Math 140A - Notes

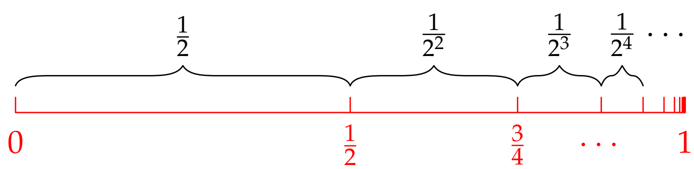
Neil Donaldson

Fall 2023

Introduction

Analysis is one of the major sub-disciplines of mathematics, being concerned with continuous functions, limits, calculus and accurate approximations.

Analytic ideas date back over 2000 years. For instance, Archimedes (c. 287–212 BC) used limit-type approaches to approximate the circumference of a circle and compute the area under a parabola.[1] The philosophical objections to such calculations are just as old: how can it make sense to sum up infinitely many infinitesimally small quantities? This was part of a deeper debate among the ancient Greeks: is the matter comprising the natural world *atomic* (consisting of minute, discrete, indivisible pieces) or *continuous* (arbitrarily and infinitesimally divisible). Several of Zeno's famous paradoxes (5^{th} C. BC) grapple with these difficulties: *Achilles and the Tortoise* essentially argues that the infinite series $\sum\limits_{n=1}^{\infty} \frac{1}{2^n} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots$ is meaningless.



As we'll see, with modern definitions it makes sense for this sum to evaluate to 1.

The work of Newton and Leibniz in the late 1600s allowed the easy application of calculus to many important problems in the sciences, but without properly addressing the ancient philosophical challenges. The logical development of calculus necessitated by this became the triumph of 18^{th}–19^{th} century mathematics. The critical notions of limit and continuity only became rigorous in the early 1800s, courtesy of Bolzano, Cauchy and Weierstrass (amongst others), with another 50 years before Riemann provided a thorough description of the definite integral.

The Math 140A/B sequence introduces analysis by focusing on these ideas. In this course we primarily consider sequences, limits, continuity and infinite series. Power series, differentiation and integration are the focus of 140B. We start, however, with something even more basic: to numerically measure continuous quantities, we need to familiarize ourselves with the *real numbers.* Since a concrete description is quite difficult, we build up to it using first the natural numbers and then the rationals. . .

[1] Archimedes' circle calculation is reminiscent of the Riemann sum approach to integration, whereas his parabolic area method required the evaluation of the infinite series $\sum_{n=0}^{\infty} \frac{1}{4^n} = \frac{4}{3}$.

1 The Set $\mathbb{N}$ of Natural Numbers

You've been using the natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$ since you learned to count. In mathematics, these must be axiomatically described. Here is one approach, known as *Peano's Axioms.*

Axioms 1.1. The natural numbers are a set $\mathbb{N}$ satisfying the following properties:

1. (Non-emptiness) $\mathbb{N}$ is non-empty.
2. (Successor function) There exists a function $f : \mathbb{N} \to \mathbb{N}$. This function is usually denoted '$+1$' so that we may write,

$$n \in \mathbb{N} \implies n + 1 \in \mathbb{N}$$

3. (Initial element) f is *not surjective.* Otherwise said, there exists an element $1 \notin \operatorname{range} f$ which is not the successor of any element.[2]
4. (Unique predecessor/order) f is *injective.* If m and n have the same successor, then $m = n$.
5. (Induction) Suppose $A \subseteq \mathbb{N}$ is a subset satisfying
   (a) $1 \in A$
   (b) $n \in A \implies n + 1 \in A$.

   Then $A = \mathbb{N}$.

Axioms 1–4 are relatively straightforward, the natural numbers are defined by repeatedly adding 1 to the initial element; for instance

$$3 := f\big(f(1)\big) = (1 + 1) + 1$$

To see why Axiom 5 is so-named, compare an easy example with a standard induction argument.

Example 1.2. Prove that $7^n - 4^n$ is divisible by 3 for all $n \in \mathbb{N}$.
Let A be the set of natural numbers for which $7^n - 4^n$ is divisible by 3. It is required to prove that $A = \mathbb{N}$.

(a) If $n = 1$, then $7^1 - 4^1 = 3$, whence $1 \in A$.

(b) Suppose $n \in A$. Then $7^n - 4^n = 3\lambda$ for some $\lambda \in \mathbb{N}$. But then

$$\begin{aligned} 7^{n+1} - 4^{n+1} &= 7 \cdot 7^n - 4^{n+1} = 7(3\lambda + 4^n) - 4^{n+1} = 3 \cdot 7\lambda + (7 - 4) \cdot 4^n \\ &= 3\big(7\lambda + 4^n\big) \end{aligned}$$

is divisible by 3. It follows that $n + 1 \in A$.

Appealing to axiom 5, we see that $A = \mathbb{N}$, hence result.
The two arguments are precisely the familiar *base case* and *induction step*.

[2] It is purely convention to denote the first natural number by 1; we could use 0, x, α, or any symbol you wish!

What about the integers? It should be clear that the integers satisfy axioms 1, 2 and 4, but not 3 and 5. For instance:

~~3~~. The function $f : \mathbb{Z} \to \mathbb{Z} : n \mapsto n+1$ is surjective (indeed bijective/invertible). The number 1 is the successor of 0.

We can reverse this observation to provide an explicit construction of the integers from the natural numbers. Simply extend the function f so that *every* element has a unique predecessor: 0 is the unique predecessor of 1, -1 the unique predecessor of 0, etc. In essence we are forcing $f(n) = n+1$ to be bijective!

Exercises 1. Most of these exercises are to refresh your memory of mathematical induction. You can use either the language of Peano's axiom 5, or the (likely) more familiar base-case/induction-step formulation.

