1 Introduction to rigorous mathematics

Chapter contents

1.1 Sets and number systems

It is surprisingly subtle to give good axiomatic presentations of the intuitive concepts of set and element, which is why set theory is still an active branch of research in the 21-st Century.

We will instead rely on our naive grasp of these concepts. In short, a *set* S is a collection of things that we call the *elements* of S.

Sets are *unordered* collections, by which we mean that the order in which the elements are listed does not matter: $\{1, 3, 2\}$ is considered to be the same set as $\{2, 1, 3\}$.

The notation $s \in S$ signifies that s is an element of S.

What kind of "things" can be elements of sets? Pretty much anything, **including sets themselves** (that is, a set can be an element of another set).

Example 1.1.

$$\begin{aligned}
\varnothing &= \{\} \\
\text{Lecturers} &= \{\text{Alex}\} \\
\text{Students} &= \{\text{Yuening, Ryan, } \ldots, \text{ Qiyun, Roy}\} \\
\text{Tutors} &= \{\text{John, Kwan Sheng, Yuyang}\} \\
\text{PeopleSets} &= \{\text{Lecturers, Students, Tutors}\} \\
\text{Suits} &= \{\clubsuit, \blacklozenge, \heartsuit, \spadesuit\} \\
\text{SomeSets} &= \{\varnothing, \text{PeopleSets}, \text{Suits}\}
\end{aligned}$$

We say that a set S is a *subset* of a set T if and only if every element of S is also an element of T, that is

$$\text{for all } s \in S \text{ we have } s \in T.$$

This is written as $S \subseteq T$.

Example 1.2.

$$\{\text{Yuening, Ryan, Qiyun}\} \subseteq \text{Students}$$
$$\{\blacklozenge, \heartsuit, \text{✈}\} \not\subseteq \text{Suits}$$
$$\{\clubsuit\} \subseteq \text{Suits}$$

Note however that it does **not** make sense to write $\clubsuit \subseteq$ Suits because:

The correct notation here is:

We say that a set S is *equal to* a set T if and only if $S \subseteq T$ and $T \subseteq S$; or, equivalently, if and only if

$$s \in S \qquad \text{if and only if} \qquad s \in T.$$

The notation $S \subsetneq T$ means that $S \subseteq T$ and $S \neq T$ (we say that S is a *proper subset* of T). Not to be confused with $S \not\subseteq T$.

1.1.1 Specifying subsets

Describing subsets by enumerating the elements is at best tedious and at worst impossible (for infinite subsets).

A common method for specifying a subset A of a set X takes the form

$$A = \{x \in X : \ P(x)\},$$

where P is a property that elements of X can have; that is, for each $x \in X$, $P(x)$ is either true or false.

Example 1.3. If $\mathbf{N} = \{0, 1, 2, 3, 4, \dots\}$ denotes the set of natural numbers, we can define

$$\text{Even} =$$
$$\text{Odd} =$$

The specification of a subset can be well-formed (that is, make mathematical sense) even if the property P holds for **all** of the elements of X, or for **none** of the elements of X:

$$\{n \in \mathbf{N} : \ n + 1 \in \mathbf{N}\} =$$
$$\{n \in \mathbf{N} : \ n + \pi \in \mathbf{N}\} =$$

1.1.2 Operations on sets

Here we assume that all the sets we consider are subsets of a fixed set X.

Union If A and B are sets, then their *union* is

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

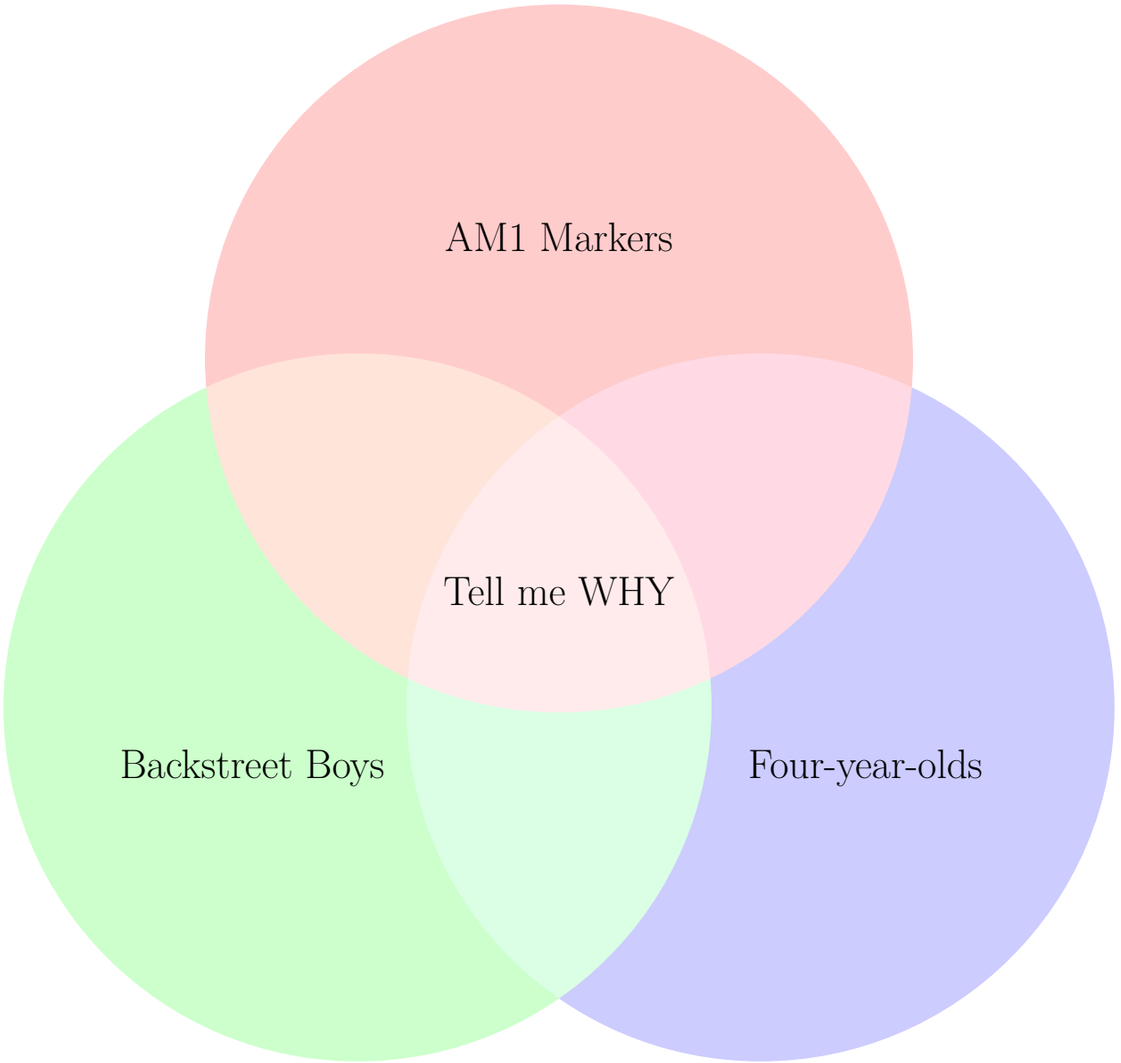
Intersection If A and B are sets, then their *intersection* is

