Chapter 3

Numbers

3.1 Some Prerequisites

You need to know the standard notation for natural numbers, $\mathbb{N} = \{1, 2, 3, \ldots\}$ the integers, $\mathbb{Z} = \{\ldots, -3, -2 - 1, 0, 1, 2, 3, \ldots\}$, and the rational numbers, $\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z} \wedge q \in \mathbb{Z} - \{0\} \right\}$.

You also need to know what a prime number is, a LCM, a HCF, the meaning of coprime and the Prime Factorisation Theorem, how to write a fraction in decimal form using division, how to write a recurring decimal as a fraction. You should understand basic ideas and be able to express them using definitions from Set Theory, e.g. the natural numbers $\mathbb{N}$ do not possess a maximal element, understand that the rationals $\mathbb{Q}$ are **totally ordered** under the usual relation $\leq$.

3.2 Introduction

If we had 24 hours to devote to Analysis, we could start by defining the natural numbers, $\mathbb{N} = \{1, 2, 3, \ldots\}$ and then use them to construct the integers, $\mathbb{Z} = \{\ldots, -3, -2 - 1, 0, 1, 2, 3, \ldots\}$, the rational numbers, $\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z} \wedge q \in \mathbb{Z} - \{0\} \right\}$ and then finally the reals, $\mathbb{R}$.

We are going to assume the existence of $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ with the usual operations you are familiar with and then define the reals, $\mathbb{R}$. We shall not have time to prove the reals exist. We could construct the reals from the rationals, but we shall not have time for this construction.

We shall begin by getting reacquainted with decimal expansions.

3.3 Decimal Expansions

We are first going to look at decimal expansions. You know that $\frac{1}{5} = 0.2$ and $\frac{1}{3} = 0.\dot{3}$. We shall prove the following proposition.

Proposition 1. *Every rational number has a finite decimal expansion or an infinite recurring decimal expansion.*

Before going into the proof it will be useful to work out the decimal expansion of $\frac{56}{111}$.

Proof of Proposition 1. By definition, every rational number can be expressed in the form $\frac{p}{q}$ where p and q are integers and $q \neq 0$. We shall assume that the fraction is in its lowest terms (i.e., p and q are coprime). We can confine ourselves to $p, q > 0$, because the decimal expansion of the positive rational $\frac{p}{q} > 0$ can be turned into the decimal expansion of the negative rational $\frac{p}{q} > 0$ merely via multiplication by -1. We can also confine ourselves to $p < q$, because for $p > q$, we can write $\frac{p}{q} = N + \frac{p'}{q}$, where $N \in \mathbb{N}$ and $p' \in \mathbb{N}$ and $p' < q$.

Let us divide p by q. We know that because $p < q$, we start with $0.\cdots$ and to obtain the first entry after the decimal place, we need to find the smallest $n \in \mathbb{Z}^+$ such that $10^n p > q$. We then place $n-1$ zeros after the decimal place and consider $\frac{10^n p}{q}$. If the remainder is 0, then the decimal expansion terminates and is finite. Otherwise, we obtain the non-zero remainder r_1 via

$$\frac{p \times 10^n}{q} = a_1 + \frac{r_1}{q},$$

where r_1 which must belong to $\{1, 2, \ldots, q-1\}$ and $a_1 \in \{1, \ldots, 9\}$. We therefore have

$$\frac{p}{q} = 0.\underbrace{0\cdots0}_{n-1 \text{ zeros}}\, a_1 \cdots$$

and to see what comes after a_1 we need to find the first $n \in \mathbb{N}$ such that $10^n r_1 > q$ and compute $\frac{10^n r_1}{q}$:

$$\frac{10^n r_1}{q} = a_2 + \frac{r_2}{q}.$$

There are three possibilities:

1. If $r_2 = 0$, the decimal expansion terminates and is clearly finite.

2. $r_2 = r_1$, then we obtain a recurring decimal

$$\frac{p}{q} = 0.\underbrace{0 \cdots 0}_{\text{zeros}}\overline{a_1 \cdots a_2}$$

3. Otherwise, $r_2 = \{1, 2, \ldots, q-1\} - \{r_1\}$ and we consider the first $n \in \mathbb{N}$ such that $10^n r_2 > q$.

As before, we have three possibilities for the remainder r_3

1. $r_3 = 0$, the decimal expansion terminates and is clearly finite.

2. $r_3 = r_1$ or $r_3 = r_2$, and so we obtain a recurring decimal

3. $r_2 = \{1, 2, \ldots, q-1\} - \{r_1, r_2\}$ and we consider the first $n \in \mathbb{N}$ such that $10^n r_3 > q$.

