Mathematical Analysis

Chapter 2
The Real Numbers

P. Boily (uOttawa)

Winter 2022

Overview

In a course on real analysis, the fundamental object of study is the set of real numbers.

In this chapter, we

- introduce $\mathbb{R}$ and some of its important properties,
- discuss the cardinality of sets, and
- provide a first analytical result, whose proof will serve as an introduction to the discipline.

Outline

2.1 – Hierarchy of Number Systems

In this first course, **analysis** is a theory on real numbers $\mathbb{R}$, that is, the objects with which we work are **real numbers**, **real sets**, and **real functions**.

We will see at a later stage that we can conduct analysis on any **metric space** (such as $\mathbb{R}^n$ and $\mathbb{C}$, for instance).

There is a natural hierarchy amongst number sets, which you have no doubt encountered in your courses:

$$\mathbb{N}^\times \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{A} \subsetneq \mathbb{R} \subsetneq \mathbb{C}.$$

The **positive integers** $\mathbb{N}^\times$ are the counting numbers; **zero** is added to $\mathbb{N}^\times$ to form $\mathbb{N}$, in which all equations $x+a=b$, $b\geq a\in\mathbb{N}^\times$ have a solution.

Similarly, the **integers** $\mathbb{Z}$ are built by adding new numbers to $\mathbb{N}$ in order for all equations of the form $x+a=b$, $a,b\in\mathbb{N}$ to have solutions.

For the **rational numbers** $\mathbb{Q}$, the equations in question have the form $ax+b=0$, $a,b\in\mathbb{Z}$, $b\neq 0$.

For the **algebraic numbers** $\mathbb{A}$, we are looking at equations of the form

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0,\quad a_i\in\mathbb{Q},$$

and for **complex numbers** $\mathbb{C}$, equations of the form

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0,\quad a_i\in\mathbb{R}.$$

In other words, number sets are generally easy to construct once we have the right building blocks... except when it comes to the **real numbers** $\mathbb{R}$.

In this chapter and the next, we will introduce concepts that will allow us to **formally define** $\mathbb{R}$.

In what follows, we will make use of the following axiom about the set $\mathbb{N}$.

Axiom. (WELL-ORDERING PRINCIPLE)
Any non-empty subset of $\mathbb{N}$ *has a smallest element.*

We shall discuss how to define the "smallest" element of a set momentarily. We shall also discuss how to measure the "size" of a set in Section 2.2: for the moment, we will leave you with the following tantalizing remark: $\mathbb{Q}$ is infinite, but **it contains infinitely more holes than it does elements**.

2.1.1 – Field and Order Properties of $\mathbb{R}$; Completeness

A **field** F is a set endowed with two binary operations: an **addition**

$$+ : F \times F \to F, \quad +(a,b) = a+b$$

and a **multiplication**

$$\cdot : F \times F \to F, \quad \cdot(a,b) = ab,$$

which satisfy the 9 **field properties**:

(A1) **commutativity of $+$:** $\forall a, b \in F$, $a + b = b + a$;

(A2) **associativity of $+$:** $\forall a, b, c \in F$, $(a + b) + c = a + (b + c)$;

(A3) **existence of neutral element for $+$:** $\exists 0 \in F$, $\forall a \in F$, $a + 0 = a$;

(A4) **inverse with respect to $+$:** $\forall a \in F$, $\exists! b \in F$, $a + b = 0$;

(M1) **commutativity of $\cdot$:** $\forall a, b \in F$, $ab = ba$

(M2) **associativity of $\cdot$:** $\forall a, b, c \in F$, $(ab)c = a(bc)$

(M3) **existence of neutral element for $\cdot$:** $\exists 1 \in F$, $\forall a \in F$, $1a = a$

(M4) **inverse with respect to $\cdot$:** $\forall a \in F^{\times}$, $\exists! b \in F$, $ab = 1$

(D1) **distributivity of $\cdot$ over $+$:** $\forall a, b, c \in F$, $a(b + c) = ab + ac$

Examples: $\mathbb{Q}$ is a field; $\mathbb{N}$ is not a field since (A4) is not satisfied for $x = 1 \in \mathbb{N}$, say; $\mathbb{Z}$ is not a field since (M4) is not satisfied for $x = 2$, say.