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

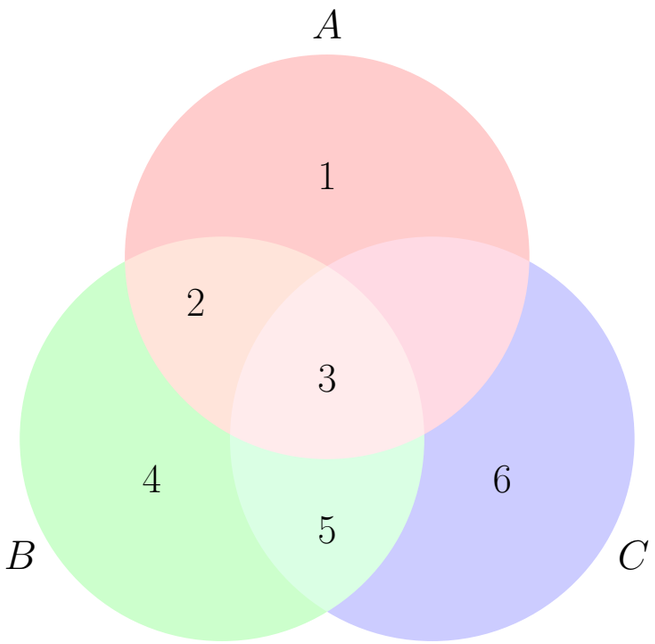
Difference If A and B are sets, then the *difference* $A \setminus B$ is

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

Example 1.4 (Everybody ♥ Venn diagrams)**.**



Example 1.5 (Everybody ♥ Venn diagrams)**.**
Let $A = \{1, 2, 3\}$, $B = \{2, 3, 4, 5\}$, $C = \{3, 5, 6\}$.



$A \cup B =$

$A \cap B =$

$A \setminus B =$

$(A \cap C) \setminus B =$

(Cartesian) product Let A and B be sets. Their *Cartesian product* is the set of all pairs:

$$A \times B = \{(a, b) : \ a \in A, b \in B\}.$$

Example 1.6. If $A = \{1, 3, 5\}$ and $B = \{\alpha, \beta\}$, then

$$A \times B =$$
$$B \times A =$$

Example 1.7.

$$\mathbf{R} \times \mathbf{R} =$$

This can be extended to the product of more than two sets:

$$S_1 \times S_2 \times \cdots \times S_n =$$

1.1.3 Numbers

Kronecker: "Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk."

There is actually an axiomatic treatment of *natural numbers* (due to Peano), but we will take them as given:

$$\mathbf{N} = \{0, 1, 2, 3, 4, 5, \ldots, 196785219, 196785220, \ldots\}$$

A natural operation on $\mathbf{N}$ is addition. This leads one to consider equations of the form

$$x + 3 = 5$$
$$x + 6 = 5$$

We can resolve this difficulty by enlarging our notion of number. Define the *set of integers* $\mathbf{Z}$ as pairs

$$\mathbf{Z} = \{(a, b) : \ a \in \mathbf{N}, b \in \mathbf{N}\}/\sim, \quad \text{where we declare} \quad (a, b) \sim (c, d) \quad \text{if } a + d = b + c.$$

But, 100% of the time, we think of the integer $(a, b) \in \mathbf{Z}$ in more conventional terms as $a - b$, and therefore write

$$\mathbf{Z} = \{\ldots, -196785220, -196785219, \ldots, -2, -1, 0, 1, 2, \ldots, 196785219, 196785220, \ldots\}.$$

Now we can solve **any** equation of the form

$$x + b = a \qquad \text{given } a, b \in \mathbf{Z}.$$

But $\mathbf{Z}$ also has another natural operation, namely multiplication. This leads one to consider equations of the form

$$3x = -6$$
$$3x = -5$$

We can enlarge our notion of number yet again. Define the *set of rational numbers* $\mathbf{Q}$ as pairs

$$\mathbf{Q} = \{(a,b) : \ a \in \mathbf{Z}, b \in \mathbf{Z} \setminus \{0\}\}/\sim, \quad \text{where we declare} \quad (a,b) \sim (c,d) \quad \text{if } ad = bc.$$