We keep on executing the above loop.

Given that the number of possible remainders is finite, eventually a remainder must be 0 or repeated. When a zero remainder is obtained, then the the loop ends and the decimal expansion is finite. When a remainder is repeated, then we know how the loop will continue, allowing us to write down the recurring decimal expansion, which is infinite.

In conclusion, every rational number can be expressed either as a finite decimal or an infinite recurring decimal.

$\square$

3.4 Irrationality of $\sqrt{2}$

To get a sense of the rationals and why they fall short, we are going to investigate the number $x > 0$ such that $x^2 = 2$. You will be more familiar with x as $\sqrt{2}$.

3.4.1 Sandwiching $\sqrt{2}$ between rationals

We know that $1 < x^2 < 4$ and so $1 < x < 2$. We can do much better though and find much tighter inequalities than this. For instance, we know $10^2x^2 = 200$ and so $14^2 < 10^2x^2 < 15^2$. Therefore $14 < 10x < 15$ and so $1.4 < x < 1.5$. We can do even better!

$$\begin{aligned}
&141^2 < 100^2x^2 < 142^2\\
\Rightarrow &141 < 100x < 142\\
\Rightarrow &1.41 < x < 1.42
\end{aligned}$$

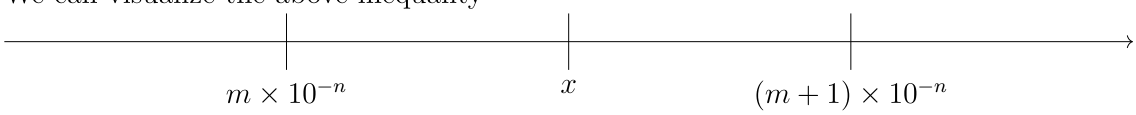
Now we are getting somewhere!

$$\begin{aligned}
&1414^2 < 1000^2x^2 < 1415^2\\
\Rightarrow &1414 < 1000x < 1415\\
\Rightarrow &1.414 < x < 1.415
\end{aligned}$$

In general we are doing the following for a given $n \in \mathbb{N}$: finding $m \in \mathbb{N}$ such that $m^2 < 10^{2n}x^2 < (m+1)^2$ and then going through the following steps:

$$\begin{aligned}
&m^2 < 10^{2n}x^2 < (m+1)^2\\
\Rightarrow &m < 10^n x < m+1\\
\Rightarrow &m \times 10^{-n} < x < (m+1) \times 10^{-n}
\end{aligned}$$

We can visualize the above inequality



Note that the distance between $m \times 10^{-n}$ and $(m+1) \times 10^{-n} \times 10^{-n}$ is 10^{-n} and so the maximum distance between $m \times 10^{-n}$ and x is strictly less than 10^{-n}, i.e.

$$x - m \times 10^{-n} < 10^{-n}.$$

Similarly,

$$(m+1) \times 10^{-n} - x < 10^{-n}.$$

Therefore, $|m \times 10^{-n} - x| < 10^{-n}$ and $|(m+1) \times 10^{-n} - x| < 10^{-n}$.

In the Exercises, you will use the above to write code to find arbitrarily tight bounds for $\sqrt{2}$ using finite decimal expansions. Note that as finite decimal expansions, the bounds are always rational.

3.4.2 Proving $\sqrt{2}$ is irrational

It seems like we can get arbitrarily close to $\sqrt{2}$ using rational numbers.* However, as you probably know, $\sqrt{2}$ is not rational, i.e. $\sqrt{2}$ is irrational. We shall prove this by a technique called reductio ad absurdum or proof by contradiction.

Proposition 2. $\sqrt{2} \notin \mathbb{Q}$

Proof. Proposition 2
We assume $\sqrt{2}$ is rational, i.e.

$$(\exists p, q \in \mathbb{N}) \left(HCF(p, q) = 1 \wedge \sqrt{2} = \frac{p}{q} \right).$$

We can see that

$$(\exists p, q \in \mathbb{N}) \left(HCF(p, q) = 1 \wedge 2q^2 = p^2 \right).$$

Therefore p^2 is even and so p is even. Hence,

$$(\exists r \in \mathbb{N})(2r = p).$$

But, $2q^2 = p^2$, and so

$$2q^2 = 4r^2 \Rightarrow q^2 = 2r^2.$$

We see that q^2 is even, which implies q is even. Therefore, p and q are both even which means they have a a common factor of 2, which violates our initial assumption. Therefore, our initial assumption is false and $\sqrt{2}$ is not a rational number.

