1. THE REAL NUMBERS

1.1 The Field Axioms

What do we mean by the *real numbers*? Certainly they include the natural numbers, integers and rational numbers. But you are likely aware of the existence of irrational (= not rational) numbers, such as $\sqrt{2}$ or π, which are also real numbers. One answer would be that a real number is a number with a decimal expansion, but then we are getting ahead of ourselves: what is meant by saying $0.333\ldots$ is the decimal expansion of $\frac{1}{3}$? Just what details are hiding behind that ellipsis?

Rather we will simply present a set of *axioms* – statements we will assume to be true of the real numbers. We will base all our arguments on these axioms, and develop theorems from these axioms alone. In Remark 5.34 we will make some brief comments about how the natural numbers, integers, rationals and reals can be constructed from simpler sets, but the details are left to more advanced set-theoretic courses.

Unless otherwise made clear, the quantities a, b, x, etc. discussed in the following will be real numbers. The labelling of these axioms largely follows the convention of Bartle & Sherbert.

Definition 1.1 *The* ***real numbers*** *are a set* $\mathbb{R}$ *together with two binary operations*

- ***addition*** $+\colon \mathbb{R}^2 \to \mathbb{R}$,
- ***multiplication*** $\times\colon \mathbb{R}^2 \to \mathbb{R}$

which satisfy the following axioms

- *the* ***field axioms*** *A1-A4, M1-M4, D, Z.*
- *the* ***order axioms*** *P1-P3.*
- *the* ***completeness axiom*** *C.*

described below. Recall that, as $+$ *and* $\times$ *are binary operations, associated with any ordered pair* (a, b) *of real numbers are real numbers* $a + b$ *and* $a \times b$*, known as their* ***sum*** *and* ***product*** *respectively.*

The **addition axioms** A1-A4 require that

(A1) $+$ is **commutative**, that is $a + b = b + a$ for all a, b.

(A2) $+$ is **associative**, that is $a + (b + c) = (a + b) + c$ for all a, b, c.

(A3) there is an **additive identity** 0, called **zero**, that satisfies $a + 0 = a$ for all a.

(A4) for each a there is an **additive inverse** $-a$ such that $a + (-a) = 0$.

Remark 1.2 *Note that the axioms of addition A1-A4 are equivalent to* $(\mathbb{R}, +)$ *being an abelian group.*

Remark 1.3 *Associativity guarantees that the sum of* $a_1, \ldots, a_k$ *is independent of how the calculation is executed. For example, four terms can be summed in five ways:*

$$((a+b)+c)+d, \quad (a+(b+c))+d, \quad (a+b)+(c+d), \quad a+((b+c)+d), \quad a+(b+(c+d)),$$

and more generally there are

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

ways to bracket a sum of n *terms. (*C_n *denotes the* n*th Catalan number.)*

It can be shown, say using strong induction, that these C_n *calculations lead to the same sum when the operation is associative.*

We now prove some basic first results about addition.

Proposition 1.4 *If* $a + x = a$ *for all* a*, then* $x = 0$*. Thus the additive identity* 0 *is unique.*

Proof. As $a + x = a$ is true for all a, then it is in particular true when $a = 0$. So we have

$$\begin{array}{rcll} x & = & x+0 & \text{by definition of 0 (A3)} \\ & = & 0+x & \text{by commutativity (A1)} \\ & = & 0 & \text{by hypothesis with } a = 0. \end{array}$$

As 0 has the given property, by the above it is the only real number with this property. ■

Proposition 1.5 *If* $a + x = a + y$*, for some* a*, then* $x = y$*. Thus additive inverses are unique.*

Proof.

$$\begin{array}{rcll} y & = & y+0 & \text{by definition of 0 (A3)} \\ & = & y+(a+(-a)) & \text{by definition of inverses (A4)} \\ & = & (y+a)+(-a) & \text{by associativity (A2)} \\ & = & (a+y)+(-a) & \text{by commutativity (A1)} \\ & = & (a+x)+(-a) & \text{by hypothesis} \\ & = & (x+a)+(-a) & \text{by commutativity (A1)} \\ & = & x+(a+(-a)) & \text{by associativity (A2)} \\ & = & x+0 & \text{by definition of inverses (A4)} \\ & = & x & \text{by definition of 0 (A3).} \end{array}$$

It follows that $-a$ is the unique additive inverse of a: if x is an additive inverse of a then

$$a + (-a) = 0 = a + x$$

and it follows that $x = -a$. ■

I wouldn't wish to suggest at this point that the previous and following proofs are the only or even the best proofs. The above proof is reasonably slick, showing in one chain of equalities that y equals x and applying one axiom at a time. But there are other proofs, some of which are arguably more natural, and any proof that is logically correct and carefully justfied is adequate to the task.

A much more natural chain of thought to get from $a + x = a + y$ to $x = y$ would involve 'subtracting a from both sides'. And we can use the axioms to argue exactly along these lines.

Proof. (Alternative proof of Proposition 1.5) Say

$$a + x = a + y.$$

Then

$$(a + x) + (-a) = (a + y) + (-a)\,.$$

By commutativity (A1) we have

$$(x + a) + (-a) = (y + a) + (-a)$$

and by associativity (A2) we then have

$$x + (a + (-a)) = y + (a + (-a))\,.$$

By A4 we have $x + 0 = y + 0$ and finally by A3 we then have $x = y$. ■

Proposition 1.6 $-(-a) = a$.

Proof.

$$\begin{array}{rcll} (-a) + a & = & a + (-a) & \text{by commutativity (A1)} \\ & = & 0 & \text{by definition of inverses (A4)} \end{array}$$

and also

$$(-a) + (-(-a)) \;=\; 0 \quad \text{by definition of inverses (A4).}$$

Hence $-(-a) = a$ as additive inverses are unique (Proposition 1.5). ■

Proposition 1.7 $-(a + b) = (-a) + (-b)\,.$

Proof. This is left as Sheet 1, Exercise 1(iii). ■

Proposition 1.8 $-0 = 0$.

Proof. By definition $0 + (-0) = 0$ and $0 + 0 = 0$. By the uniquness of additive inverses $-0 = 0$.

■

The **multiplication axioms** M1-M4 require that

(M1) $\times$ is **commutative**, that is $a \times b = b \times a$ for all a, b.

(M2) $\times$ is **associative**, that is $a \times (b \times c) = (a \times b) \times c$ for all a, b, c.

(M3) there is a **multiplicative identity** 1, called **one**, that satisfies $a \times 1 = a$ for all a.

(M4) for each $a \neq 0$ there is a **multiplicative inverse**, denoted a^{-1}, such that $a \times (a^{-1}) = 1$.

Remark 1.9 *The axioms of multiplication M1-M4 state that* $(\mathbb{R}\backslash\{0\}, \times)$ *is an abelian group.*

There are then similar results for $\times$ to those proved previously for $+$.

Proposition 1.10 *If* $a \times x = a$ *for all* a *then* $x = 1$. *So the multiplicative identity is unique.*

Proposition 1.11 *If* $a \neq 0$ *and* $a \times x = a \times y$ *then* $x = y$. *So multiplicative inverses are unique.*

Proposition 1.12 *If* $a \neq 0$ *then* $(a^{-1})^{-1} = a$.