1. Prove that $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$ for all natural numbers n.
2. Prove that $3 + 11 + \cdots + (8n-5) = 4n^2 - n$ for all $n \in \mathbb{N}$.
3. (a) Guess a formula for $1 + 3 + \cdots + (2n-1)$ by evaluating the sum for $n = 1, 2, 3$, and 4. (*For $n = 1$ the sum is simply 1*)
   (b) Prove your formula using mathematical induction.
4. Prove that $11^n - 4^n$ is divisible by 7 for all $n \in \mathbb{N}$.
5. The principle of mathematical induction can be extended as follows. A list $P_m, P_{m+1}, \ldots$ of propositions is true provided (i) P_m is true, (ii) P_{n+1} is true whenever P_n is true and $n \geq m$.
   (a) Prove that $n^2 > n+1$ for all integers $n \geq 2$.
   (b) Prove that $n! > n^2$ for all integers $n \geq 4$. (*Recall that $n! = n(n-1)\cdots 2 \cdot 1$*)
6. Prove $(2n+1) + (2n+3) + (2n+5) + \cdots + (4n-1) = 3n^2$ for all $n \in \mathbb{N}$.
7. For each $n \in \mathbb{N}$, let P_n denote the assertion "$n^2 + 5n + 1$ is an even integer".
   (a) Prove that P_{n+1} is true whenever P_n is true.
   (b) For which n is P_n actually true? What is the moral of this exercise?
8. Show that Peano's induction axiom is *false* for the set of integers $\mathbb{Z}$ by exhibiting a *proper subset* $A \subset \mathbb{Z}$ which satisfies conditions (a) and (b).
9. Consider $\mathbb{Z}_3 = \{0, 1, 2\}$ under addition modulo 3. That is,

   $$0 + 1 = 1, \quad 1 + 1 = 2, \quad 2 + 1 = 0$$

   Which of Peano's axioms are satisfied?

2 The Set $\mathbb{Q}$ of Rational Numbers

There are several ways to define the rational numbers from the integers. For instance, we could consider the set of relatively prime ordered pairs

$$\mathbb{Q} = \{(p,q) : p \in \mathbb{Z},\ q \in \mathbb{N},\ \gcd(p,q) = 1\} \subseteq \mathbb{Z} \times \mathbb{N}$$

Things are more familiar once we write $\frac{p}{q}$ instead of (p,q) and adopt the convention that $\frac{\lambda p}{\lambda q} = \frac{p}{q}$ for any non-zero $\lambda \in \mathbb{Z}$. It is easy to define the usual operations $(+, \cdot,$ etc.) consistently with those for the integers (Exercise 7).

An alternative approach involves equations. Each *linear equation* $qx - p = 0$ where $p, q \in \mathbb{Z}$ and $q \neq 0$ corresponds to a rational number! For example

$$13x + 27 = 0 \leftrightsquigarrow x = -\frac{27}{13}$$

Of course $26x + 54 = 0$ *also* corresponds to the same rational number!

Extending this process, we might consider higher degree polynomials.

Definition 2.1. A number x is *algebraic* if it satisfies an equation of the form[3]

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{$*$}$$

for some integers $a_0, \ldots, a_n$.

Examples 2.2. 1. $\sqrt{2}$ is algebraic since it satisfies the equation $x^2 - 2 = 0$.

2. $x = \sqrt[5]{7 + \sqrt{3}}$ is also algebraic:

$$x^5 - 7 = \sqrt{3} \implies (x^5 - 7)^2 = 3 \implies x^{10} - 14x^5 + 46 = 0$$

The next result is helpful for deciding whether a given number is rational and can assist with factorizing polynomials.

Theorem 2.3 (Rational Roots). *Suppose that $a_0, \ldots, a_n \in \mathbb{Z}$ and that $x \in \mathbb{Q}$ satisfies $(*)$. If $x = \frac{p}{q}$ in lowest terms, then $p \mid a_0$ and $q \mid a_n$.*

Proof. Since x satisfies the polynomial, we see that

$$a_n \left(\frac{p}{q}\right)^n + \cdots + a_1 \left(\frac{p}{q}\right) + a_0 = 0 \implies a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

All terms except the last contain a factor of p, whence $p \mid a_0 q^n$. Since $\gcd(p,q) = 1$ it follows that $p \mid a_0$. The result for q is almost identical. ∎

[3] You should be alarmed by this! We have given up on *constructing* new numbers and instead are simply *describing* their properties. No matter, a construction of the real numbers will come later.

Examples 2.4. 1. We show that $\sqrt{2}$ is irrational.[4] Plainly $x = \sqrt{2}$ satisfies the polynomial equation $x^2 - 2 = 0$. If $\sqrt{2} = \frac{p}{q}$ were rational in lowest terms, then the rational roots theorem forces

$$p \mid 2 \quad \text{and} \quad q \mid 1 \implies \sqrt{2} \in \{\pm 1, \pm 2\}$$

Since none of the numbers $\pm 1, \pm 2$ satisfy $x^2 - 2 = 0$, we have a contradiction.

2. $(\sqrt{3} - 1)^{1/3}$ is irrational. It satisfies $(x^3 + 1)^2 = 3$, from which

$$x^6 + 2x^3 - 2 = 0$$

By the theorem, if $x = \frac{p}{q}$ were rational then $p \mid 2$ and $q \mid 1$, whence $x = \pm 1, \pm 2$, none of which satisfies $(x^3 + 1)^2 = 3$.

3. $\left(\frac{4+\sqrt{3}}{5}\right)^{1/2}$ is irrational. It satisfies $5x^2 - 4 = \sqrt{3}$, from which

$$25x^4 - 40x^2 + 13 = 0$$

If $x = \frac{p}{q}$ were rational, then $p \mid 13$ and $q \mid 25$. There are twelve possibilities in all:

$$x = \pm 1, \pm 13, \pm\frac{1}{5}, \pm\frac{13}{5}, \pm\frac{1}{25}, \pm\frac{13}{25}$$

It is tedious to check all cases, but none satisfy the required polynomial.

With this example it is easier to bypass the theorem entirely: if $x \in \mathbb{Q}$ then $\sqrt{3} = 5x^2 - 4$ would also be rational!