$\square$

The underlying logic of the proof is important. We wanted to prove the statement P is true. We assumed the statement $\neg P$ (the opposite of the negation of P) was true and then derived a statement contradicting $\neg P$. We then concluded the statement P was true. This form of proof is called reductio ad absurdum or proof by contradiction.

We know that every finite decimal expansion e.g. 1.41 is a rational number, so we cannot express $\sqrt{2}$ as a finite decimal expansion, we can only approximate it. Interestingly, although there is an infinite decimal expansion of $\sqrt{2}$, it is not recurring. From the perspective of using computers to represent mathematical objects such as $\sqrt{2}$, we would like to find out how close we can get to $\sqrt{2}$ using a finite decimal expansion.

If we can get arbitrarily close to $\sqrt{2}$ using finite decimal representations, which are rational, but not actually represent $\sqrt{2}$ via a rational number, this means the set $\mathbb{Q}$ has gaps.

*Later when we study series and convergence, we shall make this intuition precise.

3.5 Defining the Reals

The set $\mathbb{Q}$ of rational numbers is incomplete. It has 'gaps', one of which occurs at $\sqrt{2}$. These gaps are really more like pinholes; they have zero width. Incompleteness is what is wrong with $\mathbb{Q}$. We could complete $\mathbb{Q}$ by filling in its gaps via what is known as a Dedekind cut and this would allow us to construct the reals. Instead, we shall take an axiomatic approach and define the reals.

3.5.1 Fields and the Field Axioms

Our starting point for defining the reals will be the idea of a field

Definition 5 (Field). *A field is a set $\mathbb{F}$ with two binary operations $+$ and $\times$ that satisfy the following properties or axioms:*

1. ***Closure under Addition:*** *For every $a, b \in \mathbb{F}$, $a + b \in \mathbb{F}$.*
2. ***Closure under Multiplication:*** *For every $a, b \in \mathbb{F}$, $a \times b \in \mathbb{F}$.*
3. ***Associative Law of Addition:*** *For every $a, b, c \in \mathbb{F}$, $(a+b)+c = a+(b+c)$.*
4. ***Associative Law of Multiplication:*** *For every $a, b, c \in \mathbb{F}$, $(a \times b) \times c = a \times (b \times c)$.*
5. ***Commutative Law of Addition:*** *For every $a, b \in \mathbb{F}$, $a + b = b + a$.*
6. ***Commutative Law of Multiplication:*** *For every $a, b \in \mathbb{F}$, $a \times b = b \times a$.*
7. ***Existence of Additive Identity:*** *There exists an element $0 \in \mathbb{F}$ such that for every $a \in \mathbb{F}$, $a + 0 = a$.*
8. ***Existence of Multiplicative Identity:*** *There exists an element $1 \in \mathbb{F}$ such that $1 \neq 0$ and for every $a \in \mathbb{F}$, $a \times 1 = a$.*
9. ***Existence of Additive Inverses:*** *For every $a \in \mathbb{F}$, there exists an element $-a \in \mathbb{F}$ such that $a + (-a) = 0$.*
10. ***Existence of Multiplicative Inverses:*** *For every $a \in \mathbb{F}$ with $a \neq 0$, there exists an element $a^{-1} \in \mathbb{F}$ such that $a \times a^{-1} = 1$.*
11. ***Distributive Law:*** *For every $a, b, c \in \mathbb{F}$, $a \times (b + c) = (a \times b) + (a \times c)$.*

We usually refer the axioms in the definition of a field as the field axioms.

Example 8. *In this example we look at the set $\{O, I\}$ and define addition, $+$, and multiplication, $\times$, on the elements of this set follows:*

$$\begin{aligned} O + O &= O \\ O + I &= I \\ I + O &= I \\ I + I &= O \end{aligned}$$

and

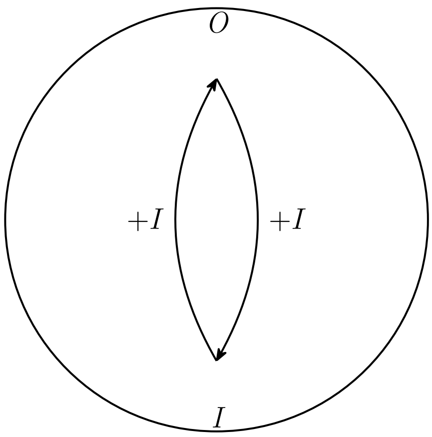
$$\begin{aligned} O \times O &= O \\ O \times I &= O \\ I \times O &= O \\ I \times I &= I \end{aligned}$$

We can check the set $\{O, I\}$ with addition, $+$, and multiplication, $\times$, defined as above forms a field – it is called the binary field and denoted by $\mathbb{F}_2$.