Proposition 1.13 *If* $a \neq 0 \neq b$ *and* $ab \neq 0$ *and* $(ab)^{-1} = a^{-1} \times b^{-1}$.

These results are left as exercises for the reader. Their proofs are very similar to the corresponding results for addition. Further, we will soon see that if $a \neq 0 \neq b$ then $ab \neq 0$ (Proposition 1.16) so the hypothesis that $ab \neq 0$ is in fact unnecessary in the last proposition.

There are two remaining field axioms to introduce.

(D) The **distributive law** states that $\times$ *distributes* over $+$. That is,

$$a \times (b + c) = (a \times b) + (a \times c)$$

for all a, b, c.

(Z) $0 \neq 1$.

The importance of axiom Z may not be immediately obvious. If it were the case that $1 = 0$, we would have (by M3 and Proposition 1.15 below) that

$$x = x \times 1 = x \times 0 = 0 \qquad \text{for all } x.$$

So the singleton set $\{0\}$ satisfies all the *other* field axioms and we need axiom Z above to make clear we are not discussing this example. We will also find axiom Z, or rather its negation, a useful conclusion for proofs by contradiction – should an initial assumption lead to the conclusion that $0 = 1$, we would know the initial assumption to be incorrect.

Some important consequences of the distributive law appear below.

Proposition 1.14 $(a + b) \times c = a \times c + b \times c$.

Proof.

$$\begin{array}{rcll} (a+b) \times c & = & c \times (a+b) & \text{by commutativity (M1)} \\ & = & c \times a + c \times b & \text{by distributivity (D)} \\ & = & a \times c + b \times c & \text{by commutativity (M1) twice.} \end{array}$$

■

Proposition 1.15 $a \times 0 = 0$.

Proof.

$$\begin{array}{rcll} a \times 0 + 0 & = & a \times 0 & \text{by definition of 0 (A3)} \\ & = & a \times (0+0) & \text{by definition of 0 (A3)} \\ & = & a \times 0 + a \times 0 & \text{by distributivity (D).} \end{array}$$

Hence $a \times 0 = 0$ by Proposition 1.5. ■

Proposition 1.16 *If $a \times b = 0$ then either $a = 0$ or $b = 0$ (or both).*

Proof. If $a \neq 0$ then we have

$$\begin{array}{rcll} 0 & = & a^{-1} \times 0 & \text{by Proposition 1.15} \\ & = & a^{-1} \times (a \times b) & \text{by hypothesis} \\ & = & (a^{-1} \times a) \times b & \text{by associativity of } \times \text{ (M2)} \\ & = & 1 \times b & \text{by definition of inverse (M4)} \\ & = & b \times 1 & \text{by commutativity of } \times \text{ (M1)} \\ & = & b & \text{by definition of 1 (M3).} \end{array}$$

(Note the above proof amounts to carefully showing that if $a \neq 0$ then we can divide by a to show $b = 0$.) Thus $b = 0$ if $a \neq 0$, or if $a \neq 0$ does not hold then $a = 0$ as required. ■

Proposition 1.17

$$(-b) \times a = -(b \times a).$$

In particular $(-1) \times a = -a$.

Proof.

$$\begin{array}{rcll} (b \times a) + ((-b) \times a) & = & (b + (-b)) \times a & \text{by Proposition 1.14} \\ & = & 0 \times a & \text{by definition of inverse (A4)} \\ & = & 0 & \text{by Proposition 1.15 and M1} \end{array}$$

and

$$(b \times a) + (-(b \times a)) \quad = \quad 0 \quad \text{by definition of inverse (A4).}$$

As additive inverses are unique then $(-b) \times a = -(b \times a)$. The final part follows from setting $b = 1$ and applying M3 and M1. ■

Proposition 1.18

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

Proof.

$$\begin{array}{rcll} (-1) \times (-1) & = & -(-1) & \text{by Proposition 1.17} \\ & = & 1 & \text{by Proposition 1.6.} \end{array}$$

■

Notation 1.19 *From now on we will instead write*

$$\begin{array}{ccc} ab & for & a \times b \\ a - b & for & a + (-b) \\ a/b \text{ or } \frac{a}{b} & for & a \times b^{-1}. \end{array}$$

Also, we define integer powers for $a \neq 0$ by

$$\begin{array}{rcll} a^0 & = & 1 & \\ a^{k+1} & = & a^k \times a & \text{for all } k = 0, 1, 2, 3, \ldots \\ a^{-l} & = & \left(a^l\right)^{-1} & \text{for all } l = 1, 2, 3, \ldots. \end{array}$$

Remark 1.20 *Note that we have only defined integer powers of a here. For $a > 0$ and rational $q = m/n$ we will, in due course (Theorem 1.72 et seq.), define*

$$a^q = \sqrt[n]{a^m}.$$

For general real x and $a > 0$, we will not be able to define

$$a^x = e^{x \log a}$$

until we meet the exponential (Definition 7.17) and logartihm functions (Definition 7.18).

Remark 1.21 *Other number systems also satisfy A1–A4, M1–M4, D, Z. Such systems are called **fields**. Fields are important algebraic structures in mathematics, and all the linear algebra and matrix theory you are meeting in Linear Algebra I extends naturally over any given field. The notion of a field was introduced by Richard Dedekind in 1871.*

The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are all examples of fields. Other examples include $\mathbb{Z}_p$, that is the integers modulo a prime number p, and the field with four elements. See extension exercises 7, 8 and 9 on Sheet 1.

$\mathbb{Z}$ is not a field as it does not meet M4 (multiplicative inverses) though it does satisfy the remainder of the field axioms. $\mathbb{N}$ further fails to meet A4 (additive inverses).

1.2 The Order Axioms

As there are many systems, *fields*, that satisfy the field axioms, we clearly require some further axioms to fully characterize the real numbers. The real numbers are commonly represented by a number line with the numbers increasing in a left-to-right fashion. So it is clear that the real numbers have other properties which we need to capture, including notions of 'being greater than' or 'being to the right of', together with other geometric notions such as distance.

There are various (ultimately equivalent) ways of introducing the notion of 'greater than'. We will again follow Bartle & Sherbert and address this by introducing axioms for what it is to be *positive*.

Definition 1.22 *(**Order Axioms**) There is a subset $\mathbb{P}$ of $\mathbb{R}$, of **positive** real numbers, that satisfies the following three axioms.*

(P1) If a and b are positive, then their sum $a+b$ is positive.

(P2) If a and b are positive, then their product ab is positive.