We always think of the rational number $(a,b) \in \mathbf{Q}$ in more conventional terms as the fraction $\frac{a}{b}$, and therefore write

$$\mathbf{Q} = \left\{ \frac{a}{b} : \ a \in \mathbf{Z}, b \in \mathbf{Z} \setminus \{0\} \right\}.$$

Now we can solve any equation of the form

$$qx = p \qquad \text{given } p \in \mathbf{Q}, q \in \mathbf{Q} \setminus \{0\}.$$

But multiplication also leads to equations of the form

$$x^2 = \frac{9}{4}$$
$$x^2 = 2$$

We introduce more numbers to fix this issue. The *set of real numbers* $\mathbf{R}$ is defined as the set of all (finite) limits of convergent sequences of rational numbers.

This allows us to solve any equation of the form

$$x^2 = a \qquad \text{given } a \in \mathbf{R}_{\geqslant 0},$$

but not equations such as

$$x^2 = -1.$$

This last problem gets sorted by introducing formal solutions $\pm i$ of this equation, giving rise to the *set of complex numbers* $\mathbf{C}$ (more about these later).

The upshot is a sequence of nested sets:

$$\mathbf{N} \subsetneq \mathbf{Z} \subsetneq \mathbf{Q} \subsetneq \mathbf{R} \subsetneq \mathbf{C},$$

each of which has arithmetic operations.

There are other number systems that are obtained by different mechanisms.

We single out one of these: as a set, it is given by

$$\mathbf{F}_2 = \{\hat{0}, \hat{1}\},$$

with addition and multiplication defined by

CAVEAT: $\mathbf{F}_2$ is **NOT** a subset of $\mathbf{N}$ (or $\mathbf{Z}$, or $\mathbf{Q}$, or $\mathbf{R}$, or $\mathbf{C}$).

1.2 Complex numbers: prerequisites

Editorial note: This section (Page 16–Page 25) contains a summary of what we expect (hope) that you already know about complex numbers. This is included for your reference; you may want to scan it quickly and double-check that it is all familiar.

1.2.1 Introduction to complex numbers

A *complex number* (generally denoted z) is a quantity consisting of a real number added to a real multiple of the number i. That is:

$$z = x + iy, \qquad \text{where } x, y \in \mathbf{R} \text{ and } i^2 = -1.$$

- x is called the *real part* of z and is denoted $\mathrm{Re}(z)$;
- y is called the *imaginary part* of z and is denoted $\mathrm{Im}(z)$.

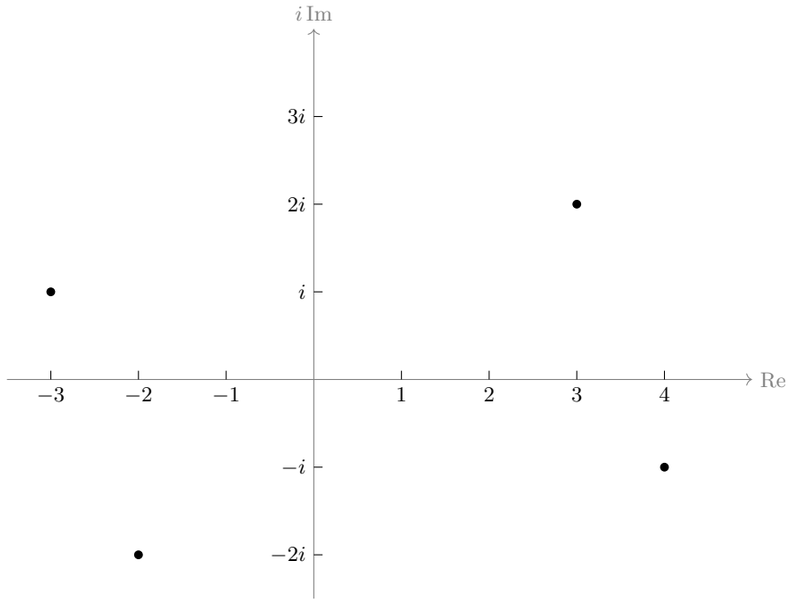
The set of all complex numbers is denoted $\mathbf{C}$.

A complex number written in the form $z = x + iy$ is said to be in *cartesian form*.

Note that the set of real numbers $\mathbf{R}$ is a subset of the set of complex numbers $\mathbf{C}$. (Why?)

1.2.2 The complex plane

Complex numbers can be represented graphically in the *complex plane*. We regard the complex number $z = x+iy$ as corresponding to a point in the plane, where the horizontal axis is now called the *real axis* and corresponds to the real part of z, while the vertical axis is the *imaginary axis* and corresponds to i times the imaginary part of z.



1.2.3 Arithmetic of Complex Numbers

Let $z_1 = a + ib$ and $z_2 = c + id$ be complex numbers.