An **order** on a set F is a binary relation "$<$" satisfying the **order properties**:

(O1) **trichotomy:** $\forall a,b,c\in F$, $a<b$ or $a=b$ or $b<a$;

(O2) **transitivity:** $\forall a,b,c\in F$, if $a<b$ and $b<c$, then $a<c$.

(O3) $\forall a,b,c\in F$, if $a<b$, then $a+c<b+c$.

(O4) **(specific to $\mathbb{R}$):** $\forall a,b,c\in \mathbb{R}$, if $a<b$ and $c>0$, then $ac<bc$.

Examples:

1. the relation "is smaller than" is an order relation on $\mathbb{N},\mathbb{Z},\mathbb{Q}$;

2. the relation "is a subset of" is not an order on $\wp(\mathbb{N})$ since

$$\{1,2\}\not\subseteq\{1,3\},\quad \{1,2\}\neq\{1,3\},\quad \{1,3\}\not\subseteq\{1,2\}.$$

Let $(F, <)$ be an ordered set and $S \subseteq F$. If $a < b$ or $a = b$, we write $a \leq b$.

The element $u \in F$ is an **upper bound of** S if $s \leq u$ for all $s \in S$. In that case, we say that S is **bounded above**.

If u is the smallest upper bound of S, we say that it is the **supremum** of S, denoted $u = \sup S$.

The element $v \in F$ is a **lower bound of** S if $v \leq s$ for all $s \in S$. In that case, we say that S is **bounded below**.

If v is the largest lower bound of S, we say that it is the **infimum** of S, denoted $u = \inf S$.

If the set S is bounded both above and below, we say that it is **bounded**.

Example: If $S = \{x \in \mathbb{Q} \mid 2 < x < 3\}$, then $\inf S = 2$.

Proof. The rational number $v = 2$ is a lower bound of S since $2 = v < x$ for all $x \in S$ (but so are $v = -1$ and $v = 1.5$). Hence $\inf S \geq 2$.

To show that 2 is indeed the greatest lower bound, we suppose that $u = \inf S > 2$ and derive a contradiction. As we already know that $\inf S \geq 2$, this will only leave one possibility: $\inf S = 2$.

By assumption, there exists $0 < \varepsilon < 1$ in $\mathbb{Q}$ such that $u = 2 + \varepsilon$. Find a rational number $u^* \in (2, u)$. By definition, $u^* \in S$, since $3 > u^* > 2$. But $u > u^*$, and so u cannot be a lower bound of S, which contradicts the hypothesis that $u = \inf S$. Thus $\inf S \not> 2$ and $\inf S = 2$. ■

This "proof" rests on thin ice: it assumes that

1. the infimum exists in the first place;

2. if the infimum exists, it is a rational number, and

3. a rational number can be found between any two distinct rationals.

These are valid **in this specific case**, but not in general. More on this later.

Example: If $S = \mathbb{N}$, then $\inf S = 1$.

Proof. The integer $v = 1$ is a lower bound since $1 = v \leq n$ for all $n \in \mathbb{N}$, so $\inf \mathbb{N} \geq 1$. But any number above 1 cannot be a lower bound of $\mathbb{N}$ since it would not be smaller than 1. Thus, $\inf S = 1$. ■

A set $(F, <)$ is **complete** if any non-empty bounded subset $S \subseteq F$ has a supremum and an infimum.

Example: $\mathbb{Q}$ is not complete.

Proof. Consider the subset $S = \{x \in \mathbb{Q}^+ \mid 2 < x^2 < 3\}$. Since $1.5 \in \mathbb{Q}^+$, then $1.5^2 = 2.25 \in \mathbb{Q}^+$. We have $2 < 1.5^2 = 2.25 < 3$, so $1.5 \in S$, and thus $S \neq \varnothing$. Furthermore, S is bounded above by 3 since $3^2 > 3$ and bounded below by 1 since $1^2 < 1$, so S is bounded.