(P3) For any a precisely one of the following is true:

$$a \text{ is positive}; \qquad a = 0; \qquad -a \text{ is positive}.$$

So to say 'a is positive' means $a \in \mathbb{P}$. Written as an interval, $\mathbb{P} = (0, \infty)$.
*The third axiom P3 is called the **trichotomy** axiom. By this axiom, 0 is not positive.*

Remark 1.23 *Any structure satisfying the field and order axioms is called an **ordered field**. $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields, and any subfield of $\mathbb{R}$ is an ordered field (see Sheet 1, Exercise 7 for such an example). However there is no subset $\mathbb{P}$ of $\mathbb{C}$ which makes it an ordered field (Proposition 1.79).*

Proposition 1.24 *1 is positive.*

Proof. By P3 precisely one of

$$1 \in \mathbb{P}, \qquad 1 = 0, \qquad -1 \in \mathbb{P}$$

must hold. Axiom Z discounts the second possibility. The third option, $-1 \in \mathbb{P}$, leads to a contradiction as follows:

$$\begin{array}{rcll} -1 \in \mathbb{P} & \implies & (-1)(-1) \in \mathbb{P} & \text{by P2} \\ & \implies & 1 \in \mathbb{P} & \text{by Proposition 1.18} \\ & \implies & -1 \in \mathbb{P} \text{ and } 1 \in \mathbb{P} & \end{array}$$

which contradicts P3. By elimination, it follows that $1 \in \mathbb{P}$. ■

There are alternative, equivalent, means of introducing order to the real numbers by defining binary relations $\leqslant$ or $<$ with appropriate properties. The equivalence of the two approaches is left to Sheet 1, Exercise 10. For now we introduce the following notation and definitions.

Notation 1.25 *(a) We write*

$$\begin{array}{lcll} a & > & b & \text{for} \quad a - b \in \mathbb{P}\,. \\ a & < & b & \text{for} \quad b - a \in \mathbb{P}\,. \\ a & \geqslant & b & \text{for} \quad a - b \in \mathbb{P} \cup \{0\}. \\ a & \leqslant & b & \text{for} \quad b - a \in \mathbb{P} \cup \{0\}. \end{array}$$

In this notation the trichotomy axiom, P3, reads as: 'precisely one of $a > 0$, $a = 0$, $a < 0$ holds'.

*(b) Elements of $\mathbb{P} \cup \{0\} = [0, \infty)$ are referred to as **non-negative**, of $\mathbb{P}^c = (-\infty, 0]$ are called **non-positive** and of $(\mathbb{P} \cup \{0\})^c = (-\infty, 0)$ are called **negative**.*

Proposition 1.26 *$a > b$ if and only if $-a < -b$. In particular, $x > 0$ if and only if $-x < 0$.*

Proof.

$$\begin{array}{rrcll} & a & > & b & \\ \iff & a-b & \in & \mathbb{P} & \text{by definition} \\ \iff & -(-a)-b & \in & \mathbb{P} & \text{by Proposition 1.6} \\ \iff & -b-(-a) & \in & \mathbb{P} & \text{by commutativity of } + \text{ (A1)} \\ \iff & -b & > & -a & \text{by definition} \\ \iff & -a & < & -b & \text{by definition.} \end{array}$$

The last claim follows as $-0 = 0$ (Proposition 1.8). ■

Proposition 1.27 *For all a, b, c*

$$a \leqslant a; \tag{1.1}$$

$$a \leqslant b \text{ and } b \leqslant a \implies a = b; \tag{1.2}$$

$$a \leqslant b \text{ and } b \leqslant c \implies a \leqslant c. \tag{1.3}$$

$$\text{either } a \leqslant b \text{ or } b \leqslant a \tag{1.4}$$

Proof. You may recognize (1.1), (1.2), (1.3) as being the reflexivity, anti-symmetry and transitivity properties of a partial order. Combined with (1.4), this means $\leqslant$ is a total order.

(a) By A4 we have $a - a = 0 \in \mathbb{P} \cup \{0\}$ and so $a \leqslant a$.

(b) By definition $a \leqslant b$ and $b \leqslant a$ mean

$$b - a \in \mathbb{P} \cup \{0\} \quad \text{and} \quad a - b = -(b-a) \in \mathbb{P} \cup \{0\}.$$

There are then two cases to consider:

(i) $b - a \in \mathbb{P}$ and $-(b-a) \in \mathbb{P}$. This contradicts trichotomy (P3).

(ii) if $b - a = 0$ then $a = b$; similarly if $a - b = 0$.

(c) If $a = b$ or $b = c$ this is trivial, so we need only consider the case where $b - a \in \mathbb{P}$ and $c - b \in \mathbb{P}$. We then have

$$c - a = (c-b) + (b-a) \in \mathbb{P},$$

by P1 as required.

(d) For $a, b \in \mathbb{R}$, precisely one of the following holds

$$\begin{array}{rcl} b - a \in \mathbb{P} & \implies & a \leqslant b; \\ b - a = 0 & \implies & a \leqslant b \text{ and } b \leqslant a; \\ -(b-a) = a - b \in \mathbb{P} & \implies & b \leqslant a. \end{array}$$

■

Proposition 1.28 *For a, b, c with $a \leqslant b$, then $a + c \leqslant b + c$.*

Proof. Note $(b + c) - (a + c) = b - a \in \mathbb{P} \cup \{0\}$. ■

Proposition 1.29 *For a, b, c with $a \leqslant b$ and $0 \leqslant c$, then $ca \leqslant cb$.*

Proof. If $c = 0$ or $a = b$ then the result holds immediately. Otherwise $b - a \in \mathbb{P}$ and $c \in \mathbb{P}$ so that, by P2, $c(b - a) \in \mathbb{P}$. By D and Proposition 1.17 we see

$$c(b - a) = cb + c(-a) = cb - ca \in \mathbb{P}$$

and so $ca < cb$ as required. ■

Corollary 1.30 *For a, b, c with $a \leqslant b$ and $c \leqslant 0$. Then $ca \geqslant cb$.*

Proof. This is left as Sheet 1, Exercise 1(v). ■

Corollary 1.31 *$a^2 \geqslant 0$ for any real a.*

Proof. By the trichotomy axiom we have $a > 0$ or $a = 0$ or $a < 0$. If $a > 0$ then $a^2 \in \mathbb{P}$ by P1 and so $a^2 \geqslant 0$. If $a < 0$ then $a^2 > a0 = 0$ by Corollary 1.30 and Proposition 1.15. If $a = 0$ then $a^2 = 0 \geqslant 0$ again. ■

Proposition 1.32 *If $a > 0$ then $a^{-1} > 0$.*

Proof. Certainly $a^{-1} \neq 0$ and if $a^{-1} < 0$ then $-a^{-1} > 0$ giving the contradiction

$$-1 = \left(-a^{-1}\right) a > 0$$

by P2. ■

Corollary 1.33 *If $0 < a < b$ then $b^{-1} < a^{-1}$.*

Proof. By the previous proposition and P2

$$a^{-1} - b^{-1} = a^{-1}b^{-1}(b - a) > 0.$$

■

Using the order axioms we may define the **maximum** and **minimum** of two numbers.

Definition 1.34 *Define* $\max\colon \mathbb{R}^2 \to \mathbb{R}$ *and* $\min\colon \mathbb{R}^2 \to \mathbb{R}$ *by*

$$\max(x, y) = \begin{cases} x & \text{if } x \geqslant y; \\ y & \text{if } y > x. \end{cases} \qquad \min(x, y) = \begin{cases} y & \text{if } x \geqslant y; \\ x & \text{if } y > x. \end{cases}$$

By the trichotomy axiom, these are well-defined functions.