4. We factorize the polynomial $3x^3 + x^2 + x - 2 = 0$. By the rational roots theorem, if $x = \frac{p}{q}$ is a rational root, then $p \mid 2$ and $q \mid 3$ which gives several possibilities:

$$x \in \left\{\pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}\right\}$$

It doesn't take long to try these and observe that $x = \frac{2}{3}$ is the only rational solution. The polynomial has a factor of $3x - 2$ which we can extract by long division to obtain

$$3x^3 + x^2 + x - 2 = (3x - 2)(x^2 + x + 1)$$

The quadratic has no real roots: absent complex numbers, the factorization is complete.

It is far from clear that there exist non-algebraic (or *transcendental*) numbers, of which e and π are the most famous examples. These satisfy no polynomial equation with integer coefficients, though demonstrating this is tricky.

---

[4] Compare this to the standard proof of the irrationality of $\sqrt{2}$ as seen in a previous course. Note how easy it is to extend our approach to $\sqrt{3}$, $\sqrt{29}$, $\sqrt[3]{2}$, $\sqrt[5]{8}$, etc.

Exercises 2. 1. Describe all the linear equations which correspond to the rational number $\frac{101}{29}$.

2. Show that $\sqrt{3}$, $\sqrt{5}$ and $\sqrt{24}$ are not rational numbers.
   (*Hint: what are the relevant polynomials?*)

3. Show that $2^{1/3}$ and $13^{1/4}$ are not rational numbers.

4. Show that $(2+\sqrt{2})^{1/2}$ is not rational.

5. Show that $(3+\sqrt{2})^{2/3}$ is not rational.

6. Explain why $4-7b^2$ must be rational if b is rational.

7. Given rational numbers (p,q) and (r,s) as ordered pairs, what are the rational numbers $(p,q)+(r,s)$ and $(p,q)\cdot(r,s)$?
   (*Hint: what is* $\frac{p}{q}+\frac{r}{s}$*?*)

8. Let $n \in \mathbb{N}$. Use the rational roots theorem to prove that $\sqrt{n}$ is rational if and only if it is an *integer.*

3 Ordered Fields

Thus far, we have formally constructed the natural numbers and used them to (loosely) build the integers and rational numbers. It is a significantly greater challenge to *construct* the real numbers. We start by thinking about ordered fields, of which both $\mathbb{Q}$ and $\mathbb{R}$ are examples.

Axioms 3.1. A *field* $\mathbb{F}$ is a set together with two binary operations $+$ and $\cdot$ which satisfy the following (for all $a, b, c \in \mathbb{F}$),[5]

	Addition	Multiplication
Closure	$a + b \in \mathbb{F}$	$ab \in \mathbb{F}$
Associativity	$a + (b + c) = (a + b) + c$	$a(bc) = (ab)c$
Commutativity	$a + b = b + a$	$ab = ba$
Identity	$\exists 0 \in \mathbb{F}$ such that $a + 0 = a$	$\exists 1 \in \mathbb{F}$ such that $a \cdot 1 = a$
Inverse	$\exists -a \in \mathbb{F}$ such that $a + (-a) = 0$	If $a \neq 0$, $\exists a^{-1} \in \mathbb{F}$ such that $aa^{-1} = 1$
Distributivity	$a(b + c) = ab + ac$	

A field $\mathbb{F}$ is *ordered* if we also have a binary relation $\leq$ which satisfies (again for all $a, b, c \in \mathbb{F}$):

O1 $a \leq b$ or $b \leq a$

O2 $a \leq b$ and $b \leq a \implies a = b$

O3 $a \leq b$ and $b \leq c \implies a \leq c$

O4 $a \leq b \implies a + c \leq b + c$

O5 $a \leq b$ and $0 \leq c \implies ac \leq bc$

For an ordered field, the symbol $<$ is used in the usual way: $x < y \iff x \leq y$ and $x \neq y$.

As with Peano's axioms for the natural numbers, these are not worth memorizing. Instead you should quickly check that you believe all of them for your current understanding of the real numbers; you can't *prove* anything since the real numbers haven't yet been defined!

Example 3.2. It is worth considering the rational numbers in a little more detail. Recall (Section 2) how $\mathbb{Q}$ may be defined as a set of ordered pairs $\frac{p}{q} \leftrightsquigarrow (p, q) \in \mathbb{Z} \times \mathbb{N}$. It moreover inherits a natural ordering from $\mathbb{Z}$ and $\mathbb{N}$:

$$\frac{p}{q} \leq \frac{r}{s} \iff ps \leq qr \qquad \text{(remember that } q, s > 0\text{)}$$

[5] We write multiplication $\cdot$ as juxtaposition unless it is helpful for clarity. We also use the common shorthand $a^2 = a \cdot a$. If you know some abstract algebra:

- The addition axioms say that $(\mathbb{F}, +)$ is an abelian group.
- The multiplication axioms say that $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group.
- The distributive axiom describes how addition and multiplication interact.

It is now possible, though tedious, to *prove* that each of the axioms of an ordered field holds for $\mathbb{Q}$, using only basic facts about multiplication, addition and ordering *within the integers.* For instance,

O3 Suppose $a \le b$ and $b \le c$. Write $a = \frac{p}{q}$, $b = \frac{r}{s}$ and $c = \frac{t}{u}$ where all three denominators are positive. By assumption,

$$\begin{aligned} ps \le qr \text{ and } ru \le st \implies psu \le qru \le qst \implies pu \le qt \\ \implies a = \frac{p}{q} \le \frac{t}{u} = c \end{aligned}$$

Basic Results about ordered fields

As with the axioms of an ordered field, it is not worth *memorizing* these.