We can also see the definition $I + I = O$ implies that the additive inverse of I is I and we can represent this fact as $-I = I$. We can visualize how addition works in $\mathbb{F}_2$ by taking the following sequence

$$\underbrace{(-I)+(-I)+(-I)+(-I)}_{=O}, \underbrace{(-I)+(-I)+(-I)}_{=I}, \underbrace{(-I)+(-I)}_{=O}, \underbrace{-I}_{=I}, O, I, \underbrace{I+I}_{=O}, \underbrace{I+I+I}_{=I}, \underbrace{I+I+I+I}_{=O}$$

and representing it via the following clock-like diagram



It is important to note that $\mathbb{Z}$ is not a field: 2 does not have a multiplicative inverse within $\mathbb{Z}$. However, $\mathbb{Q}$ is a field.

We will give examples of how to prove fundamental properties you are highly familiar within the context of the real numbers. The proofs follows from the field axioms. The 'rule' behind writing out a proof is that you have to start with the assumptions, which you get from definitions. You cannot write down something you think is obvious without showing how it follows logically from the definitions – this is hard because at school you learnt how to use the field axioms automatically without thinking about them. An intelligent use of the Distributive Law is often key.

Lemma 1. *In a field $\mathbb{F}$, the additive identity satisfies the following property*

$$(\forall x \in \mathbb{F}) x \times 0 = 0.$$

Proof.

1. Start with the Distributive Law

$$(\forall a, b, c \in \mathbb{F}) a \times (b + c) = (a \times b) + (a \times c).$$

with $a = x$, $b = x$ and $c = 0$, and so

$$x \times (x + 0) = (x \times x) + (x \times 0)$$

2. We now use the Existence of Additive Identity

$$x + 0 = x$$

and so

$$\begin{aligned} x \times x &= (x \times x) + (x \times 0) \\ x^2 &= x^2 + (x \times 0) \end{aligned}$$

3. Use the Existence of Additive Inverses to see that $x^2 + (-x^2) = 0$ and Associativity of Addition together with Commutativity of Addition

$$\begin{aligned} x^2 + (-x^2) &= (x^2 + (x \times 0)) + (-x^2) \\ x^2 + (-x^2) &= ((x \times 0) + x^2) + (-x^2) \\ x^2 + (-x^2) &= (x \times 0) + (x^2 + (-x^2)) \\ 0 &= (x \times 0) + 0 \\ 0 &= (x \times 0) \end{aligned}$$

□

Lemma 2. *In a field $\mathbb{F}$, $(\forall x \in \mathbb{F})$, the additive inverse of x is $-1 \times x$, i.e.*

$$(\forall x \in \mathbb{F}) - x = -1 \times x.$$

Proof. Suppose $x \in \mathbb{F}$, where $\mathbb{F}$ is a field. Now

$$\begin{aligned} x + (-1 \times x) &= \overbrace{x \times 1}^{\text{multiplicative identity}} + \overbrace{x \times (-1)}^{\text{commutativity of } \times} \\ &= x \times (1 + (-1)), \text{Distributive Law} \\ &= x \times 0, \text{(-1) is the additive inverse of the multiplicative identity} \\ &= 0, \text{via Lemma 1.} \end{aligned}$$

Now we have just shown that $x + (-1 \times x) = 0$. Now, using the additive inverse of x, denoted by $-x$, have

$$(x + (-1 \times x)) + (-x) = -x \Rightarrow (x + (-1 \times x)) + (-x) \qquad = -x.$$

Now using the associativity of addition

$$x + ((-1 \times x) + (-x)) = -x.$$

Using the commutativity of addition, we have $(-1 \times x) + (-x) = (-x) + (-1 \times x)$, and so

$$x + ((-x) + (-1 \times x)) = -x.$$

Once again, using the associativity of addition

$$(x + (-x)) + (-1 \times x) = -x.$$

Finally, using the fact that -x is the additive inverse of x, we have

$$-1 \times x = -x.$$

□

Lemma 3. *The additive inverse of the multiplicative identity satisfies the following equation*

$$(-1)^2 = 1$$

Proof. 1. By definition the additive inverse of the multiplicative identity is (-1), where $1 + (-1) = 0$