We can extend these to functions of finitely many variables. For example, recursively we can define

$$\max(a_1, \ldots, a_n, a_{n+1}) = \max(\max(a_1, \ldots, a_n), a_{n+1}).$$

Example 1.35 $\max(x,y) = -\min(-x,-y)$ *for any* x, y.

Solution. We argue by cases, recalling that if $x < y$ then $-x > -y$ by Proposition 1.26.

	$\max(x,y)$		$-\min(-x,-y)$
$x > y$	x	$-x < -y$	$-(-x) = x$
$x = y$	x	$x = y$	$-(-x) = x$
$x < y$	y	$-y < -x$	$-(-y) = y$

■

Definition 1.36 *We define the* ***modulus*** *function* $|\quad| : \mathbb{R} \to \mathbb{R}$ *by*

$$|x| = \begin{cases} x & \text{if } x \geqslant 0; \\ -x & \text{if } x < 0. \end{cases}$$

These cases are disjoint and cover all possibilities by the trichotomy axiom, so we obtain a well-defined function. $|x|$ *is read as 'mod* x*' or 'the modulus of* x*', and also referred to as 'the absolute value of* x*'.*

Remark 1.37 *As the maximum, minimum and modulus functions are defined in terms of different cases, proofs involving them commonly need to demonstrate the result in a case-by-case manner.*

Proposition 1.38 *For any* x*:*

(a) $0 \leqslant |x|$.
(b) $x \leqslant |x|$.
(c) $|-x| = |x|$.
(d) $|x|^2 = x^2$.

Proof. (a) For $x \geqslant 0$ this is obvious. If $x < 0$ then $|x| = -x > 0$ by definition of $>$.

(b) If $x \geqslant 0$ then $x = |x|$ and so $x \leqslant |x|$. If $x < 0$ then $x < 0 \leqslant |x|$ from (a).

(c) If $x \geqslant 0$ then by Proposition 1.26 we have $-x \leqslant -0 = 0$. So by definition

$$|-x| = -(-x) = x = |x|.$$

If $x < 0$ then $-x > 0$. So $|-x| = -x = |x|$ by definition.

(d) In either case we have $|x|^2 = x^2$ or $|x|^2 = (-x)^2 = x^2$ by Proposition 1.17. ■

Proposition 1.39 ***(Modulus of a product)*** $|ab| = |a|\,|b|$.

Proof. If either $a = 0$ or $b = 0$ then the LHS and RHS are both zero. If $a, b > 0$ then there is nothing to prove. If $a > 0 > b$ then $ab < 0$ and

$$|ab| = -(ab) = a(-b) = |a|\,|b|$$

by Proposition 1.17. Any if $a, b < 0$ then $ab > 0$ and

$$|ab| = ab = (-a)(-b) = |a|\,|b|$$

by Proposition 1.17. ■

Definition 1.40 *Let $S \subseteq \mathbb{R}$ and $f\colon S \to \mathbb{R}$. Then f is said to be:*

- ***increasing*** *if $f(x) \leqslant f(y)$ whenever $x \leqslant y$.*
- ***decreasing*** *if $f(x) \geqslant f(y)$ whenever $x \leqslant y$.*
- ***strictly increasing*** *if $f(x) < f(y)$ whenever $x < y$.*
- ***strictly decreasing*** *if $f(x) > f(y)$ whenever $x < y$.*

Proposition 1.41 *The function $f(x) = x^2$ is strictly increasing on $[0, \infty)$.*

Proof. Given $0 \leqslant a < b$,

$$f(b) - f(a) = b^2 - a^2 = (b-a)(b+a).$$

As $b - a \in \mathbb{P}$ and $b + a \in \mathbb{P}$ then $f(b) - f(a) \in \mathbb{P}$ and so $f(b) > f(a)$, showing that f is strictly increasing. ■

Theorem 1.42 *(**Triangle Inequality**) For any real numbers a, b,*

$$|a+b| \leqslant |a| + |b|\,,$$

with equality if and only if $(a \geqslant 0$ and $b \geqslant 0)$ or $(a \leqslant 0$ and $b \leqslant 0)$.

Proof. Note that

$$\begin{array}{rcll} |a+b|^2 & = & (a+b)^2 & \text{by Proposition 1.38(d)} \\ & = & a^2 + 2ab + b^2 & \\ & = & |a|^2 + 2ab + |b|^2 & \text{by Proposition 1.38(d)} \\ & \leqslant & |a|^2 + 2\,|ab| + |b|^2 & \text{by Proposition 1.38(b)} \\ & = & |a|^2 + 2\,|a|\,|b| + |b|^2 & \text{by Proposition 1.39} \\ & = & (|a| + |b|)^2\,. & \end{array}$$

As $f(x) = x^2$ is strictly increasing on $[0, \infty)$, then $|a| + |b| < |a+b|$ is impossible and the result follows. The cases when equality holds are left to Sheet 1, Exercise 3(i). ■

See Remark 1.84 for an explanation of the inequality's name.

Corollary 1.43 *(**Reverse triangle inequality**) For any real numbers a, b,*

$$|a-b| \geqslant ||a| - |b||\,.$$

Proof. Note by the triangle inequality that

$$\begin{array}{rcccl} |a-b| + |b| & \geqslant & |a| & \implies & |a-b| \geqslant |a| - |b|\,, \\ |b-a| + |a| & \geqslant & |b| & \implies & |a-b| \geqslant |b| - |a|\,, \end{array}$$

and as $||a| - |b||$ equals $|a| - |b|$ or $|b| - |a|$ then the reverse triangle inequality follows. ■

We can use the modulus function to define *distance* on the real line (which is the same as *difference*).

Definition 1.44 *Given real numbers x, y, the* ***distance*** $d(x, y)$ *between x and y is defined to be*

$$d(x, y) = |x - y| .$$

The function $d\colon \mathbb{R}^2 \to \mathbb{R}$ satisfies the properties of a ***metric****, namely, for any real x, y, z:*

(M1) $d(x, y) \geqslant 0$ *and* $d(x, y) = 0$ *if and only if* $x = y$.

(M2) $d(x, y) = d(y, x)$.

(M3) $d(x, z) \leqslant d(x, y) + d(y, z)$.

Property M3 is equivalent to the triangle inequality. Properties M1 and M2 follow readily from properties of the modulus function.

We conclude with two useful inequalities.