Theorem 3.3. *Let $\mathbb{F}$ be a ordered field with at least two elements $0 \neq 1$. Then:*

1. $a + c = b + c \implies a = b$
2. $a \cdot 0 = 0$
3. $(-a)b = -(ab)$
4. $(-a)(-b) = ab$
5. $ac = bc$ and $c \neq 0 \implies a = b$
6. $ab = 0 \implies a = 0$ or $b = 0$
7. $a \le b \implies -b \le -a$
8. $a \le b$ and $c \le 0 \implies bc \le ac$
9. $0 \le a$ and $0 \le b \implies 0 \le ab$
10. $0 \le a^2$
11. $0 < 1$
12. $0 < a \implies 0 < a^{-1}$
13. $0 < a < b \implies 0 < b^{-1} < a^{-1}$

All of these statements should be intuitive for the fields $\mathbb{Q}$ and $\mathbb{R}$. Try *proving* a few using only the axioms; they are easiest done in the order presented. For instance, part 2 might be proved as follows:

$$\begin{aligned} & a \cdot 0 + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 && \text{(additive identity/distibutive axioms)} \\ \implies & 0 = a \cdot 0 && \text{(part 1)} \end{aligned}$$

We finish with one final useful ingredient.

Definition 3.4. If $\mathbb{F}$ is an ordered field, then the *absolute value* of $a \in \mathbb{F}$ is

$$|a| := \begin{cases} a & \text{if } a \ge 0 \\ -a & \text{if } a < 0 \end{cases}$$

Theorem 3.5. *In any ordered field:*

1. $|a| \ge 0$
2. $|ab| = |a| \cdot |b|$
3. $|a + b| \le |a| + |b|$ *($\triangle$-inequality)*

All three parts are immediate if you consider the $\pm$-cases separately for a, b.

Exercises 3. 1. Which of the axioms of an ordered field fail for $\mathbb{N}$? For $\mathbb{Z}$?

2. Prove parts 11 and 13 of Theorem 3.3.

   (*Remember you can use any of the parts that come before...*)

3. (a) Prove that $|a+b+c| \leq |a|+|b|+|c|$ for all $a, b, c \in \mathbb{R}$.
   (*Hint: Apply the triangle inequality twice. Don't consider eight separate cases!*)

   (b) Use induction to prove

   $$|a_1 + a_2 + \cdots + a_n| \leq |a_1| + |a_2| + \cdots + |a_n|$$

   for any $a_1, \ldots, a_n \in \mathbb{R}$.

4. (a) Show that $|b| < a \iff -a < b < a$.

   (b) Show that $|a-b| < c \iff b-c < a < b+c$

   (c) Show that $|a-b| \leq c \iff b-c \leq a \leq b+c$

5. Let $a, b \in \mathbb{R}$. Show that if $a \leq b_1$ for every $b_1 > b$, then $a \leq b$.

   (*Hint: draw a picture if you're stuck. This is a very important example!*)

6. Following Example 3.2, prove that $\mathbb{Q}$ satisfies axiom O5.

   (*Hint: if $a = \frac{p}{q}$, etc., what is meant by $ac \leq bc$?*)

7. (Hard!) The complex numbers $\mathbb{C} = \{x+iy : x, y \in \mathbb{R}\}$ form a field. Consider the lexicographic ordering of $\mathbb{C}$ defined by

   $$x+iy \leq p+iq \iff \begin{cases} x < p \text{ or} \\ x = p \text{ and } y \leq q \end{cases}$$

   Which of the order axioms O1–O5 are satisfied by the lexicographic ordering?

   (*Don't prove your claims if an axiom is satisfied, but provide a counter-example if not*)

4 The Completeness Axiom

While we still haven't provided an explicit *definition* of the real numbers, you should be comfortable with the fact that both $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields. The question remains of how to distinguish them? Perhaps surprisingly, only one additional axiom is required: the *completeness axiom* or *least upper bound principle.* To explain this we first need some terminology.

Definition 4.1 (Maxima, Minima & Boundedness). Let $S \subseteq \mathbb{R}$ be non-empty.

1. S is *bounded above* if it has an *upper bound* M:

$$\exists M \in \mathbb{R} \text{ such that } \forall s \in S,\ s \leq M$$

2. We write $M = \max S$, the *maximum* of S, if M is an upper bound for S *and* $M \in S$.

3. S *bounded below*, a *lower bound* m, and the *minimum* $\min S$ are defined similarly.

4. S is *bounded* if it is bounded above and below. We say that S is *bounded by* M if

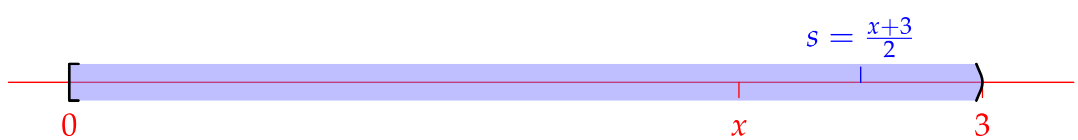
$$\forall s \in S,\ |s| \leq M$$

Examples 4.2. 1. If S is a finite set, then it is bounded and has both a maximum and a minimum. For instance, $S = \{-3, \pi, 12\}$ has $\min S = -3$ and $\max S = 12$.

2. $\mathbb{N}$ has minimum 1, but no maximum. $\mathbb{Z}$ and $\mathbb{Q}$ have neither: both are *unbounded.*

3. The interval $S = [0, 3) = \{x \in \mathbb{R} : 0 \leq x < 3\}$ is bounded, for example by $M = 5$, it has minimum 0 and no maximum. While this last is likely intuitive, it worth giving an explicit argument, in this case by contradiction.

   Suppose $x = \max S$ exists. It is helpful to draw a picture to get the lay of the land. Since $x \in S$, we've placed x *inside* the interval, away from 3.



   The crux of the proof is to observe that there exists $s \in S$ which is *larger* than x. The natural choice is the average $s := \frac{1}{2}(x+3)$. Now observe that

$$3 - s = s - x = \frac{1}{2}(3 - x) > 0$$

   In particular,

   - $s \in S$ since it is non-negative and $s < 3$.
   - $s > x$.