2. Start with the Distributive Law

$$(\forall a, b, c \in \mathbb{F}) a \times (b + c) = (a \times b) + (a \times c).$$

with $a = -1$, $b = -1$ and $c = 1$, and so

$$(-1) \times ((-1) + 1) = (-1) \times (-1) + ((-1) \times 1)$$

3. Using the Commutativity of Addition, $1 + (-1) = 0 \iff (-1) + 1 = 0$ and using the Existence of Multiplicative Identity $(-1) \times 1 = -1$, and so

$$(-1) \times 0 = (-1)^2 + (-1)$$

4. Now we use Lemma 1 to obtain

$$0 = (-1)^2 + (-1)$$

5. Use the Existence of Additive Inverses to see that $(-1) + 1 = 0$ and Existence of Additive Identity to see that $0 + 1 = 1$ and $(-1)^2 + 0 = (-1)^2$

$$\begin{aligned} 0 + 1 &= (-1)^2 + (-1) + 1 \\ 1 &= (-1)^2 \end{aligned}$$

□

There are important properties of the reals which do not follow from the field axioms alone. For example we cannot show that $(\forall x \in \mathbb{F} - \{0\}) x \neq -x$. Let us denote this statement by P. If P did indeed follow from the field axioms, it would be true for all fields, i.e.

$$(\forall \text{ fields}) P \text{ is true}$$

The negation of this statement is

$$(\exists \text{ a field}) P \text{ is false}$$

We know the negation is true because the statement P is false in the field $\mathbb{F}_2$. This is instance of showing a claim is false via a counterexample.

3.5.2 Ordered Fields

A totally ordered set was defined in Definition 2. The distinguishing feature of a totally ordered set X relative to a poset is that we can order every pair of elements in X, i.e.

$$(\forall x, y \in X), \text{ exactly one of } x < y, x = y, y < x, \text{ holds.}$$

This property is so important, we have a name for it: trichotomy.

Now to define an ordered field, we don't simply ask for a field with an order. The order has to interact nicely with the field operations.

Definition 6 (Ordered field)**.** . *An ordered field is a field $\mathbb{F}$ with a relation $\leq$ that makes $\mathbb{F}$ into a totally ordered set such that*

1. *$x \leq y$ implies $x + z \leq y + z$ (Addition preserves order)*
2. *$x \leq y$ and $0 \leq z$ imply $x \times z \leq y \times z$ (Multiplication preserves order when multiplying by a positive number)*

We can see that in $\mathbb{F}_2$ addition does not preserve order, so $\mathbb{F}_2$ cannot be an ordered field.

Lemma 4. *Suppose $\mathbb{F}$ is an ordered field. Then $(\forall x \in \mathbb{F} - \{0\})x \neq -x$.*

Proof. Let $\mathbb{F}$ be an ordered field and let $x \in \mathbb{F} - \{0\}$.

We consider the two elements x and 0 which can be compared because the elements of $\mathbb{F}$ form a totally ordered set. We have $x < 0 \vee x = 0 \vee 0 < x$. The case $x = 0$ is ruled out by assumption. Therefore $x < 0 \vee 0 < x$.

1. We consider the case $x < 0$

$$\begin{aligned} & x < 0 \\ \Rightarrow\ & x + x < 0 + x, \text{Addition preserves order} \\ \iff\ & x + x < x, \text{Existence of Additive Identity} \end{aligned}$$

We have $x + x < x \wedge x < 0$, so by transitivity, we have $x + x < 0$.

Now, taking this further

$$\begin{aligned} & x + x < 0 \\ \Rightarrow\ & (x+x) + (-x) < 0 + (-x), \text{Addition preserves order} \\ \Rightarrow\ & x + (x + (-x)) < 0 + (-x), \text{Associativity of addition} \\ \Rightarrow\ & x + 0 < 0 + (-x), \text{Existence of additive inverse} \\ \Rightarrow\ & x < -x, \text{Existence of additive identity} \end{aligned}$$

2. We consider the case $0 < x$

$$\begin{aligned} & 0 < x \\ \Rightarrow\ & x + 0 < x + x, \text{Addition preserves order} \\ \iff\ & x < x + x, \text{Existence of Additive Identity} \end{aligned}$$

We have $0 < x \wedge x < x + x$, so by transitivity, we have $0 < x + x$.