Theorem 1.45 ***(Bernoulli's inequality***[1]*)* *Let x be a real number with $x > -1$ and let n be a positive integer. Then*

$$(1 + x)^n \geqslant 1 + nx.$$

Proof. We shall prove the inequality by induction – note that the inequality is immediate when $n = 1$. Suppose that

$$(1 + x)^N \geqslant 1 + Nx$$

holds for all real $x > -1$ and a particular $N \geqslant 1$. Then $1 + x > 0$ and $Nx^2 \geqslant 0$ as $N > 0$ and $x^2 \geqslant 0$. Hence

$$\begin{array}{rcll} (1 + x)^{N+1} & = & (1 + x)(1 + x)^N & \text{by definition} \\ & \geqslant & (1 + x)(1 + Nx) & \text{by hypothesis and Proposition 1.29} \\ & = & 1 + (N + 1)x + Nx^2 & \text{by A1–A4} \\ & \geqslant & 1 + (N + 1)x & \text{by Proposition 1.28.} \end{array}$$

The result follows by induction. ■

Proposition 1.46 ***(Powers dominate polynomials)*** *Let a be a real number with $a > 1$, and k be a positive integer. Then there exists $c > 0$ such that*

$$a^n \geqslant cn^k \quad \textit{for} \quad n = 1, 2, 3, \ldots$$

Proof. Let $a = 1 + b$, so that $b > 0$, and take $n > k$. Then

$$n \geqslant k + 1 \quad \Longrightarrow \quad \frac{n - k}{n} = 1 - \frac{k}{n} \geqslant 1 - \frac{k}{k + 1} = \frac{1}{k + 1}.$$

[1] Named after Jacob Bernoulli (1655-1705) who applied the inequality frequently in a text of 1689.

By the binomial theorem,

$$\begin{aligned} a^n &= 1 + \binom{n}{1}b + \binom{n}{2}b^2 + \cdots + \binom{n}{k}b^k + \cdots + b^n \\ &\geqslant \binom{n}{k}b^k \quad \text{[as all other terms are positive]} \\ &= \frac{n\,(n-1)\cdots(n-k+1)}{k!}b^k \end{aligned}$$

$$\begin{aligned} &> \frac{(n-k)^k}{k!}b^k \\ &= \frac{b^k}{k!}\left(\frac{n-k}{n}\right)^k n^k \\ &\geqslant \left(\frac{b^k}{k!\,(k+1)^k}\right)n^k, \end{aligned}$$

with the last line following from the previous inequalities. We have thus

$$c = \frac{b^k}{k!\,(k+1)^k}$$

is such that $a^n/n^k \geqslant c$ for $n > k$. If instead we set

$$c = \min\left\{a, \frac{a^2}{2^k}, \ldots, \frac{a^k}{k^k}, \frac{b^k}{k!\,(k+1)^k}\right\} > 0$$

then $a^n/n^k \geqslant c$ holds for $n \geqslant 1$. (It's important to note that the above choice of c is independent of n, depending only on a and k.) ■

Example 1.47 *In each of the cases (a) and (b),*

$$\begin{aligned} &(a) \quad x(n) = \frac{3^n + n^3}{2^n}, \quad y(n) = n^4 + 3n^2; \\ &(b) \quad x(n) = \frac{2^n + n^5}{n^2}, \quad y(n) = \frac{(-3)^n}{n^3 + 1}, \end{aligned}$$

determine
(i) whether there exists $c > 0$ such that $x(n) \geqslant cy(n)$ for all n;
(ii) whether there exists $c > 0$ such that $x(n) \leqslant cy(n)$ for all n;
(iii) whether neither (i) nor (ii) applies.

Thoughts: This example now has genuine flavours of analysis; we are no longer simply applying axioms. First thoughts are often qualitative, appreciating which terms in the sequences are significant and which are relatively negligible. For example, in answering (a) we will ultimately

ignore the n^3 term in the numerator; it is helpful, in the sense its presence increases $x(n)$, but it is inconsequential by comparison with 3^n, so we simply do not need to make any use of it. It's also important to note that the example requires us to find a positive c, if it exists, and not in any sense a minimum such c. The existence of any such c is sufficient to answer the question; see Sheet 1, Exercise 11 for further comment.

Solution. (a) Note that $n^3/2^n > 0$ for all n. By Proposition 1.46, there exist $c_1, c_2 > 0$ such that

$$\left(\frac{3}{2}\right)^n \geqslant c_1 n^4 \quad \text{and} \quad \left(\frac{3}{2}\right)^n \geqslant c_2 n^2$$

for all n. Hence

$$\begin{aligned} \frac{3^n + n^3}{2^n} &\geqslant \left(\frac{3}{2}\right)^n \\ &= \frac{1}{2}\left(\frac{3}{2}\right)^n + \frac{1}{2}\left(\frac{3}{2}\right)^n \\ &\geqslant \frac{c_1}{2} n^4 + \frac{c_2}{6}\left(3n^2\right) \\ &\geqslant \min\left(\frac{c_1}{2}, \frac{c_2}{6}\right)\left(n^4 + 3n^2\right). \end{aligned}$$

Hence (i) holds in this case by setting $c = \min\left(c_1/2, c_2/6\right)$.

(b) Note immediately that (ii) cannot hold as $x(n)$ is always positive and $y(n)$ is negative when n is odd. So (i) can only apply if $x(n)$ exceeds some $cy(n)$ for all even n. For even n the inequality $x(n) \geqslant cy(n)$ is equivalent to

$$\left(n^3 + 1\right)\left(\frac{2}{3}\right)^n + \left(\frac{n^8 + n^5}{3^n}\right) \geqslant cn^2.$$

By Proposition 1.46, there exists a number K which exceeds the LHS for all n, whilst the RHS increases without bound as n increases. So no such c exists. To appreciate this in detail, note that:

- There exists $c_1 > 0$ such that $(3/2)^n \geqslant c_1 n^3$ and hence $n^3\,(2/3)^n \leqslant 1/c_1$.
- $(2/3)^n < 1$.
- There exists $c_2 > 0$ such that $3^n \geqslant c_2 n^8$ and hence $n^8/3^n \leqslant 1/c_2$.
- There exists $c_3 > 0$ such that $3^n \geqslant c_3 n^5$ and hence $n^5/3^n \leqslant 1/c_3$.

Thus we require there to be $c > 0$ such that

$$\frac{1}{c}\left(\frac{1}{c_1} + 1 + \frac{1}{c_2} + \frac{1}{c_3}\right) \geqslant n^2 \geqslant n$$

for all positive integers n. The LHS would then be an upper bound for the unbounded $\mathbb{N}$ which does not exist. (See Corollary 1.55.) ■

1.3 The Completeness Axiom

At this stage we can surely persuade ourselves that we could write down proofs of all the usual *algebraic* properties of $\mathbb{R}$, and all the usual order properties of $\leqslant$.

Many structures share these properties – the ordered fields – and in particular both $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields. So why won't $\mathbb{Q}$ suffice? Why do mathematicians not settle for working with this rather nice field of easily understood ratios of integers; countable, too, so that we can list the elements?

The ancient Greeks had at least one reason – in $\mathbb{Q}$ we can't find an element to measure the length of the hypotenuse of a right-angled isosceles triangle with two short sides of length 1. Here is the proof of that fact.

Theorem 1.48 *There is no element $\alpha \in \mathbb{Q}$ such that $\alpha^2 = 2$*

Proof. If there were such an α, then we could write $\alpha = m/n$ for some $m, n \in \mathbb{Z}, n \neq 0$. Further we could assume that this fraction is in lowest terms, so that m and n are coprime. Then $2n^2 = m^2$. As m^2 is even then m is also even as a product of odd numbers is odd. We can then write $m = 2k$ and hence $n^2 = 2k^2$. But then n, too, is even by the same reasoning and m/n wasn't in lowest terms after all. This is the required contradiction. ■

So $\mathbb{Q}$ is lacking in some ways, certainly if we wish to discuss distances, and we look to describe the way(s) $\mathbb{R}$ is different from $\mathbb{Q}$.