   Since S contains an element larger than x, it follows that x cannot be the maximum of S. In conclusion, S has no maximum.

The following should be immediate: try proving them yourself.

Lemma 4.3. 1. *If M is an upper bound for S, so is $M+\varepsilon$ for any $\varepsilon \geq 0$.*

2. *If $\max S$ exists, then it is unique.*

3. *A set is bounded if and only if it is bounded above and below. In particular, if m, M are lower/upper bounds, then S is bounded by*

$$\forall s \in S,\ |s| \leq \max(|m|, |M|)$$

Example 4.4. Before introducing the key axiom, we consider a variation on the previous example. We show that the following set has no maximum:

$$S = \mathbb{Q} \cap [0, \sqrt{2}) = \{x \in \mathbb{Q} : 0 \leq x < \sqrt{2}\}$$

The approach is similar to before: given a hypothetical maximum x, find an element $s \in S$ between x and $\sqrt{2}$. The challenge is that we can't simply use the *average* $\frac{1}{2}(x+\sqrt{2})$: this isn't rational (*why?*) and so doesn't lie in S!

To fix this, we informally invoke sequences: this might seem quite hard at the moment, but will be made rigorous later. The rough idea is to construct a sequence (s_n) of elements of S which increases to $\sqrt{2}$. Eventually one of these must be larger than x.

Define a sequence of rational numbers (s_n) by $s_n = \frac{1}{10^n}\lfloor 10^n\sqrt{2}\rfloor$, where $\lfloor\ \rfloor$ denotes the *floor function*.[6] The sequence simply recovers the first n decimal places of $\sqrt{2}$:

$$s_0 = 1, \quad s_1 = 1.4 = \frac{14}{10}, \quad s_2 = 1.41 = \frac{141}{100}, \quad s_3 = 1.414 = \frac{1414}{1000}, \quad \ldots$$

and has the following properties:

- $s_n \in S$ since any truncating decimal is rational and certainly $0 \leq s_n < \sqrt{2}$.
- $\sqrt{2} - s_n < 10^{-n}$ follows since $10^n\sqrt{2} - \lfloor 10^n\sqrt{2}\rfloor < 1$.

Now suppose $x = \max S$ exists. Since $x \in S$, we have $x < \sqrt{2}$. Choose $N \in \mathbb{N}$ large enough so that $10^{-N} < \sqrt{2} - x$. Then $s_N \in S$ and

$$\sqrt{2} - s_N < 10^{-N} < \sqrt{2} - x \implies x < s_N$$

The hypothetical maximum x is not an upper bound for S: contradiction.

[6] $\lfloor y\rfloor$ is the greatest integer less than or equal to y; informally *round down*. For example $\lfloor \pi\rfloor = 3$. This approach is a something of a hack: it can be sped up enormously using the upcoming density of $\mathbb{Q}$ in $\mathbb{R}$ (Corollary 4.12); indeed the Archimedean property on which it depends is necessary for $\lfloor y\rfloor$ to be well-defined.

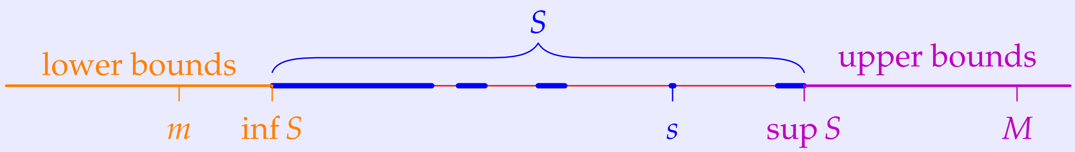
Suprema and Infima

We now generalize the idea of maximum and minimum values for bounded sets.

Example 4.5. The interval $[2,5)$ has *least upper bound* 5: among all upper bounds, 5 is the smallest.

Definition 4.6. Let $S \subseteq \mathbb{R}$ be non-empty.

1. If S is bounded above, its *supremum* $\sup S$ is its *least upper bound*. Otherwise said,
   (a) $\sup S$ is an upper bound: $\forall s \in S,\ s \le \sup S$,
   (b) $\sup S$ is the least such: if M is an upper bound, then $\sup S \le M$.
2. If S is bounded below, its *infimum* $\inf S$ is its *greatest lower bound*. Equivalently,
   (a) $\inf S$ is a lower bound: $\forall s \in S,\ \inf S \le s$,
   (b) $\inf S$ is the greatest such: if m is a lower bound, then $m \le \inf S$.



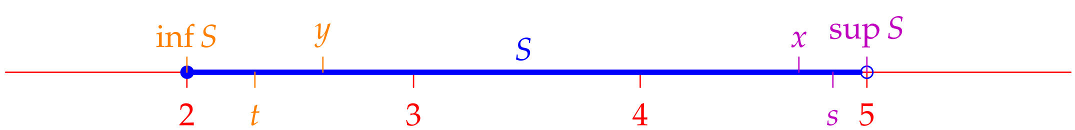
Example (4.5 cont). We verify the supremum and infimum for $S = [2,5)$; parts (a), (b) are the properties in the above definition.

(a) Since $s \in S \iff 2 \le s < 5$, we see that 5 is an upper bound and 2 a lower bound.

(b) Given $x < 5$, define[7] $s := \max\{\frac{1}{2}(x+5), 4\}$. Observe that $x < s < 5$ from which $s \in S$ is *larger* than x. It follows that x is *not* an upper bound for S, and that 5 is the least such.

Similarly, if $y > 2$, define $t := \min\{\frac{1}{2}(y+2), 4\}$ to see that $t \in S$ is *smaller* than y, which cannot therefore be a lower bound for S.

We conclude that $\sup S = 5$ and $\inf S = 2$.



We are assuming something quite important here!

Axiom 4.7 (Completeness of $\mathbb{R}$). If $S \subseteq \mathbb{R}$ is non-empty and bounded above, then $\sup S$ exists (and is a real number!).