Equality: The complex numbers z_1 and z_2 are equal if and only if

$$\mathrm{Re}(z_1) = \mathrm{Re}(z_2) \qquad \text{and} \qquad \mathrm{Im}(z_1) = \mathrm{Im}(z_2).$$

Addition: We add z_1 and z_2 as follows:

$$z_1 + z_2 = (a + ib) + (c + id) = (a + c) + i(b + d).$$

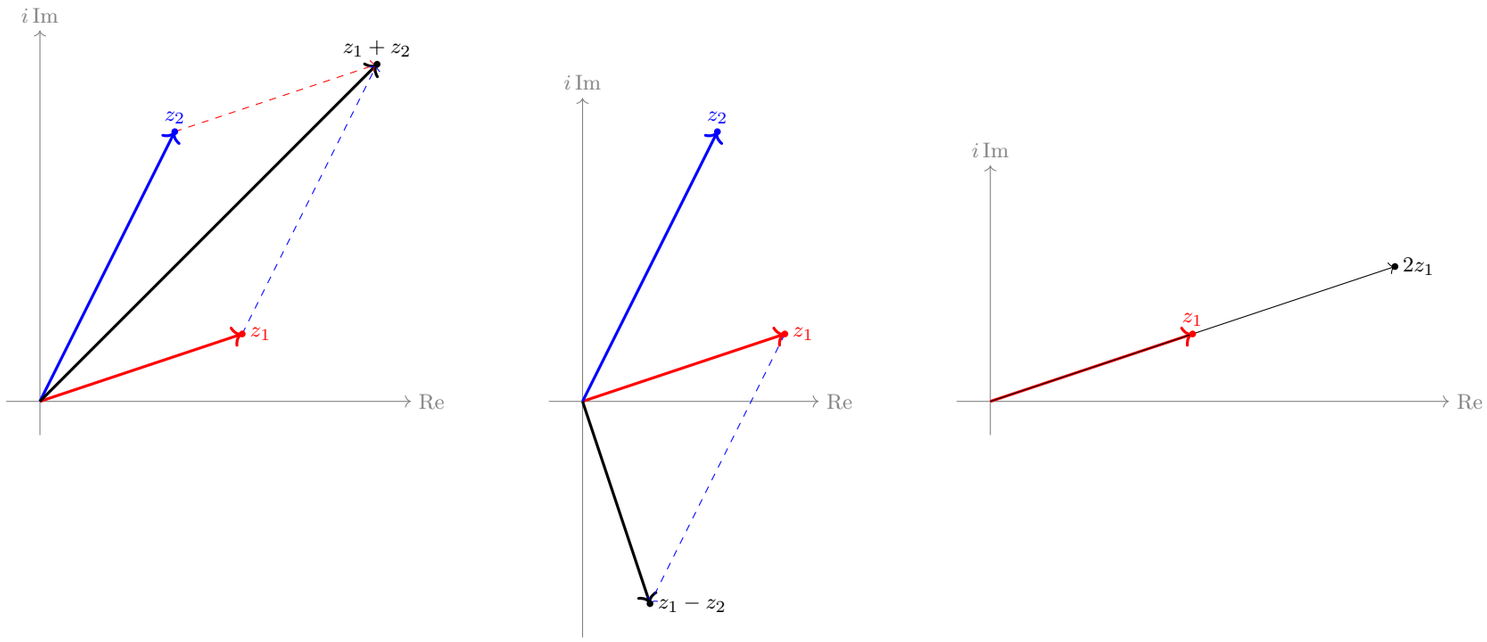
Subtraction: We subtract z_2 from z_1 as follows:

$$z_1 - z_2 = (a + ib) - (c + id) = (a - c) + i(b - d).$$

Multiplication by $k \in \mathbf{R}$: We multiply z_1 by $k \in \mathbf{R}$ as follows:

$$kz_1 = k(a + ib) = (ka) + i(kb).$$

Complex addition, subtraction, and multiplication by a real number can be represented geometrically in the complex plane, and should remind you of vector arithmetic.



Multiplication of complex numbers We multiply complex numbers by simply 'expanding the brackets', remembering that $i^2 = -1$:

$$\begin{aligned} z_1 z_2 &= (a + ib)(c + id) \\ &= ac + aid + ibc + ibid \\ &= (ac - bd) + i(ad + bc). \end{aligned}$$

The complex conjugate If $z = a + ib$ is a complex number, then the *complex conjugate* of z is denoted $\bar{z}$ (pronounced "z bar"), and is defined to be

$$\bar{z} = a - ib.$$

That is, the real part stays the same and the imaginary part changes sign.

Division of complex numbers Suppose we want to divide two complex numbers:

$$\frac{a+ib}{c+id}. \tag{1}$$

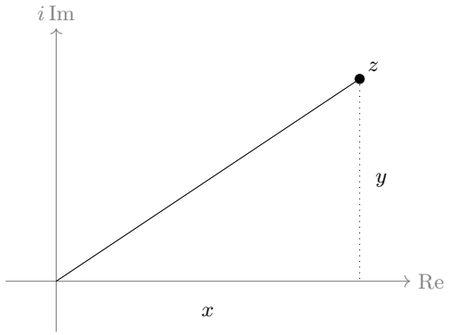
In order to get an answer in the form $x+iy$ we need to make the denominator real. To do so, we can make use of the fact that a complex number multiplied by its conjugate is real. So, we simply multiply top and bottom of Equation (1) by the complex conjugate of the denominator:

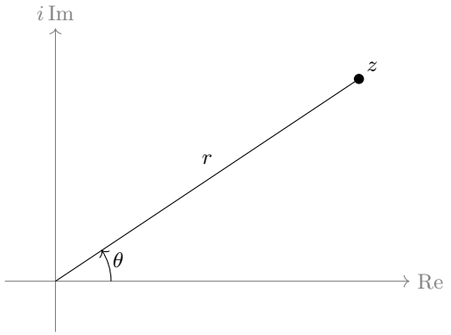
$$\begin{aligned}\frac{a+ib}{c+id} &= \frac{a+ib}{c+id} \times \frac{c-id}{c-id} \\ &= \frac{(ac+bd)+i(bc-ad)}{c^2+d^2} \\ &= \frac{ac+bd}{c^2+d^2} + i\,\frac{bc-ad}{c^2+d^2}\end{aligned}$$

1.2.4 Modulus and Argument

The position of a complex number z in the complex plane can be specified in two different ways:

- by its real and imaginary parts x and y, such that $z = x + iy$;
- by its distance r from the origin, and the angle θ from the positive real axis.