Definition 1.49 *Let $B \subseteq \mathbb{R}$.*

*We say that b_1 is a **least element** or **minimum** of B if (i) $b_1 \in B$ and (ii) $b_1 \leqslant b$ for all $b \in B$. In this case we write $b_1 = \min B$.*

*We say that b_2 is a **greatest element** or **maximum** of B if (i) $b_2 \in B$ and (ii) $b \leqslant b_2$ for all $b \in B$. In this case we write $b_2 = \max B$.*

Example 1.50 *1 is the minimum of $[1, 2)$ but there is no maximum for this set. If $x \in [1, 2)$ were a maximum then $x < 2$ and so $1 + x/2$ is a greater element of the set.*

Proposition 1.51 *A maximum (if it exists) is unique. Similarly a minimum is unique.*

Proof. Suppose that b and c are both maxima of B. Then as $b \in B$ and c is a maximum, $b \leqslant c$; as $c \in B$ and b is a maximum then $c \leqslant b$. By anti-symmetry $b = c$. Similarly minima are unique if defined. ■

Proposition 1.52 *Every non-empty subset of $\mathbb{N}$ has a minimum.*

Proof. Suppose, for a contradiction, that S is a non-empty subset of $\mathbb{N}$ with no minimum and define

$$S^* = \{n \in \mathbb{N} \mid \text{none of } 0, 1, \ldots, n \text{ is in } S\}.$$

We shall show that $S^* = \mathbb{N}$ and conclude that S is empty, a contradiction.

Note that $0 \in S^*$. If not then 0 is in S and S has a minimum (namely 0). Now suppose that n is in S^*. This means that none of $0, 1, \ldots, n$ is in S. It follows that $n + 1$ is not in S, or else $n + 1$ would be the minimum of S. Hence none of $0, 1, \ldots, n, n + 1$ is in S or equivalently $n + 1$ is in S^*. By induction $S^* = \mathbb{N}$ and so S is empty. ■

Definition 1.53 *Let $B \subseteq \mathbb{R}$.*

*We say that l is a **lower bound** of B if $l \leqslant b$ for all $b \in B$ and that B is **bounded below**.*

*We say that u is an **upper bound** of B if $b \leqslant u$ for all $b \in B$ and that B is **bounded above**.*

We say that $B \subseteq \mathbb{R}$ is bounded if it is bounded above and below.

Example 1.54 *(a) 23 and π are both upper bounds of $[1, 2)$. And 1 is a lower bound as is -37. The set of upper bounds is $[2, \infty)$ and the set of lower bounds is $(-\infty, 1]$.*

(b) $\mathbb{Q}$ is neither bounded above nor below, $\mathbb{N}$ is bounded below, $(-\infty, e]$ is bounded above.

(c) $\varnothing$ is bounded. The set of upper bounds for $\varnothing$ is $\mathbb{R}$ as is the set of lower bounds.

The below results follow from Proposition 1.52 or can be similarly proved.

Corollary 1.55 *(a) A non-empty subset of $\mathbb{Z}$ which is bounded below has a minimum.*

(b) A non-empty subset of $\mathbb{Z}$ or $\mathbb{N}$ which is bounded above has a maximum.

(c) $\mathbb{N}$ has no maximal element.

We are now ready to give our final axiom which characterises the real numbers.

Definition 1.56 ***(Completeness Axiom)***

(C) Let $S \subseteq \mathbb{R}$ be a non-empty set which is bounded above. Then the set of upper bounds of S has a least element.

Remark 1.57 ***(Equivalent axioms)*** *There are various alternative axioms that are equivalent to the completeness axiom as stated in C. One such is:*

- *Let A and B be non-empty bounded sets such that $a \leqslant b$ for all $a \in A$ and $b \in B$. Show that there exists c such that $a \leqslant c \leqslant b$ for all $a \in A$ and $b \in B$.*

This is shown to be equivalent to C in Sheet 2, Exercise 10.

In this course we will meet further equivalent assumptions:

- *Bounded, monotone sequences converge (Theorem 5.3, Sheet 4, Exercise 6).*
- *Cauchy completeness (Theorem 5.29) and the Archimedean property.*
- *The Nested Intervals Theorem (Theorem 5.7) and the Archimedean property.*
- *The Bolzano-Weierstrass Theorem (Theorem 5.20).*

Another famous equivalent axiom is Dedekind completeness (which is off-syllabus):

- *A Dedekind cut is a set $\varnothing \neq A \subsetneq \mathbb{Q}$ satisfying (i) if $x < y, x \in \mathbb{Q}$, $y \in A$ then $x \in A$ and (ii) if $x \in A$ then there exists $y \in A$ with $y > x$. Dedekind completeness states that $A = (-\infty, z) \cap \mathbb{Q}$ for a unique real number z.*

Remark 1.58 *(**Uniqueness of the real numbers**) The completeness axiom is the last axiom we will introduce in defining the real numbers. Two natural questions arise: do the real numbers exist and is the set of real numbers unique?*

The first question is not meant ontologically. But, rather than just assuming that there is a set $\mathbb{R}$ which satisfies the field axioms, the order axiom and completeness axiom, can such a set be constructed with those properties from more concrete sets such as $\mathbb{N}$, $\mathbb{Z}$ or $\mathbb{Q}$? We will address this aspect of the existence of $\mathbb{R}$ when we meet Cauchy sequences (Remark 5.34).

The second question – the uniqueness of $\mathbb{R}$ – is also a subtle one. What does uniqueness mean here? It is true that, up to order isomorphism, there is a unique complete ordered field. For those wishing to understand the details of this statement see Körner pp.359-360.

Definition 1.59 *We call this least element the **least upper bound** or **supremum** of S, written as $\sup S$. Note that we can refer to $\sup E$ as **the** least upper bound as we have already shown in Proposition 1.51 that minima are unique.*

Example 1.60 *2 is the supremum of $[1, 2)$.*

Proof. For all $x \in [1, 2)$, $1 \leqslant x < 2$ by definition, so clearly 2 is an upper bound. Now suppose that there was a smaller upper bound, t. So $t < 2$, and as t is an upper bound, $t \geqslant 1$. Then $\frac{3}{2} \leqslant \frac{t+2}{2} < 2$. So $\frac{t+2}{2} \in [1, 2)$ but $t < \frac{t+2}{2}$ contradicting the fact that t was an upper bound. ■

Example 1.61 *The set of upper bounds of $\varnothing$ is $\mathbb{R}$ which has no minimum element.*

Proposition 1.62 *If $S \subseteq \mathbb{R}$ has a maximum then $\max S = \sup S$.*

Proof. Note $\max S \geqslant x$ for all $x \in S$ by definition of being a maximum. Further if u is an upper bound for S then $u \geqslant \max S$ by virtue of $\max S$ being an element of S. Hence $\max S$ is the least upper bound. ■