It is this property that distinguishes the real numbers from the rationals.[8] Note that every bounded set S of *rational* numbers has a supremum; the issue is that $\sup S$ *might not be rational*!

[7]The number 4 is merely an arbitrary element to make sure $s \in S$ in case x were huge and negative!

[8]If you've studied abstract algebra, then a more rigorous statement should make sense: every ordered field with $0 \ne 1$ and which satisfies the completeness axiom is isomorphic to the real numbers.

Example (4.4 cont). The set $S = \mathbb{Q} \cap [0, \sqrt{2})$ has $\sup S = \sqrt{2}$. We check conditions (a), (b) in Definition 4.6.

(a) Certainly $\sqrt{2}$ is an upper bound for S, since every element is less than $\sqrt{2}$.

(b) If $x < \sqrt{2}$ is given, then our previous argument says there exists some $s_N \in S$ for which $s_N > x$. Plainly x isn't an upper bound.

In conclusion, $\sqrt{2}$ is the smallest upper bound for S.

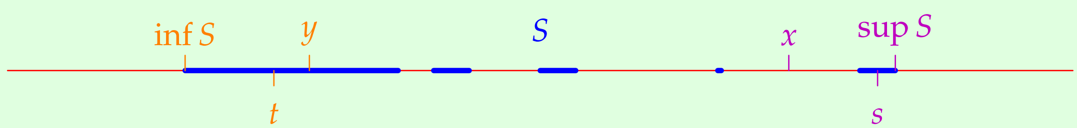
Consider the contrapositive of part (b) of Definition 4.6 after replacing M with x.

> If $x < \sup S$, then x is *not* an upper bound for S.

If we unpack this further, we recover a useful existence result. Indeed this is precisely what we did in both previous examples.

Lemma 4.8. 1. *If $x < \sup S$, then $\exists s \in S$ such that $s > x$.*

2. *If $y > \inf S$, then $\exists t \in S$ such that $t < y$.*



This observation will be used repeatedly, so make sure it is well understood.

Examples 4.9. We state the following without proof or calculation. You should be able to justify all these statements using the definition, or by mirroring the above examples.

1. A bounded set has many possible bounds, but only one supremum or infimum.
2. If S has a maximum, then $\max S = \sup S$. Similarly $\min S = \inf S$ if a minimum exists.
3. $S = \mathbb{Q} \cap (\pi, 4)$ has $\sup S = 4$ and $\inf S = \pi$.
4. $S = \{\frac{1}{n} : n \in \mathbb{N}\} = \{\ldots, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, 1\}$ has $\sup S = \max S = 1$, $\inf S = 0$, and no minimum.
5. $S = \bigcup_{n=1}^{\infty} [n, n + \frac{1}{2}) = [1, 1.5) \cup [2, 2.5) \cup [3, 3.5) \cup \cdots$ has $\inf S = 1$. It is not bounded above.
6. $S = \bigcap_{n=1}^{\infty} [\frac{1}{n}, 1 + \frac{1}{n})$ has $\inf S = 1 = \sup S$ since $S = \{1\}$.

The completeness axiom only asserts the existence of the supremum of a bounded set. By reflecting across zero (see Exercise 9), we obtain the same thing for the infimum.

Theorem 4.10 (Existence of Infima). *If $S \subseteq \mathbb{R}$ non-empty and bounded below, then $\inf S \in \mathbb{R}$ exists.*

The Archimedean Property and the Density of the Rationals

We finish this section by discussing the distribution of the rational numbers among the real numbers.

Theorem 4.11 (Archimedean Property). *If $b > 0$ is a real number, then $\exists n \in \mathbb{N}$ such that $n > b$. Equivalently:*[9] $a, b > 0 \implies \exists n \in \mathbb{N}$ *such that* $an > b$.

In this result we assume nothing about $\mathbb{R}$ except that is an ordered field satisfying the completeness axiom and $0 \neq 1$. The natural numbers in this context are *defined* as the subset

$$\mathbb{N} = \{1, 1+1, 1+1+1, \ldots\} \subseteq \mathbb{R}$$

Proof. Suppose the result were false. Then $\exists b > 0$ such that $n \leq b$ for all $n \in \mathbb{N}$; that is, $\mathbb{N}$ is bounded above! By completeness, $\sup \mathbb{N}$ exists, and we trivially see that

$$0 < 1 \implies \sup \mathbb{N} < \sup \mathbb{N} + 1 \implies \sup \mathbb{N} - 1 < \sup \mathbb{N}$$

By Lemma 4.8, $\exists n \in \mathbb{N}$ such that $n > \sup \mathbb{N} - 1$. But then $\sup \mathbb{N} < n + 1$ which is clearly a natural number! Thus $\sup \mathbb{N}$ is not an upper bound for $\mathbb{N}$: contradiction. ∎

The use of completeness is *necessary*: there exist non-Archimedean ordered fields!

Corollary 4.12 (Density of $\mathbb{Q}$ in $\mathbb{R}$). *Between any two real numbers, there exists a rational number.*

The idea is simple: given $a < b$, stretch the interval by an integer factor n until it contains an integer m, before dividing by n to obtain $a < \frac{m}{n} < b$. The Archimedean property shows the existence of m, n.

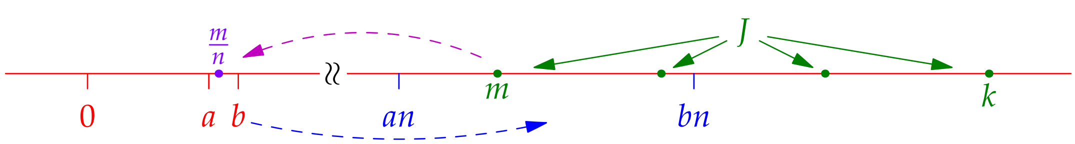
Proof. WLOG suppose $0 \leq a < b$. The Archimedean property applied to $\frac{1}{b-a} > 0$ says

$$\exists n \in \mathbb{N} \text{ such that } n > \tfrac{1}{b-a}$$

A second application says $\exists k \in \mathbb{N}$ such that $k > an$. Now consider

$$J := \{j \in \mathbb{N} : an < j \leq k\}$$

and define $m = \min J$: this exists since J is a finite non-empty set of natural numbers.[10]



Clearly $m > an > m - 1$, since $m = \min J$. But then $m \leq an + 1 < bn$. We conclude that

$$an < m < bn \implies a < \frac{m}{n} < b$$ ∎

It is immediate that any interval (a, b) now contains *infinitely many* rational numbers.