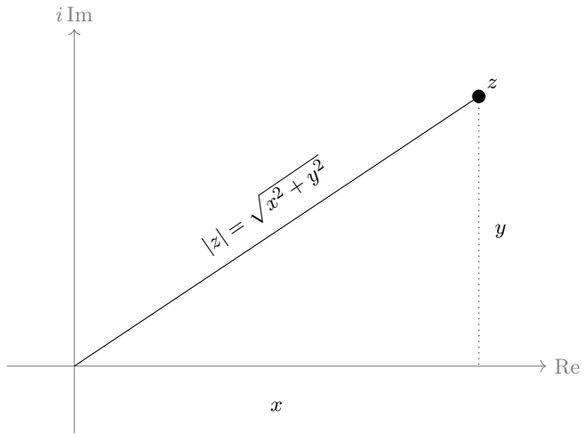




The *modulus* of z, denoted $|z|$, is the distance r from z to the origin in the complex plane.

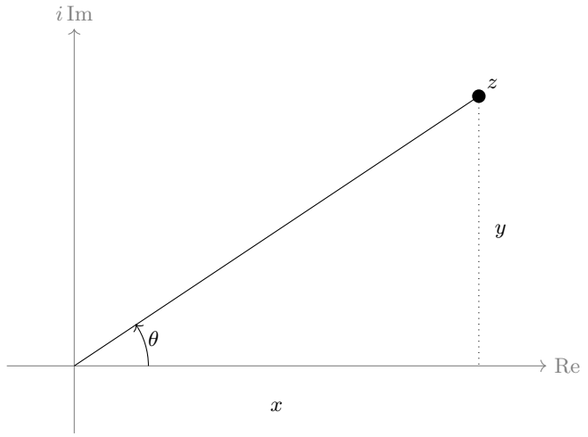
Writing $z = x + iy$, we can find $|z|$ by Pythagoras:

$$|z| = \sqrt{x^2 + y^2}.$$



The *argument* of z, denoted $\arg(z)$, is the angle θ that z makes with the positive real axis in the complex plane.

To determine the argument of a complex number $z = x + iy$, draw z in the complex plane and use standard triangles if possible to determine $\theta = \arg(z)$.



If θ is not a standard angle, we may note that

$$\tan(\theta) = \frac{y}{x}.$$

If θ is in the first or fourth quadrant we may conclude $\theta = \arctan(\frac{y}{x})$.
(Recall that the range of arctan is $(-\frac{\pi}{2}, \frac{\pi}{2})$.)

Caution The argument of z is not unique, since adding multiples of 2π does not change the position of z in the complex plane.

However, there is only one value of the argument that satisfies

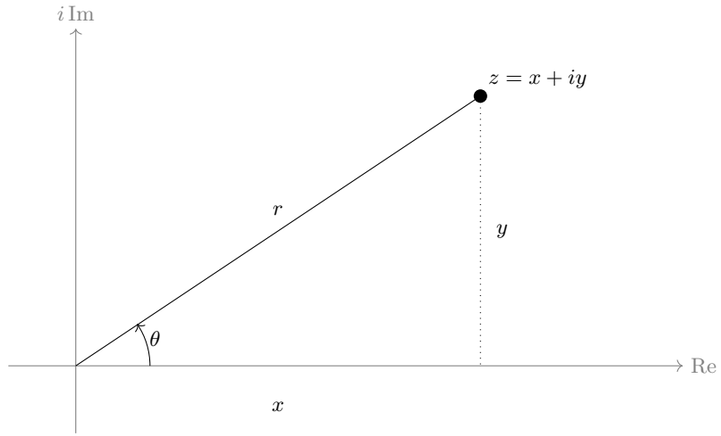
$$-\pi < \theta \leqslant \pi.$$

This is called the *principal argument* of z and is sometimes denoted $\mathrm{Arg}(z)$ with a capital A.

1.3 Complex numbers: the sequel

1.3.1 Polar Form and Complex Exponential

Recall that any complex number $z = x + iy$ can be specified by its modulus r and argument θ.



From the diagram above, we see that

$$\cos\theta = \qquad \text{and} \qquad \sin\theta =$$

$$\Rightarrow \quad x = \qquad \text{and} \qquad y =$$

Substituting these back into z we obtain

$$\begin{aligned} z &= x + iy \\ &= r\cos\theta + i\, r\sin\theta \\ &= r\left(\cos\theta + i\sin\theta\right). \end{aligned}$$

This last expression is called the *polar form* of the complex number z.

There is a very useful way of writing the polar form of a complex number.

The *complex exponential* $e^{i\theta}$ is defined to be

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

We can now write a complex number z in *exponential polar form*

$$z = re^{i\theta},$$

where $r = |z|$ and $\theta = \arg(z)$.

Properties of the complex exponential Using the definition of the complex exponential and basic properties of trigonometric functions, it is fairly straightforward to obtain the following:

1. $e^{i0} = 1$

2. $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$

3. $\dfrac{e^{i\theta_1}}{e^{i\theta_2}} = e^{i(\theta_1-\theta_2)}$

Notice that these properties are consistent with the usual index laws for working with exponentials (and so are easy to remember!).