Now, taking this further

$$\begin{aligned} & 0 < x + x \\ \Rightarrow\ & 0 + (-x) < (x+x) + (-x), \text{Addition preserves order} \\ \Rightarrow\ & 0 + (-x) < x + (x + (-x)), \text{Associativity of addition} \\ \Rightarrow\ & 0 + (-x) < x + 0, \text{Existence of additive inverse} \\ \Rightarrow\ & -x < x, \text{Existence of additive identity} \end{aligned}$$

□

Lemma 5. *Let $\mathbb{F}$ be an ordered field and $x \in \mathbb{F}$. Then $x^2 \geq 0$.*

Proof. By trichotomy, either $x < 0, x = 0$ or $x > 0$.

$$\begin{aligned} x = 0 &\Rightarrow x \times x = 0 \times 0 \\ &\Rightarrow x^2 = 0, \text{using Lemma 1} \end{aligned}$$

$$\begin{aligned}x > 0 \Rightarrow x^2 &> 0 \times x, \text{Multplication by a positive element preserves order}\\ \Rightarrow x^2 &> 0, \text{using Lemma 1}\\ \Rightarrow x^2 &\geq 0.\end{aligned}$$

$$\begin{aligned}x < 0 &\Rightarrow x + (-x) < 0 + (-x), \text{Addition preserves order}\\ &\Rightarrow 0 < -x, \text{Additive Inverse and Additive Identity}\\ &\Rightarrow 0 \times (-x) < (-x) \times (-x), \text{Multplication by a positive element preserves order}\\ &\Rightarrow 0 < (-x)^2, \text{via Lemma 1}\end{aligned}$$

Now

$$\begin{aligned}(-x)^2 &= (-x) \times (-x)\\ &= (-1 \times x) \times (-1 \times x), \text{via Lemma 2}\\ &= (x \times -1) \times (-1 \times x), \text{Commutativity of Multiplication}\\ &= x \times (-1 \times (-1 \times x)), \text{Associativity of Multiplication}\\ &= x \times ((-1 \times -1) \times x)), \text{Associativity of Multiplication}\\ &= x \times (1 \times x)), \text{Lemma 3}\\ &= x \times x, \text{Multplicative Identity}\\ &= x^2\end{aligned}$$

Therefore, $x^2 > 0 \Rightarrow x > 0$. □

Note carefully that the proofs rely on manipulating definitions!

3.5.3 Bounds

Let us consider the set $S = \{1, 2\} \subset \mathbb{Z}^+$. We can see that $2, 3, 4, 5, \dots$ are all greater than or equal to every element of S. $2, 3, 4, 5, \dots$ are all upper bounds for S that are in $\mathbb{Z}^+$ and 2 is the least upper bound. We make this idea precise via the following definitions.

Definition 7 (Upper bound)**.** *Let X be a totally ordered set and let $S \subseteq X$. An upper bound for the subset S is an element $B \in X$ such that $(\forall s \in S) s \leq B$. If the subset S has an upper bound, then we say that S is bounded above.*

We need X to be totally ordered so can decide whether or not one element is $\leq$ another element. It is also obvious from our example that an upper bound is not unique. Note that the upper bound for S does not have be within S.

Definition 8 (Least upper bound)**.** *An upper bound $\underline{B}$ for S is a least upper bound or supremum if nothing smaller than $\underline{B}$ is an upper bound. That is, we need*

1. $(\forall s \in S) s \leq \underline{B}$, *i.e.* $\underline{B}$ *is an upper bound*

2. $(\forall y < \underline{B})(\exists a \in S) a > y$, *i.e. every element smaller than* $\underline{B}$ *is not an upper bound*

We usually write $\sup S$ *for the supremum of* S *when it exists. If* $\sup S \in S$, *then we call it* $\max S$, *the maximum of* S.

Definition 9 (Lower bound)**.** *Let X be a totally ordered set and let $S \subseteq X$. A lower bound for the subset S is an element $b \in X$ such that $(\forall s \in S) s \geq b$. If the subset S has a lower bound, then we say that S is bounded below.*

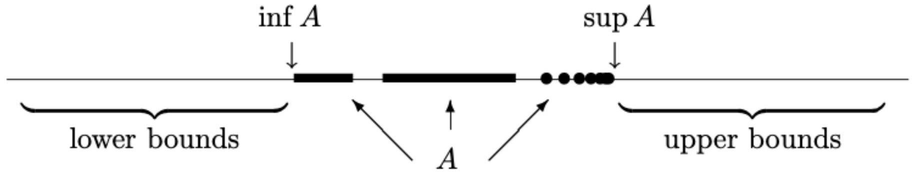
Definition 10 (Greatest lower bound)**.** *An lower bound $\overline{b}$ for S is a greatest lower bound or infimum if nothing larger than $\overline{b}$ is a lower bound. That is, we need*

1. $(\forall s \in S) s \geq \overline{b}$, *i.e.* $\overline{b}$ *is an upper bound*

2. $(\forall y > \overline{b})(\exists a \in S) a < y$, *i.e. every element larger than* $\overline{b}$ *is not a lower bound*

We usually write $\inf S$ *for the infimum of* S *when it exists. If* $\inf S \in S$, *then we call it* $\min S$, *the minimum of* S.