[9] Just replace b with $\frac{b}{a}$.

[10] This part of the argument is needed because, in this context, we haven't established the well-ordering property of $\mathbb{N}$ (equivalent to Peano's fifth axiom).

Exercises 4. 1. Decide if each set is bounded above and/or below. If it is, *state* its supremum and/or infimum (no working is required).

(a) $(0,1)$ (b) $\{2,7\}$ (c) $\{0\}$

(d) $\bigcup_{n=1}^{\infty}[2n,2n+1]$ (e) $\{1-\frac{1}{3^n}:n\in\mathbb{N}\}$ (f) $\{r\in\mathbb{Q}:r^2<2\}$

(g) $\bigcup_{n=1}^{\infty}(1-\frac{1}{n},1+\frac{1}{n})$ (h) $\{\frac{1}{n}:n\in\mathbb{N}\text{ and }n\text{ is prime}\}$ (i) $\{\cos(\frac{n\pi}{3}):n\in\mathbb{N}\}$

2. Modelling Example 4.4, *sketch* an argument that $S=\mathbb{Q}\cap(\pi,4]$ has no minimum.
(*Hint: let s_n be π rounded up to n decimal places*)

3. Let S be a non-empty, bounded subset of $\mathbb{R}$.
   (a) Prove that $\inf S\le\sup S$.
   (b) What can you say about S if $\inf S=\sup S$?

4. Let S and T be non-empty subsets of $\mathbb{R}$ with the property that $s\le t$ for all $s\in S$ and $t\in T$.
   (a) Prove that S is bounded above and T bounded below.
   (b) Prove that $\sup S\le\inf T$.
   (c) Give an example of such sets S,T where $S\cap T$ is non-empty.
   (d) Give an example of such sets S,T where $S\cap T$ is empty, and $\sup S=\inf T$.

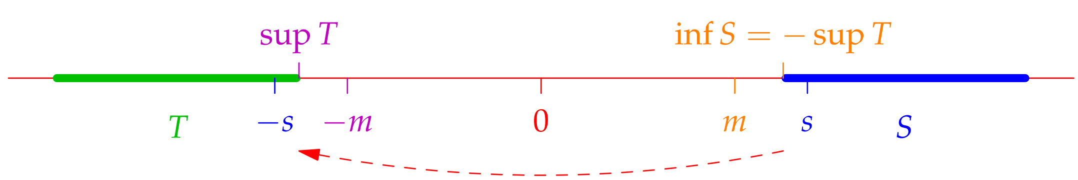
5. Prove that if $a>0$ then there exists $n\in\mathbb{N}$ such that $\frac{1}{n}<a<n$.

6. Let $\mathbb{I}=\mathbb{R}\setminus\mathbb{Q}$ be the set of *irrational* numbers. Given real numbers $a<b$, prove that there exists $x\in\mathbb{I}$ such that $a<x<b$.
(*Hint: First show* $\{r+\sqrt{2}:r\in\mathbb{Q}\}\subseteq\mathbb{I}$)

7. Let A,B be non-empty bounded subsets of $\mathbb{R}$, and let S be the set of all sums
$$S:=\{a+b:a\in A,b\in B\}$$
   (a) Prove that $\sup S=\sup A+\sup B$.
   (b) Prove that $\inf S=\inf A+\inf B$.

8. Show that $\sup\{r\in\mathbb{Q}:r<a\}=a$ for each $a\in\mathbb{R}$.

9. We prove Theorem 4.10 on the existence of the infimum.
Let $S\subseteq\mathbb{R}$ be non-empty and let m be a lower bound for S. Define $T=\{t\in\mathbb{R}:-t\in S\}$ by reflecting S across zero.



   (a) Prove that $-m$ is an upper bound for T.
   (b) By completeness (Axiom 4.7), $\sup T$ exists. Prove that $\inf S=-\sup T$ by verifying Definition 4.6 parts 2(a) and (b).

5 The Symbols $\pm\infty$

Thus far the only subsets of the real numbers that have a supremum are those which are *non-empty* and *bounded above*. In this very short section, we introduce the ∞-symbol to provide all subsets of the real numbers with both a supremum and an infimum.

Definition 5.1. Let $S \subseteq \mathbb{R}$ be any subset. If S is bounded above/below, then $\sup S/\inf S$ are as in Definition 4.6. Otherwise:

1. We write $\sup S = \infty$ if S is *unbounded above*, that is

$$\forall x \in \mathbb{R}, \exists s \in S \text{ such that } s > x$$

2. We write $\inf S = -\infty$ if S is *unbounded below*,

$$\forall y \in \mathbb{R}, \exists t \in S \text{ such that } t < y$$

3. By convention, $\sup \varnothing := -\infty$ and $\inf \varnothing := \infty$, though these will rarely be of use to us.

The symbols $\pm\infty$ have *no other meaning* (as yet): in particular, they are *not numbers*! If one is willing to abuse notation and write $x < \infty$ and $y > -\infty$ for any real numbers x, y, then the conclusions of Lemma 4.8 are precisely statements 1 & 2 in the above definition!

Examples 5.2. 1. $\sup \mathbb{R} = \sup \mathbb{Q} = \sup \mathbb{Z} = \sup \mathbb{N} = \infty$, since all are unbounded above. We also have $\inf \mathbb{R} = \inf \mathbb{Q} = \inf \mathbb{Z} = -\infty$ (recall that $\inf \mathbb{N} = \min \mathbb{N} = 1$).