We generally work with the exponential polar form $re^{i\theta}$ instead of the trigonometric polar form $r(\cos\theta + i\sin\theta)$.

If we have two complex numbers

$$z_1 = r_1 e^{i\theta_1} \qquad \text{and} \qquad z_2 = r_2 e^{i\theta_2},$$

we conclude that their product is given by

$$z_1 z_2 =$$

Interpreting this geometrically shows that the product of two complex numbers in polar form is obtained by multiplying their moduli and adding their arguments:

$$|z_1 z_2| =$$
$$\arg(z_1 z_2) = \qquad .$$

Consider two complex numbers written in polar form:

$$z_1 = r_1 e^{i\theta_1} \qquad \text{and} \qquad z_2 = r_2 e^{i\theta_2} \neq 0.$$

Then

$$\frac{z_1}{z_2} =$$

The geometric interpretation is that the quotient of two complex numbers in polar form is obtained by dividing their moduli and subtracting their arguments:

$$\left|\frac{z_1}{z_2}\right| =$$

$$\arg\left(\frac{z_1}{z_2}\right) =$$

1.3.2 Powers of complex numbers

Let $z = re^{i\theta}$. *De Moivre's Theorem* states that for any integer n:

$$z^n = r^n e^{in\theta}.$$

This formula is consistent with the usual exponent laws

$$z^n =$$

De Moivre's Theorem can be used to avoid expanding the brackets when finding large powers of complex numbers. For instance:

$$(1 + i\sqrt{3})^8 =$$

1.3.3 Nasty trigonometric identities via the complex exponential

First note the *binomial formula*

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j,$$

where $\binom{n}{j}$ is the $(j+1)$-st number in the $(n+1)$-st row of *Pascal's triangle*:

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 2 & & 1 & \\ 1 & & 3 & & 3 & & 1 \end{array}$$

Each entry is obtained by summing the two entries above it in the previous row, in other words:

$$\binom{0}{0} = \qquad \binom{0}{j} = \qquad \text{for all } j \neq 0, \quad \binom{n}{j} = \qquad\qquad\qquad \text{for all } n \geqslant 1.$$

Note: To expand $(a-b)^n$, regard it as $\big(a+(-b)\big)^n$.
This means that the signs of the terms will alternate $+, -, +, -, \ldots$

For example:

$$(a+b)^5 =$$

$$(a-b)^5 =$$

We also make the following observation regarding $\cos(n\theta)$ and $\sin(n\theta)$.

Since

$$e^{in\theta} = \cos(n\theta) + i\sin(n\theta),$$

we have

$$\cos(n\theta) =$$

$$\sin(n\theta) =$$

Example 1.8. Express $\cos(3\theta)$ as a polynomial in $\cos\theta$.

Here is another way of relating trigonometric functions to complex exponentials:

$$\cos\theta = \frac{1}{2}\left(e^{i\theta} + e^{-i\theta}\right)$$
$$\sin\theta = \frac{1}{2i}\left(e^{i\theta} - e^{-i\theta}\right)$$

Example 1.9. Prove that

$$\sin^3\theta = \frac{3}{4}\sin\theta - \frac{1}{4}\sin(3\theta).$$

1.3.4 Solving polynomial equations in C

Theorem 1.10 (Fundamental Theorem of Algebra)**.** *Any polynomial of degree n with complex coefficients has n complex roots (counted with multiplicity).*

How do we actually find these roots?

Let's start with the special case of solving for z in

$$z^n = w,$$

where $n \in \mathbf{N}$ and $w \in \mathbf{C}$ is a fixed, given complex number.

Example 1.11. Find all complex solutions of $z^3 = 1$.

Example 1.12. Find the fourth roots of $-1 + i\sqrt{3}$.

The general case $z^n = w$ is treated in the same fashion:

Let $z = re^{i\theta}$ and $w = se^{i\phi}$ be the respective exponential polar forms. The equation becomes

$$\begin{aligned} & (re^{i\theta})^n = se^{i\phi} \\ \Rightarrow \qquad & r^n e^{in\theta} = se^{i\phi} \end{aligned}$$

Equating the modulus and argument gives

$$\begin{array}{lll} r^n = s & \text{and} & e^{in\theta} = e^{i\phi} \\ \Rightarrow \quad r = s^{\frac{1}{n}} & & \Rightarrow \quad n\theta = \phi + 2k\pi, \qquad k \in \mathbf{Z} \\ & & \Rightarrow \quad \theta = \dfrac{1}{n}(\phi + 2k\pi), \qquad k \in \mathbf{Z}. \end{array}$$

Therefore, the n-th roots of $w = se^{i\phi}$ are:

$$w^{\frac{1}{n}} = s^{\frac{1}{n}}\, e^{i(\frac{1}{n}(\phi+2k\pi))} \qquad \text{for } k = 0, 1, \ldots, n-1.$$

Notes:

1. Observe that $k = 0, 1, \ldots, n-1$ gives n different n-th roots of w. We stop at $n-1$ since for $k = n$ we would be adding a whole multiple of 2π to the argument, which would give the same complex number as $k = 0$.

2. You do **not** need to memorise the formula above. It is easy to derive the n-th roots of a complex number w by starting with $z^n = w$, expressing w in exponential polar form and solving for z.

In the case of a general complex polynomial

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0,$$

we have

- $c \in \mathbf{C}$ is a root of p (that is $p(c) = 0$) if and only if $(z - c)$ is a factor of $p(z)$.
- the Fundamental Theorem of Algebra tells us that $p(z)$ factors into linear terms:

  $$p(z) = a_n (z - c_1)(z - c_2) \ldots (z - c_n)$$

  with $c_i \in \mathbf{C}$.
- if p has **real coefficients** and $c \in \mathbf{C}$ is a root of p, then the complex conjugate $\overline{c}$ is also a root of p.