We will see shortly that S has no supremum/infimum in $\mathbb{Q}$ (since no rational x is such that $x^2 = 2$ or $x^2 = 3$). Thus $\mathbb{Q}$ is not complete. ■

The set $\mathbb{R}$ of **real numbers** is the smallest complete ordered field containing $\mathbb{N}$, with order $a < b \Longleftrightarrow b - a > 0$.

2.1.2 – Archimedean Property

Classically, $\mathbb{R}$ is constructed using **Dedekind cuts** or **Cauchy sequences**: in effect, $\mathbb{R}$ is constructed by "filling the holes" of $\mathbb{Q}$.

We will discuss Cauchy sequences in Chapter 3 and provide the outline of $\mathbb{R}$'s construction in an interlude.

For now, we assume that $\mathbb{R}$ is available and that is satisfies the properties mentioned previously.

The course's first result seems intuitively "obvious" but its proof is not.

Theorem 1. (Archimedean Property)
Let $x \in \mathbb{R}$. Then $\exists n_x \in \mathbb{N}^{\times}$ such that $x < n_x$.

Proof. Suppose that there is no such integer. Then $x \geq n \ \forall n \in \mathbb{N}$.

Consequently, x is an upper bound of $\mathbb{N}^\times$. But $\mathbb{N}^\times$ is a non-empty subset of $\mathbb{R}$. Since $\mathbb{R}$ is complete, $\alpha = \sup \mathbb{N}^\times$ exists.

By definition of the supremum (the smallest upper bound), $\alpha - 1$ is not an upper bound of $\mathbb{N}^\times$ (otherwise α would not be the smallest upper bound, as $\alpha - 1 < \alpha$ would be a smaller upper bound).

Since $\alpha - 1$ is not an upper bound of $\mathbb{N}^\times$, $\exists m \in \mathbb{N}^\times$ such that $\alpha - 1 < m$. Using the properties of $\mathbb{R}$, we must then have $\alpha < m + 1 \in \mathbb{N}^\times$; that is, α is not an upper bound of $\mathbb{N}^\times$.

This contradicts the fact that $\alpha = \sup \mathbb{N}^\times$, and so, since $\mathbb{N}^\times \neq \varnothing$, x cannot be an upper bound of $\mathbb{N}^\times$. Thus $\exists n_x \in \mathbb{N}^\times$ such that $x < n_x$. ■

Example: Show that $\inf\{\frac{1}{n} \mid n \in \mathbb{N}^\times\} = 0$.

Proof. Since $0 \leq \frac{1}{n}$ for all $n \in \mathbb{N}^\times$, 0 is a lower bound of the set. Suppose that $\varepsilon > 0$ is also a lower bound. Then $\varepsilon \leq \frac{1}{n}$ for all $n \in \mathbb{N}^\times$, which means that $n \leq \frac{1}{\varepsilon}$ for all $n \in \mathbb{N}^\times$. This contradicts the Archimedean Property, so 0 is the smallest lower bound of the set. ■

Theorem 2. (Variants of the Archimedean Property)
Let $x, y \in \mathbb{R}^+$. Then $\exists n_1, n_2, n_3 \geq 1$ such that

1. $x < n_1 y$;
2. $0 < \frac{1}{n_2} < y$, *and*
3. $n_3 - 1 \leq x < n_3$.

Proof.

1. Let $z = \frac{x}{y} > 0$. By the Archimedean property, $\exists n_1 \geq 1$ such that $z = \frac{x}{y} < n_1$. Then $x < n_1 y$.

2. If $x = 1$, then part 1 implies $\exists n_2 \geq 1$ such that $0 < 1 < n_2 y$. Then $0 < \frac{1}{n_2} < y$.

3. Let $L = \{m \in \mathbb{N}^\times : x < m\}$. By the Archimedean property, $L \neq \varnothing$. Indeed, there is at least one $n \geq 1$ such that $x < n$. By the well-ordering principle, L has a smallest element, say $m = n_3$. Then $n_3 - 1 \notin L$ (otherwise, $n_3 - 1$ would be the least element of L, which it is not) and so $n_3 - 1 \leq x < n_3$.