2. If $a < b$, then *any* interval $[a, b]$, (a, b), $[a, b)$ or $(a, b]$ has supremum b and infimum a, even if one end is infinite. For example,

$$S = (7, \infty) = \{x \in \mathbb{R} : x > 7\}$$

has $\sup S = \infty$ and $\inf S = 7$.

3. Let $S = \{x \in \mathbb{R} : x^3 - 4x < 0\}$. With a little factorization, we see that

$$x^3 - 4x = x(x-2)(x+2) < 0 \iff x < -2 \text{ or } 0 < x < 2$$

It follows that $S = (-\infty, -2) \cup (0, 2)$, from which $\sup S = 2$ and $\inf S = -\infty$.

Exercises 5. 1. Give the infimum and supremum of each of the following sets:

(a) $\{x \in \mathbb{R} : x < 0\}$
(b) $\{x \in \mathbb{R} : x^3 \leq 8\}$
(c) $\{x^2 : x \in \mathbb{R}\}$
(d) $\{x \in \mathbb{R} : x^2 < 8\}$

2. Let $S \subseteq \mathbb{R}$ be non-empty, and let $-S = \{-s : s \in S\}$. Prove that $\inf S = -\sup(-S)$.

3. Let $S, T \subseteq \mathbb{R}$ be non-empty such that $S \subseteq T$. Prove that $\inf T \leq \inf S \leq \sup S \leq \sup T$.

4. If $\sup S < \inf S$, what can you say about S?

6 A Development of $\mathbb{R}$ (non-examinable)

The comment in footnote 8 essentially constitutes a *synthetic* definition of the real numbers: there is essentially just one set with the required properties. It is nice, however, to be able to provide an explicit construction. The following approach uses *Dedekind cuts.*

First one defines $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$. Use Peano's axioms and proceed as in sections 1 and 2. The operations $+, \cdot$ and $\leq$ are defined, first on $\mathbb{N}$ and then for $\mathbb{Z}$ and $\mathbb{Q}$ building on the concepts for the integers.

Definition 6.1. A *Dedekind cut* α^* is a non-empty proper subset of $\mathbb{Q}$ with the following properties:

1. If $r \in \alpha^*$ and $s \in \mathbb{Q}$ with $s < r$, then $s \in \alpha^*$.
2. α^* has no maximum.

Define $\mathbb{R}$ to be the set of all Dedekind cuts!

The rough idea is that a real number α corresponds to the Dedekind cut α^* of all *rational numbers less than* α. While this is the idea, it doesn't stand up as a *definition* due to circular logic: α cannot be defined in terms of itself!

Examples 6.2. 1. For any *rational number* r, the corresponding *real number* is the Dedekind cut

$$r^* = \{x \in \mathbb{Q} : x < r\}$$

For instance $4^* = \{x \in \mathbb{Q} : x < 4\}$ is the Dedekind cut definition of the *real number* 4.

2. It is a little trickier to explicitly define Dedekind cuts corresponding to irrational numbers, though some are relatively straightforward. For instance the real number $\sqrt{2}$ would be the Dedekind cut

$$\sqrt{2}^* = \{x \in \mathbb{Q} : x < 0 \text{ or } x^2 < 2\}$$

It remains to *prove* that the set of Dedekind cuts satisfies all the axioms of a complete ordered field. The full details are too much for us, so here is a rough overview.

- Define the ordering of Dedekind cuts via

  $$\alpha^* \leq \beta^* \iff \alpha^* \subseteq \beta^*$$

  One can now prove axioms O1–O3 and that the ordering corresponds to that of $\mathbb{Q}$.

- Define addition of cuts via

  $$\alpha^* + \beta^* := \{a + b : a \in \alpha^*, b \in \beta^*\}$$

  This suffices to prove the addition axioms and O4: a careful definition of $-\alpha^*$ is required.

- Multiplication is horrible: if $\alpha^*, \beta^* \geq 0$ then

  $$\alpha^*\beta^* := \{ab : a \geq 0, a \in \alpha^*, b \geq 0, b \in \beta^*\} \cup \{q \in \mathbb{Q} : q < 0\}$$

  which may be carefully extended to cover situations when α^* or $\beta < 0$. Once can then prove the multiplication axioms, the final order axiom O5, and the distributive axiom.

- The completeness axiom must also be verified, though it comes almost for free! If $A \subseteq \mathbb{R}$ (so that A is a set of Dedekind cuts), then the supremum of A is

$$\sup A = \bigcup_{\alpha^* \in A} \alpha^*$$

An alternative approach to $\mathbb{R}$ using sequences of rational numbers will be given later in the course.

Exercises 6. 1. Show that if α^*, β^* are Dedekind cuts, then so is

$$\alpha^* + \beta^* = \{r_1 + r_2 : r_1 \in \alpha^*, r_2 \in \beta^*\}$$

2. Let α^*, β^* be Dedekind cuts and define the 'product':

$$\alpha^* \cdot \beta^* = \{r_1 r_2 : r_1 \in \alpha^*, r_2 \in \beta^*\}$$

   (a) Calculate some 'products' using the cuts $0^*, 1^*$ and $(-1)^*$.

   (b) Discuss why this definition of 'product' is unsatisfactory for defining multiplication in $\mathbb{R}$.

3. We verify the Archimedean property (Theorem 4.11) using the Dedekind cut definition of $\mathbb{R}$ (it is somewhat easier since the unboundedness of $\mathbb{N}$ and $\mathbb{Q}$ are baked in).

   (a) Explain why every cut β^* is bounded above by some rational number.
   (*Hint: if β^* satisfies Definition 6.1 parts 1 & 2 but is unbounded above, then what is it?*)

   (b) If $\beta^* > 0^*$ is a positive cut bounded above by $\frac{p}{q}$ with $p, q \in \mathbb{N}$, show that $n := p + 1$ corresponds to a cut for which $n^* > \beta^*$.