Figure 3.1: This figure illustrates where the infimum and supremum lie for a particular set A.



Example 9. *Let* $X = \mathbb{Q}$ *and* $A = \{x \in X : 0 \leq x \leq 1\}$. *While 3 is clearly an upper bound for* A, *so is 2. 1 is special because it is the least upper bound. We therefore have* $\sup A = 1$, *and because* $\sup A = 1 \in A$, *we also have* $\max A = 1$.

Example 10. *Let* $X = \mathbb{Q}$ *and* $A = \{x \in X : 0 < x < 1\}$. *We have* $\sup A = 1$, *but* A *does not have a maximum, because* $1 = \sup A \notin A$.

Example 11. *Let* $X = \mathbb{Q}$ *and* $A = \{x \in X : x^2 < 2\}$. A *does not have a supremum because* $\sqrt{2} \notin X$.

Definition 11 (Least upper bound property)**.** *A totally ordered set* X *has the least upper bound property if every non-empty subset of* X *that is bounded above has a supremum.*

Definition 12 (Greatest lower bound property)**.** *A totally ordered set* X *has the greatest lower bound property if every non-empty subset of* X *that is bounded below has a infimum.*

3.5.4 Completion

We can see that the rationals are a field, but do not satisfy the least upper bound property, because the rationals have 'gaps'. The addition of the least upper bound property forces the gaps to be filled!

It is simple to check that an ordered field with the least upper bound property has the greatest lower bound property.

Definition 13 (Real numbers)**.** $\mathbb{R}$ *is an ordered field with the least upper bound property.*

The least upper bound property is important because it ensures there are no 'gaps'.

Of course, it is very important to show that an ordered field with the least upper bound property exists, or else we will be studying nothing. It is also nice to show that such a field is unique (up to isomorphism). However, we will not prove these in this course.

In a field, we can define the 'natural numbers' to be $2 = 1 + 1, 3 = 1 + 2$ etc. Then an important property of the real numbers is:

Lemma 6 (Archimedean property v1)**.** *Let* $\mathbb{F}$ *be an ordered field with the least upper bound property. Then the set* $\{1, 2, 3, \ldots\} \subset \mathbb{F}$ *is not bounded above.*

Proof. We shall assume $\{1, 2, 3, \ldots\}$ is bounded above. We also know $\mathbb{F}$ has the least upper bound property and $\{1, 2, 3, \ldots\}$ is a subset of $\mathbb{F}$. Therefore, $\{1, 2, 3, \ldots\}$ has a least upper bound, which we denote by x. Therefore, $x - 1$ is not an upper bound for $\{1, 2, 3, \ldots\}$, and so we can find $n \in \{1, 2, 3, \cdots\}$ such that $n > x - 1$. But $n + 1 \in \{1, 2, 3, \ldots\}$ and $n + 1 > x$, so we have a contradiction. Therefore, the set $\{1, 2, 3, \ldots\} \subset \mathbb{F}$ is not bounded above. □

Definition 14. *Define the absolute value function* $|\cdot| : \mathbb{R} \to \mathbb{R}$ *to be*

$$|x| = \begin{cases} x, \, x \geq 0 \\ -x, \, x < 0 \end{cases}$$

Example 12. *Suppose x and y are real numbers. Prove the following statements:*

1. *If $x \leq y + \epsilon$ for every $\epsilon > 0$, then $x \leq y$.*
2. *If $|x - y| < \epsilon$ for every $\epsilon > 0$, then $x = y$.*

Proof.

1. We start from the statement

$$(\forall \epsilon > 0) \, x \leq y + \epsilon.$$

Now we know $\mathbb{R}$ is a totally ordered set, and so we have either $x \leq y$ or $x > y$. We now rule out the case $x > y$. $x > y \iff x - y > 0$, and so we can pick $\epsilon = \frac{1}{2}(x - y)$. Therefore,

$$(\forall \epsilon > 0) \, x \leq y + \epsilon \Rightarrow x \leq y + \frac{1}{2}(x - y) \iff x - y \leq 0 \iff x \leq y,$$

which is a contradiction.

2. We assume $x \neq y$, which implies $\frac{1}{2}|x - y| > 0$. Now

$$(\forall \epsilon > 0)|x - y| < \epsilon \Rightarrow |x - y| < \frac{1}{2}|x - y| \iff |x - y| < 0,$$

which contradicts $x \neq y$. Therefore, $x = y$.