There are other variants, but these are the ones we will use the most. ■

It is thus always possible to find an integer greater than any specified real number. This result is extremely useful – we use it next to show the existence of **irrational numbers**.

Corollary. The positive root of $x^2 = 2$ lies in $\mathbb{R}$ but not in $\mathbb{Q}$.

Proof. We first show that any solution of $x^2 = 2$ cannot be rational.

Suppose the equation $x^2 = 2$ has a rational positive root $r = p/q$, with $\gcd(p, q) = 1$. Then $p^2/q^2 = 2$, or $p^2 = 2q^2$. Hence p^2 is even, and so p is also even. Indeed, if $p = 2k + 1$ is odd, then so is $p^2 = 2(2k^2 + 2k) + 1$.

Set $p = 2m$. Then $(2m)^2 = 2q^2$, or $2m^2 = q^2$. Thus q^2 and q are even. Consequently, both p and q are even, which contradicts the hypothesis $\gcd(p, q) = 1$. The equation $r^2 = 2$ cannot then have a solution in $\mathbb{Q}$.

But we have not yet shown that the equation has a solution in $\mathbb{R}$.

Consider the set $S = \{s \in \mathbb{R}^+ : s^2 < 2\}$, where $\mathbb{R}^+$ denotes the set of positive real numbers. This set in not empty as $1 \in S$. Furthermore, S is bounded above by 2. Indeed, if $t \geq 2$, then $t^2 \geq 4 > 2$, whence $t \notin S$.

By completeness of $\mathbb{R}$, $u = \sup S \geq 1$ exists. It is enough to show that neither $u^2 < 2$ and $u^2 > 2$ can hold. The only remaining possibility is that $u^2 = 2$.

- If $u^2 < 2$, then $\frac{2u+1}{2-u^2} > 0$. By the Archimedean property, $\exists n > 0$ such that $\frac{2u+1}{2-u^2} < n$. By re-arranging the terms, we get

$$0 < \frac{1}{n}(2u+1) < 2 - u^2.$$

Then

$$\left(u+\frac{1}{n}\right)^2 = u^2+\frac{2u}{n}+\frac{1}{n^2} \quad \leq \quad u^2+\frac{2u}{n}+\frac{1}{n}$$
$$= \quad u^2+\frac{1}{n}(2u+1) < u^2+2-u^2 = 2.$$

Since $(u+\frac{1}{n})^2 < 2$, $u+\frac{1}{n} \in S$. But $u < u+\frac{1}{n}$; u is then not an upper bound of S, which contradicts the fact that $u = \sup S$. Thus $u^2 \not< 2$.

- If $u^2 > 3$, then $\frac{2u}{u^2-2} > 0$. By the Archimedean property, $\exists n > 0$ such that $\frac{2u}{u^2-3} < n$. By re-arranging the terms, we get

$$0 > -\frac{2u}{n} > 2-u^2.$$

Then

$$\left(u-\frac{1}{n}\right)^2 = u^2-\frac{2u}{n}+\frac{1}{n^2} > u^2-\frac{2u}{n} > u^2+2-u^2 = 2.$$

Since $(u-\frac{1}{n})^2 > 2$, $u-\frac{1}{n}$ is an upper bound of S. But $u > u-\frac{1}{n}$; u can not then be the supremum of S, which is a contradiction. Thus $u^2 \not> 2$.

That leaves only one alternative (since we know that $u \in \mathbb{R}$): $u^2 = 2$, and $u = \sqrt{2} \in \mathbb{R}$. ■

From this point on, when we mention the Archimedean Property, we mean one of the four variants from Theorems 1 and 2.

2.1.3 – Absolute Value and Useful Inequalities

The real numbers enjoy another set of useful and interesting properties.