Example 1.13. Solve

$$z^4 - 2z^2 + 4 = 0.$$

Example 1.14. Let $k \in \mathbf{N}$. Solve

$$z^k + z^{k-1} + \cdots + z + 1 = 0.$$

1.4 Proof techniques

We explore various types of proofs by observing them in action. Note that a particular statement will often have more than one proof, and these can be of very different types.

Example 1.15 (Direct proof)**.** Let n be an integer. If n is odd then n^2 is odd.

It is essential to know the mathematical meaning of each word in a statement. In our case, we need to remember the definition of *odd integer*: $n \in \mathbf{Z}$ is odd if and only if there exists $k \in \mathbf{Z}$ such that $n = 2k + 1$.

Example 1.16. Let n be an integer. If n^2 is even, then n is even.

There's a rather clear logical connection between the statement in Example 1.15 and the one in Example 1.16:

Example 1.17 (Proof by contradiction)**.** If $x \in \mathbf{Q}$, then $x^2 \neq 2$.

This is often paraphrased as "$\sqrt{2}$ is irrational", but again we prefer the clearer version of the statement.

Example 1.18 (Geometric proof)**.** If a, b, c are the side lengths of a right triangle, with c the length of the side opposite the right angle, then

$$a^2 + b^2 = c^2.$$

Example 1.19 (Proof by contradiction)**.** The number of prime numbers is infinite.

Both the statement and its proof by Euclid (which we'll give below) require some basic terms from number theory.

Let $a, b \in \mathbf{Z}$. We say that *a divides b* if and only if there exists $c \in \mathbf{Z}$ such that

$$b = ac$$

There are a lot of synonyms for a divides b: $a \mid b$, a is a divisor of b, b is divisible by a, b is a multiple of a.

Example 1.20.

$$6 \mid 18, \qquad 6 \nmid 15, \qquad 6 \mid 0$$

Homework 1.21. If $a, b_1, b_2 \in \mathbf{Z}$ are such that a divides both b_1 and b_2, then a divides $b_1 + b_2$ and $b_1 - b_2$.

We say that $n \in \mathbf{N}$ is *prime* if and only if it has exactly two positive divisors (namely 1 and n).

So 1 is not a prime, but the following are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$$

We will need a fact that we do not prove here: Every integer $n > 1$ has at least one prime divisor.

Euclid's Theorem can be generalised in many ways. Here is one of them: Any subset of $\mathbf{N}$ of the form $\{x = ak + b : \ k \in \mathbf{Z}\}$ with $\gcd(a, b) = 1$ contains infinitely many prime numbers. (This is referred to as "primes in arithmetic progressions" and the proof is beyond our scope.)

Counterexamples

Not every mathematical statement is true! The best way to show that a statement is **false** is to provide an *explicit counterexample*, that is an explicit case where the hypotheses of the statement are satisfied but the conclusion does not hold.

Example 1.22. In 1650, Fermat conjectured that

$$2^{2^n} + 1 \quad \text{is prime for all } n \in \mathbf{Z}_{\geqslant 0}.$$

Prove that this is false.

1.5 Functions

A *function* $f: A \longrightarrow B$ consists of

- a set A called the *domain* of f
- a set B called the *codomain* of f
- a rule f that specifies how to map each element $a \in A$ to an element $f(a) \in B$.

Example 1.23.

$$f: [1,2] \longrightarrow \mathbf{R} \qquad \text{given by} \qquad f(x) = \frac{1}{x}$$
$$g: \text{Students} \longrightarrow \mathbf{N} \qquad \text{given by} \qquad g(x) = \text{ID number of } x.$$

We say that two functions $f: A \longrightarrow B$ and $g: C \longrightarrow D$ are *equal* if and only if all of the following conditions are satisfied:

- Their domains are equal as sets: $A = C$.
- Their codomains are equal as sets: $B = D$.
- Their rules agree at every point of the domain: $f(x) = g(x)$ for all $x \in A$.

Example 1.24 (Three distinct functions)**.**

$$\begin{array}{rlll} f: & [1,2] \longrightarrow \mathbf{R} & \text{given by} & f(x) = \dfrac{1}{x} \\ g: & \mathbf{R} - \{0\} \longrightarrow \mathbf{R} & \text{given by} & g(x) = \dfrac{1}{x} \\ h: & \mathbf{R} - \{0\} \longrightarrow \mathbf{R} & \text{given by} & h(x) = \log(|x|). \end{array}$$

Example 1.25 (Two equal functions)**.**

$$\begin{array}{rlll} f: & \mathbf{R} \longrightarrow [0,\infty) & \text{given by} & f(x) = \\ g: & \mathbf{R} \longrightarrow [0,\infty) & \text{given by} & g(x) = \end{array}$$

Let $f : A \longrightarrow B$ be a function.

If for every $b \in B$ the equation $f(a) = b$ has

- has at most one solution, we say that f is *injective*; we normally prove this by verifying the equivalent condition

$$\text{for all } x, y \in A, \text{ if } f(x) = f(y) \text{ then } x = y;$$

- has at least one solution, we say that f is *surjective*; in other words

$$\text{for all } b \in B, \text{ there exists } a \in A \text{ such that } b = f(a);$$

- has exactly one solution, we say that f is *bijective*; equivalently, f is both injective and surjective.

