2.1.3 Modulo fields

Another example of finite fields are sets of integers of the form $\{0, 1, 2, 3, \ldots, n\}$ where n is a prime, together with **modular addition** and **modular product**. To understand modular arithemetics, we recall the fact that on a circle, an angle can have a negative value but also greater than 360° values are possible (see Figure 0.3): 390° is equivalent to 30°, −30° is equivalent to 330°, etc. The set of integer values $0°, 1°, 2°, \ldots, 359°$ on a

circle is an example of a modular set: if for example we add together two angles of values deg 100 and 300° we get the equivalent angle deg 60. If we subtract deg 300 from deg 100 the result is an angle of deg 160.

We say that on a circle, the values $360°, 720°, -360°$ etc. are all **cungruent** to 0 modulo 360. In mathematical notation we represent this fact as e.g.

$$720 \equiv 0 \pmod{360}. \tag{2.1.1}$$

Note that from this point forward we drop the degrees unit, and deal with pure integers. The notation for the set $\{0, 1, 2, \ldots, 359\}$ is $\mathbb{Z}_{360}$. Generally speaking, the set $\{0, 1, 2, \ldots, n\}$ is denoted as $\mathbb{Z}_n$.

Note 2.1 About modulo set notation

It is not common to use the notation $\mathbb{Z}_n$ for the modulo-n set, since it is also used for a different algebraic construct, namely the n-adic ring. However, due to the simplicity of the notation, and the fact that we don't discuss rings in this chapter we are using it in this book. Common notations for the set are $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/n$.

Addition and multiplication on $\mathbb{Z}_n$ is done by the following rather straight forward definition:

Definition 2.2 Operations in $\mathbb{Z}_n$

In the set $\mathbb{Z}_n$ addition and multiplication are defined as the following:

- **Addition**: For any two elements $a, b \in \mathbb{Z}_n$, $a + b := (a + b) \pmod{n}$.
- **Multiplication**: For any two elements $a, b \in \mathbb{Z}_n$, $a \cdot b := (a \cdot b) \pmod{n}$.

Example 2.1 Operations in $\mathbb{Z}_n$

The tables below show addition and multiplication results of numbers in different modulo sets $\mathbb{Z}_n$ for some values of n:

n	$2+3$	$2\cdot 3$
4	1	2
5	0	1
6	5	0
7	5	6
8	5	6
9	5	6
10	5	6
11	5	6

n	$4+7$	$4\cdot 7$
8	3	4
9	2	1
10	1	8
15	11	13
20	11	8
27	11	1
28	11	0
30	11	28

Figure 2.1 shows the equivalency between integers and the elements of $\mathbb{Z}_5$.

Only the sets $\mathbb{Z}_n$ for which n is a prime number are also fields. Let's define this

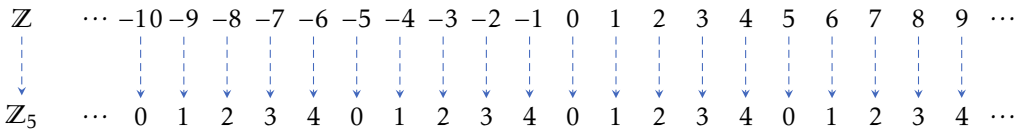


Figure 2.1 An example of the periodicity of $\mathbb{Z}_5$: the top numbers are the ordinary integers, each showing their respective congruent modulo 5 below (blue dashed arrow).

property precisely:

Theorem 2.3 $\mathbb{Z}_p$ is a field

Any modulo set $\mathbb{Z}_p$ where p is a prime number greater than 1 is also a field together with the operations as defined in 2.2.

In order to prove 2.3 we use two lemmas: the first is known as **Bézout's lemma**:

Lemma 2.1 Bézout's lemma

For any two positive integers a, b there exist two integers x, y such that

$$\gcd(a,b) = xa + yb.$$

Note 2.2 $\gcd(a,b)$

$\gcd(a,b)$ is the **greatest common devisor** of the two integers a and b. For example, $\gcd(36,24) = 12$ since the divisors of 36 are 1, 2, 3, 4, 6, 9, 12, 18, 36, and the divisors of 24 are 1, 2, 3, 4, 6, 8, 12, 24.

An example of Bézout's lemma is the following:

Example 2.2 Bézout's lemma in action

For the two positive integers $a = 60,\ y = 114$

$$\gcd(60,114) = 6.$$

Therefore, Bézout's lemma says that there exist two integers x, y such that

$$6 = 60x + 114y.$$

Indeed, two such integers exist: $x = 2$ and $y = -1$.

(SHOULD WE PROVE THE LEMMA?..)

The second lemma we use is the following:

Lemma 2.2 $\gcd(n, p, =) 1$

Given a positive prime number p, then for any positive integer $n < p$,

$$\gcd(p, n) = 1.$$

Proving the lemma:

Proof 2.2 $\gcd(n, p, =) 1$

We assume that $\gcd(p, n) \neq 1$. Then there exist an integer $a \leq n < p$ which divides both n and p, meaning that p has a divider, contrary to the suumption that p is a prime number. Therefore $\gcd(n, p)$ must equal 1.

QED

Now we can proceed to the proof of 2.3:

Proof 2.3 $\mathbb{Z}_p$ **is a field**

- **Closure under both operations**: The definition of the modulo operator limit any $M \pmod p$ (where $M \in \mathbb{Z}$) to be in $[0, p-1]$. Therefore the result of using the operators given in 2.2 must be within the same range, and thus in $\mathbb{Z}_p$.

- **Commutativity and associativity of both operations**: For any two numbers $a, b \in \mathbb{Z}_p$ the result $a + b$ and $a \cdot b$ under $\mathbb{Z}$ is both commutative and associative. Therefore the result modulo n is the same no matter the order of operations.

- **Additive identity**: The number $0 \in \mathbb{Z}_p$ is the additive identity, since for each $a \in \mathbb{Z}_p$, $a + 0 = a$.

- **Multiplicative identity**: The number $1 \in \mathbb{Z}_p$ is the additive identity, since for each $a \in \mathbb{Z}_p$, $a \cdot 1 = a$.

- **Additive inverse**: ...

- **Multiplicative inverse**: ...

- **Distributivity of multiplication over addition**: ...

QED

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.