Theorem 3. (Bernoulli's Inequality)
Let $x \geq -1$. *Then* $(1+x)^n \geq 1+nx$, $\forall n \in \mathbb{N}$.

Proof. We prove the result by induction on n.

- If $n=1$, then $(1+x)^1 = 1+x \geq 1+1x$.
- Suppose that the result is true for $n=k$, that is $(1+x)^k \geq 1+kx$. We have to show that it is also true for $n=k+1$.

But

$$\begin{aligned}(1+x)^{k+1} &= (1+x)^k(1+x) \\ \boxed{\text{Ind. Hyp.}} &\geq (1+kx)(1+x) \\ &= 1+(k+1)x+kx^2 \\ &\geq 1+(k+1)x,\end{aligned}$$

which completes the proof. ■

Note: at first glance, it might appear that we did not use the hypothesis that $x \geq -1$. But the assumption is essential – if $1+x<0$, the use of the Induction Hypothesis in the string of inqualities is invalid.

Theorem 4. (Cauchy's Inequality)
If $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are real numbers, then

$$\left(\sum a_i b_i\right)^2 \leq \left(\sum a_i^2\right)\left(\sum b_i^2\right).$$

(The indices are understood to run from 1 to n in what follows.) Furthermore, if $b_j \neq 0$ for one of $1 \leq j \leq n$, then equality holds if and only if $\exists s \in \mathbb{R}$ such that $a_i = sb_i$ for all $i = 1, \ldots, n$.

Proof. For any $t \in \mathbb{R}$,

$$0 \leq \sum (a_i + tb_i)^2 = \sum a_i^2 + 2t \sum a_i b_i + t^2 \sum b_i^2.$$

The right-hand side of this inequality is a polynomial of degree 2 in t.

It is always greater than or equal to 0: it has at most 1 real root, i.e. its discriminant

$$\left(2\sum a_ib_i\right)^2-4\left(\sum a_i^2\right)\left(\sum b_i^2\right)\leq 0,$$

and so

$$\left(\sum a_ib_i\right)^2\leq\left(\sum a_i^2\right)\left(\sum b_i^2\right).$$

If all the b_i are 0, the equality holds trivially, as both the left and right side of the Cauchy inequality are 0.

So suppose $b_i\neq 0$ for at least one of the values j between 1 and n. We have two statements to prove.

If $a_i = sb_i$ for all $i = 1, \ldots, n$ and $s \in \mathbb{R}$ is fixed then

$$\begin{aligned}\left(\sum a_i b_i\right)^2 &= \left(\sum s b_i^2\right)^2 = s^2\left(\sum b_i^2\right)^2 = s^2\left(\sum b_i^2\right)\left(\sum b_i^2\right)\\ &= \left(\sum s^2 b_i^2\right)\left(\sum b_i^2\right) = \left(\sum a_i^2\right)\left(\sum b_i^2\right).\end{aligned}$$

On the other hand, if

$$\left(\sum a_i b_i\right)^2 = \left(\sum a_i^2\right)\left(\sum b_i^2\right)$$

then

$$4\left(\sum a_i b_i\right)^2 - 4\left(\sum a_i^2\right)\left(\sum b_i^2\right) = 0.$$

But the left-hand side of this expression is the discriminant of the following polynomial of degree 2 in t:

$$\sum(a_i + tb_i)^2 = \sum a_i^2 + 2t\sum a_ib_i + t^2\sum b_i^2.$$

Since the discriminant is 0, the polynomial has a unique root, say $t = -s$,

$$\therefore \sum(a_i - sb_i)^2 = 0.$$

Since $(a_i - sb_i)^2 \geq 0$ for all $i = 1, \ldots, n$, then

$$\begin{aligned} (a_i - sb_i)^2 = 0 &\quad \text{for all } i = 1, \ldots, n \\ \therefore a_i - sb_i = 0 &\quad \text{for all } i = 1, \ldots, n \\ \therefore a_i = sb_i &\quad \text{for all } i = 1, \ldots, n. \qquad \blacksquare \end{aligned}$$