□

Theorem 1 (Triangle Inequality)**.** *If $x, y \in \mathbb{R}$, then*

$$|x + y| \leq |x| + |y|.$$

Proof.

$$\begin{aligned} & -|x| \leq x \leq |x| \wedge -|y| \leq y \leq |y| \\ \Rightarrow & -|x| - |y| \leq x + y \leq |x| + |y| \\ \iff & -(|x| + |y|) \leq x + y \leq |x| + |y| \\ \iff & |x + y| \leq |x| + |y| \end{aligned}$$

□

3.6 Induction

The construction of the natural numbers, starting from 1 and building $2 = 1 + 1$, $3 = 1 + 1 + 1$ underlies the Principle of Mathematical Induction, which we can state as

$$\forall P(P(1) \wedge (\forall k \in \mathbb{N})P(k) \Rightarrow P(k+1) \Rightarrow (\forall n \in \mathbb{N})P(n)).$$

Here $P(n)$ is some statement, such as $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$

Example 13. *Prove that*

$$(\forall n \in \mathbb{Z}^+) \sum_{i=1}^{n} i = \frac{1}{2}n(n+1).$$

Proof. We start with the base case: when $n = 1$

$$\sum_{i=1}^{n} i = 1$$

and

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

Therefore, our result is true for the base case of $n = 1$.

Now we show that the inductive step is true, i.e.

$$\forall k \in \mathbb{Z}^+ \left(\sum_{i=1}^{k} i = \frac{1}{2}k(k+1) \Rightarrow \sum_{i=1}^{k+1} i = \frac{1}{2}(k+1)(k+2) \right)$$

We assume that $\sum_{i=1}^{k} i = \frac{1}{2}k(k+1)$. Now

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + k + 1 \\ &= \frac{1}{2}k(k+1) + (k+1) \\ &= (k+1)\left(\frac{1}{2}k + 1\right) \\ &= (k+1)\left(\frac{k+2}{2}\right) \\ &= \frac{1}{2}(k+1)(k+2).\end{aligned}$$

Therefore, by the principle of mathematical induction

$$(\forall n \in \mathbb{Z}^{+}) \sum_{i=1}^{n} i = \frac{1}{2}n(n+1).$$

□

3.7 Exercises

1. Find $\sqrt{7}$ to 3 decimal places by hand without aid from a machine.
2. Write computer code in R or Python to find the square root of a natural number to any required degree of accuracy. You cannot use the square root function!
3. Prove that $\sqrt{3}$ is irrational.
4. Prove that for all primes p, $\sqrt{p}$ is irrational.
5. Two quantities are in the golden ratio if their ratio is the same as the ratio of their sum to the larger of the two quantities. Expressed algebraically, for quantities a and b with $a > b > 0$,

   $$\frac{a+b}{a} = \frac{a}{b} = \varphi$$

   where $\varphi > 0$ denotes the golden ratio.

(a) Prove that $\varphi^2 = \varphi + 1$ and hence derive an expression for φ

(b) Prove that φ is irrational.

(c) Explain why

$$\varphi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}.$$

6. Two quantities are in the silver ratio (or silver mean) if the ratio of the smaller of those two quantities to the larger quantity is the same as the ratio of the larger quantity to the sum of the smaller quantity and twice the larger quantity. Show that the silver ratio is $1 + \sqrt{2}$.

7. Find out what the reverse triangle inequality is, state it, and prove it.

8. Let $a, b \in \mathbb{R}^+$, and let us denote

$$QM = \sqrt{\frac{a^2 + b^2}{2}}, \quad AM = \frac{a + b}{2}, \quad GM = \sqrt{ab} \text{ and } HM = \left(\frac{a^{-1} + b^{-1}}{2}\right)^{-1},$$

where QM is the quadratic mean of a and b, AM is the arithmetic mean of a and b, GM is the geometric mean of a and b, and HM is the harmonic mean of a and b.

Prove that

$$QM \geq AM \geq GM \geq HM.$$

with equalities if and only if $a = b$.

9. Compute, without proofs, the suprema and infima of the following sets:

(a) $\{n \in \mathbb{N} : n^2 < 10\}$.

(b) $\{n/(m + n) : m, n \in \mathbb{N}\}$.

(c) $\{n/(2n + 1) : n \in \mathbb{N}\}$.

(d) $\{n/m : m, n \in \mathbb{N} \text{ with } m + n \leq 10\}$.