The codomain is related to the notion of *range* of a function. If $f: A \longrightarrow B$, we define

$$\text{range}(f) = \{b \in B : \text{ there exists } a \in A \text{ such that } b = f(a)\}$$

Note that in algebra, the range is also called the *image* of f.

Clearly the range is always a subset of the codomain. The range is equal to the codomain if and only if f is surjective.

Example 1.26.

Given functions $f: A \longrightarrow B$ and $g: B \longrightarrow C$, we can form their *composition* $g \circ f: A \longrightarrow C$ by

$$(g \circ f)(x) = g(f(x)) \qquad \text{for all } x \in A.$$

For any set S, there is a special function called the *identity (function) on* S. It is denoted $\mathrm{id}_S: S \longrightarrow S$ and given by

$$\mathrm{id}_S(x) = x \qquad \text{for all } x \in S.$$

A function $f: A \longrightarrow B$ is *invertible* if and only if there exists a function $g: B \longrightarrow A$ such that

$$g \circ f = \mathrm{id}_A \qquad \text{and} \qquad f \circ g = \mathrm{id}_B .$$

Challenge: Prove that if a function g as above exists, then it is unique.

We are therefore justified in calling g ***the*** *inverse of* f and denoting it f^{-1}.

Proposition 1.27. *A function $f : A \longrightarrow B$ is invertible if and only if it is bijective.*

1.6 Counting

Mathematically, to count a set S means to produce a bijection between S and some "standard" set.

A set S is *finite* if and only if it is empty or there exists a bijection between S and $\{1, 2, \ldots, n\}$ for some $n \in \mathbf{N}$. If n exists, it is unique, and it is called the *cardinality (or size)* of S and denoted $\#S$.

A set S is *infinite* if and only if it is not finite.

A set S is *countable* if and only if there exists a bijection between S and $\mathbf{N}$ (or equivalently, between $\mathbf{N}$ and S).

A set S is *uncountable* if and only if S is infinite and not countable. (In other words, S is uncountable if and only if there are no bijective functions from S to $\mathbf{N}$ and no bijective functions from S to $\{1, \ldots, n\}$ for any $n \in \mathbf{N}$.)

Example 1.28. The set $\{\text{Alice}, \text{Bob}, \text{Charles}\}$

Example 1.29. The set $2\mathbf{N} = \{2k : \ k \in \mathbf{N}\} = \{0, 2, 4, 6, \dots\}$

Example 1.30. The set of integers $\mathbf{Z}$

Theorem 1.31 (Schröder–Bernstein)**.** *If A and B are sets and there exist injective functions $f : A \longrightarrow B$ and $g : B \longrightarrow A$, then there exists a bijection from A to B.*

Corollary 1.32. *The set of rational numbers* $\mathbf{Q}$ *is countable.*

Example 1.33. The set of real numbers $\mathbf{R}$ is

We'll use the following without proof:

Lemma 1.34. *If $A \subseteq B$ and A is uncountable, then B is uncountable.*

1.7 The principle of mathematical induction

Certain mathematical statements are actually infinite collections of statements indexed by the natural numbers, for instance:

For any $n \in \mathbf{N}$, the sum of the first n positive integers is $n(n+1)/2$.

This is made of:

The principle of mathematical induction I. Let $\{P(n) : n \in \mathbf{N}\}$ be a collection of mathematical statements. If

(a) $P(0)$ is true, and

(b) for all $k \in \mathbf{N}$, $P(k) \Longrightarrow P(k+1)$,

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

(A slight variant allows the starting point to be some $n_0 \in \mathbf{N}$, not restricted to $n_0 = 0$.)

The principle of mathematical induction is equivalent to the *least element property* of the natural numbers:

Every non-empty subset of $\mathbf{N}$ has a least element.

Example 1.35. For all $n \in \mathbf{N}$ we have

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Example 1.36. For any $n \geqslant 3$, the sum of the interior angles of an n-sided convex polygon is $(n-2)\pi$.

Principle of mathematical induction II. Let $\{P(n) : n \in \mathbf{N}\}$ be a collection of mathematical statements. If

(a) $P(0)$ is true, and

(b) for all $k \in \mathbf{N}$, $\Big(P(0)$ and $P(1)$ and$\ldots$ and $P(k)\Big) \Longrightarrow P(k+1)$,

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

This appears to be a **weaker** statement than Mathematical induction I (think about it!), but they are actually equivalent.

Example 1.37. Every integer $n \geqslant 2$ factors into a product of one or more prime numbers.

Example 1.38. If n is an odd integer then $n(n^2 - 1)$ is divisible by 24.

Example 1.39. For each $n \geqslant 1$, the number c_n of ways of cutting a stick of length n into pieces of integer length is 2^{n-1}.

Experiment:

1.8 Inequalities

In addition to its arithmetic operations and their properties, the set of real numbers $\mathbf{R}$ has the structure given by the order relation denoted $a > b$. This satisfies:

(P1) If $a > 0$ and $b > 0$ then $a + b > 0$ and $ab > 0$.

(P2) For every $a \in \mathbf{R}$, exactly one of the following statements is true: $a = 0$, $a < 0$, or $a > 0$.

Example 1.40. The square of any nonzero real number is positive.

Example 1.41. Find $n_0 \in \mathbf{N}$ such that $n^3 > (n+1)^2$ for all $n \geqslant n_0$.

[**Hint**: Add $3k^2 + 3k + 1$ to both sides of $k^3 > (k+1)^2$.]

Example 1.42. Find $n_0 \in \mathbf{N}$ such that $n! > n^3$ for all $n \geqslant n_0$.

[**Hint**: Reduce to the polynomial case by multiplying both sides of $k! > k^3$ by $(k+1)$.]