Proposition 1.63 *(**The Approximation Property**) Let S be bounded above and non-empty and let $\varepsilon > 0$. Then there exists $s \in S$ such that*

$$\sup S - \varepsilon < s \leqslant \sup S.$$

Proof. If this were not the case, then $\sup S - \varepsilon$ is an upper bound of S less than the least upper bound, which is a contradiction. ■

Remark 1.64 *To prove that a real number M is the supremum of a set $S \subseteq \mathbb{R}$ it is enough to show that (i) $s \leqslant M$ for all $s \in S$ and either (ii) for any upper bound M' of S we have $M \leqslant M'$ or alternatively (ii)' for any $\varepsilon > 0$ there is $s \in S$ such that $M - \varepsilon < s \leqslant M$.*

Corollary 1.65 *Let S be bounded above and non-empty. There is a function $a \colon \mathbb{N} \to \mathbb{R}$, such that*

$$\sup S - \frac{1}{n} < a(n) \leqslant \sup S \qquad \text{for all } n \geqslant 1.$$

In due course, we will see that this means there is a sequence $(a(n))$ in S which converges to $\sup S$.

We would like to make the symmetric definition for the maximum (if it exists) of the lower bounds of a set which is bounded below. One way would be to introduce yet another axiom guaranteeing its existence. But we don't need to do this; we now have sufficient axioms to prove this as a theorem.

Theorem 1.66 *Let T be a non-empty set which is bounded below. Then the set of lower bounds of T has a greatest element.*

Proof. Let $S = \{-t \mid t \in T\}$. As T is non-empty then S is also non-empty.

In Proposition 1.26 we showed that $x \leqslant y \iff -y \leqslant -x$. Let l be a lower bound of T. Then $l \leqslant t$ for all $x \in T$ and so $-t \leqslant -l$ for all $t \in T$. That is $s \leqslant -l$ for all $s \in S$. Hence S is bounded above, and non-empty, so by the completeness axiom, $\sup S$ exists.

We shall prove (i) $-\sup S$ is a lower bound of T, (ii) if l is a lower bound of T then $l \leqslant -\sup S$.

(i) If $t \in T$ then $-t \in S$ and so $-t \leqslant \sup S$. Hence $t \geqslant -\sup S$ and we see $-\sup S$ is a lower bound of T.

(ii) If $l \leqslant t$ for all $t \in T$ then $-l \geqslant -t$ for all $t \in T$. Hence $-l \geqslant \sup S$ by virtue of $\sup S$ being the least upper bound of S. Finally $l \leqslant -\sup S$. ■

Definition 1.67 *This element is known as* ***the greatest lower bound*** *or* ***infimum*** *of T and is written* $\inf T$.

- By an argument similar to Proposition 1.51 we can show easily show that infima are unique.
- Note if T has a minimum element then $\min T = \inf T$.

Example 1.68 $\sup[1, 2) = 2$ *and* $\inf[1, 2) = 1$. *Also* $\min[1, 2) = 1$ *whilst* $\max[1, 2)$ *does not exist.*

Corollary 1.69 *(**The Approximation Property for infima**) Let T be bounded below and non-empty and let $\varepsilon > 0$. Then there exists $t \in T$ such that*

$$\inf T \leqslant t < \inf T + \varepsilon.$$

Corollary 1.70 *Let T be bounded below and non-empty. There is a function $a\colon \mathbb{N} \to \mathbb{R}$, such that for all n we have*

$$\inf T \leqslant a(n) < \inf T + \frac{1}{n}.$$

Again we will shortly see that this means there is a sequence $(a(n))$ in T which converges to $\inf T$.

Example 1.71 *Let S be a bounded subset of $\mathbb{R}$. Let $c < 0$ and set $cS = \{cs \mid s \in S\}$. Show that cS bounded above, and that* $\sup(cS) = c \inf S$.

Solution. (i) As S is bounded below then $s \geqslant \inf S$ for all $s \in S$. As $c < 0$ then $cs \leqslant c \inf S$ for all $s \in S$ and hence $c \inf S$ is an upper bound for cS. We now have to show that $c \inf S$ is the *least* upper bound of cS and there are two ways of showing this:

(ii) Suppose that u is an upper bound of cS. Then $cs \leqslant u$ for all $s \in S$ and hence $s \geqslant u/c$ for all $s \in S$. This means that u/c is a lower bound of S and in particular $\inf S \geqslant u/c$ as $\inf S$ is the greatest lower bound of S. Then $c \inf S \leqslant u$ and we finally see that $c \inf S$ is less than or equal to any other upper bound of cS.

(ii)' Alternatively let $\varepsilon > 0$ and then, as $\inf S$ is the greatest lower bound for S, there is $s \in S$ such that

$$\inf S \leqslant s < \inf S - \varepsilon/c \qquad \Longrightarrow \qquad c \inf S - \varepsilon < cs \leqslant c \inf S,$$

verifying the supremum approximation property. ■

Theorem 1.72 *($\sqrt{2}$ **exists**) There exists a unique positive number α such that $\alpha^2 = 2$.*

Proof. Let $S = \{x \in \mathbb{R} \mid x^2 < 2\}$. Note that $1^2 = 1 < 2$, so that $1 \in S$ and in particular S is non-empty. Further if $x > 2$ then

$$x^2 = xx > 2x > 4 > 2.$$

Hence 2 is an upper bound for S and so we may define

$$\alpha = \sup S.$$

Note further that $\alpha \geqslant 1 > 0$ is positive. We split the remainder of the proof into showing that $\alpha^2 < 2$ and $\alpha^2 > 2$ both lead to contradictions. By the trichotomy axiom it then follows that $\alpha^2 = 2$.

- Suppose for a contradiction that $\alpha^2 < 2$. Our aim is to show that $(\alpha + h)^2 < 2$ for some $h > 0$ which would give a contradiction. Let $0 < h < 1$ so that $h^2 < h$ in particular. Then
$$(\alpha + h)^2 = \alpha^2 + 2h\alpha + h^2 < \alpha^2 + 2h\alpha + h = \alpha^2 + (2\alpha + 1)\, h.$$
We will have $\alpha^2 + (2\alpha + 1)\, h < 2$, and hence $(\alpha + h)^2 < 2$, if further
$$h < \frac{2 - \alpha^2}{2\alpha + 1},$$
noting the RHS is positive. So we set
$$0 < h < \min\left(1, \frac{2 - \alpha^2}{2\alpha + 1}\right),$$
then $\alpha + h \in S$. But this contradicts $\alpha = \sup S$.

- Suppose instead that $\alpha^2 > 2$. Our aim is to show that $(\alpha - h)^2 > 2$ for some $h > 0$ which again gives a contradiction. Note

$$(\alpha - h)^2 = \alpha^2 - 2h\alpha + h^2 > \alpha^2 - 2h\alpha.$$

So if further

$$0 < h < \frac{\alpha^2 - 2}{2\alpha},$$

then $(\alpha - h)^2 > 2$. As $x \mapsto x^2$ is an increasing function for $x > 0$ then no element of S lies in the interval $(\alpha - h, \alpha)$ which contradicts the approximation property.

Finally, by trichotomy, $\alpha^2 = 2$ is the only remaining possibility. To show uniqueness of α suppose that β is a positive number such that $\beta^2 = 2$. Then

$$\alpha^2 = \beta^2 \quad \Longrightarrow \quad \alpha^2 - \beta^2 = (\alpha + \beta)(\alpha - \beta) = 0.$$

It follows that $\beta = \alpha$ or $\beta = -\alpha$. As $\alpha > 0$ then $-\alpha < 0$ and so α is the only positive solution of $x^2 = 2$.

■

Remark 1.73 *Note that this result shows that $\mathbb{Q}$ does not satisfy the completeness axiom as the set $\{x \in \mathbb{Q} \mid x^2 < 2\}$ does not have a supremum in $\mathbb{Q}$.*

Notation 1.74 *We write $\sqrt{2}$ for α.*

Theorem 1.75 *Let a be any positive real number. Then there exists a unique real number – denoted by $\sqrt{a}$ – whose square is a.*

Proof. This just involves a refining of the previous argument. See also Example 5.9. ■

We've already noted (Corollary 1.55) that $\mathbb{N}$ has no maximal element. This is something that can be proved within the axioms for $\mathbb{N}$. Situating $\mathbb{N}$ within $\mathbb{R}$ we now note:

Theorem 1.76 ***(Archimedean Property)*** *$\mathbb{N}$ is not bounded within $\mathbb{R}$. That is, for any $x \in \mathbb{R}$ there exists $n \in \mathbb{N}$ such that $x < n$.*

Proof. If not, $\mathbb{N}$ is bounded above and not empty. Set $\alpha = \sup \mathbb{N}$. Then so $\alpha - 1 < k$ for some $k \in \mathbb{N}$ by the approximation property. But as $k + 1 \in \mathbb{N}$ and $\alpha < k + 1$, contradicting α being an upper bound for $\mathbb{N}$. ■

Corollary 1.77 *Let $\varepsilon > 0$. Then $0 < \frac{1}{n} < \varepsilon$ for some $n \in \mathbb{N}$.*

Proof. Apply the Archimedean Property to $1/\varepsilon$. ■

Corollary 1.78 *Given reals a, b with $a < b$ then there exists a rational number q and an irrational number r such that $a < q < b$ and $a < r < b$.*

Proof. Left as Sheet 2, Exercises 5ii and 5iii. ■

1.4 Complex numbers

[This section is by way of recap from the *Introduction to Complex Numbers* course. and will not be lectured.]

We can define $\mathbb{C}$ from $\mathbb{R}$ by taking the set $\mathbb{C}$ to be $\mathbb{R}^2$, the set of real ordered pairs and defining addition $+$ and multiplication $\times$ by

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2)\\ (a_1, b_1) \times (a_2, b_2) &= (a_1 a_2 - b_1 b_2, a_2 b_1 + a_1 b_2)\,.\end{aligned}$$

So that, for example

$$(0,1)^2 = (0,1) \times (0,1) = \left(0^2 - 1^2, 0 \times 1 + 0 \times 1\right) = (-1, 0)\,.$$

We more commonly write i for $(0,1)$ and write $a + bi$ for (a, b), so that the above equation states $i^2 = -1$. Further we identify each real number r with $r + 0i$ and so can think of the reals as a subset of the complex numbers.

It is not hard to check that the field axioms A1-A4, M1-M4, D, Z are all true of the complex numbers.

Proposition 1.79 *There is no subset $\mathbb{P}$ of $\mathbb{C}$ which satisfies the order axioms P1–P3.*

Proof. Suppose for a contradiction that such $\mathbb{P} \subseteq \mathbb{C}$ exists. By P3, precisely one of the following holds:

$$i \in \mathbb{P}; \qquad i = 0; \qquad -i \in \mathbb{P}.$$

If $i = 0$ then $1 = i^4 = 0^4 = 0$ which contradicts Z. If $i \in \mathbb{P}$ then by P2 we have $-i = i^3 \in \mathbb{P}$, but then $\pm i \in \mathbb{P}$ which contradicts P3. Assuming $-i \in \mathbb{P}$ leads to the same contradiction. Hence not one of the the possibilities required by P3 holds and no subset $\mathbb{P} \subseteq \mathbb{C}$ exists with the requisite properties. ■

So the complex numbers cannot be made into an ordered field. There is, though, the complex modulus function, that we can use to determine the 'size' of complex numbers. Let $z = x + yi$, where $x = \operatorname{Re} z$ and $y = \operatorname{Im} z$, throughout the following.

Definition 1.80 *The **modulus** of z, written $|z|$, is given by*

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

This makes sense as $x^2 + y^2 \geqslant 0$.

Definition 1.81 *The **conjugate** of z, written $\bar{z}$ (or z^* in some texts), is given by*

$$\bar{z} = x - yi.$$

None of the following properties is at all difficult to prove – they are algebra, not analysis.

1. If z is real (i.e. $z = x + 0i$) then $|z| = |x|$; that is the definitions of real and complex modulus agree where applicable.
2. $|z| = |\bar{z}|$.
3. $|z|^2 = z\bar{z}$.
4. $|\operatorname{Re} z| \leqslant |z|$, $|\operatorname{Im} z| \leqslant |z|$.
5. $z + \bar{z} = 2 \operatorname{Re} z$.
6. $z - \bar{z} = 2i \operatorname{Im} z$.
7. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.
8. $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$.

Theorem 1.82 *For $z, w \in \mathbb{C}$,*

$$|zw| = |z|\,|w|.$$

Proof. Let $z = x + yi$ and $w = u + vi$. Then all we need is the factorisation

$$(xv + yu)^2 + (xu - yv)^2 = (x^2 + y^2)(u^2 + v^2)$$

and the existence of unique non-negative square roots. ■

Theorem 1.83 *(**Triangle Inequality**) For complex numbers z, w,*

$$|z + w| \leqslant |z| + |w|.$$

Proof. Using the above properties.

$$\begin{aligned} |z+w|^2 &= (z+w)\,(\overline{z+w}) \\ &= (z+w)\,(\bar{z}+\bar{w}) \\ &= z\bar{z} + (z\overline{w} + \bar{z}w) + w\overline{w} \\ &= z\bar{z} + 2\operatorname{Re}(z\overline{w}) + w\overline{w} \\ &\leqslant z\bar{z} + 2|z\overline{w}| + w\overline{w} \\ &= |z|^2 + 2|z|\,|w| + |w|^2 \\ &= (|z| + |w|)^2. \end{aligned}$$

■

Remark 1.84 *The name 'triangle inequality' is clearer to explain in $\mathbb{C}$ rather than in $\mathbb{R}$. Consider the triangle in $\mathbb{C}$ with vertices $A = 0$, $B = z$ and $C = z + w$. Then $|z + w| = |AC|$, $|z| = |AB|$ and $|BC| = |(z + w) - z| = |w|$. So the triangle inequality states that the length of one edge is less than the sum of the lenghts of the other two edges.*