Theorem 5. (Triangle Inequality) *If* $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{R}$*,*

$$\left(\sum (a_i + b_i)^2\right)^{1/2} \leq \left(\sum a_i^2\right)^{1/2} + \left(\sum b_i^2\right)^{1/2}.$$

Furthermore, if $b_j \neq 0$ *for one of* $1 \leq j \leq n$*, then equality holds if and only if* $\exists s \in \mathbb{R}$ *such that* $a_i = sb_i$ *for all* $i = 1, \ldots, n$*.*

Proof. Taking the square root on both sides of the inequality below yields the desired result:

$$\begin{aligned}
\sum (a_i + b_i)^2 &= \sum a_i^2 + 2\sum a_i b_i + \sum b_i^2 \\
\boxed{\text{Cauchy Ineq.}} &\leq \sum a_i^2 + 2\left(\sum a_i^2\right)^{1/2}\left(\sum b_i^2\right)^{1/2} + \sum b_i^2 \\
&= \left(\left(\sum a_i^2\right)^{1/2} + \left(\sum b_i^2\right)^{1/2}\right)^2.
\end{aligned}$$

If all the b_i are 0, the equality holds trivially, as both the left and right side of the Triangle Inequality are $\left(\sum a_i^2\right)^{1/2}$.

So suppose $b_i \neq 0$ for at least one of the values j between 1 and n. If $a_i = sb_i$ for all $i = 1, \ldots, n$ and $s \in \mathbb{R}$ is fixed, then equality holds since:

$$\begin{aligned}
\left(\sum (a_i + b_i)^2\right)^{1/2} &= \left(\sum (sb_i + b_i)^2\right)^{1/2} = \left(\sum (s+1)^2 b_i^2\right)^{1/2} \\
&= \left((s+1)^2 \sum b_i^2\right)^{1/2} = (s+1)\left(\sum b_i^2\right)^{1/2}, \text{ and} \\
\left(\sum a_i^2\right)^{1/2} + \left(\sum b_i^2\right)^{1/2} &= \left(\sum s^2 b_i^2\right)^{1/2} + \left(\sum b_i^2\right)^{1/2} \\
&= s\left(\sum b_i^2\right)^{1/2} + \left(\sum b_i^2\right)^{1/2} = (s+1)\left(\sum b_i^2\right)^{1/2}.
\end{aligned}$$

On the other hand, if

$$\left(\sum(a_i+b_i)^2\right)^{1/2}=\left(\sum a_i^2\right)^{1/2}+\left(\sum b_i^2\right)^{1/2}$$

then

$$\sum(a_i+b_i)^2=\left(\left(\sum a_i^2\right)^{1/2}+\left(\sum b_i^2\right)^{1/2}\right)^2.$$

Developing both sides of this expression yields

$$\sum a_i^2+2\sum a_ib_i+\sum b_i^2=\sum a_i^2+2\left(\sum a_i^2\right)^{1/2}\left(\sum b_i^2\right)^{1/2}+\sum b_i^2,$$

or simply

$$\sum a_ib_i=\left(\sum a_i^2\right)^{1/2}\left(\sum b_i^2\right)^{1/2}.$$

Elevating both sides to the second power yields

$$\left(\sum a_ib_i\right)^2 = \left(\sum a_i^2\right)\left(\sum b_i^2\right).$$

By Cauchy's Inequality, $\exists s \in \mathbb{R}$ such that $a_i = sb_i$ for all $i = 1, \ldots, n$. ■

In the Triangle Inequality, if we set $n = 1$, we obtain the very useful inequality:

$$\sqrt{(a+b)^2} \leq \sqrt{a^2} + \sqrt{b^2},$$

which we usually write $|a+b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$.

The function $|\cdot| : \mathbb{R} \to \mathbb{R}$ is the **absolute value**, which can be used to represent the distance between a real number and the origin.

It is defined by

$$|x| = \begin{cases} x, & x \geq 0 \\ x, & x \leq 0 \end{cases}$$

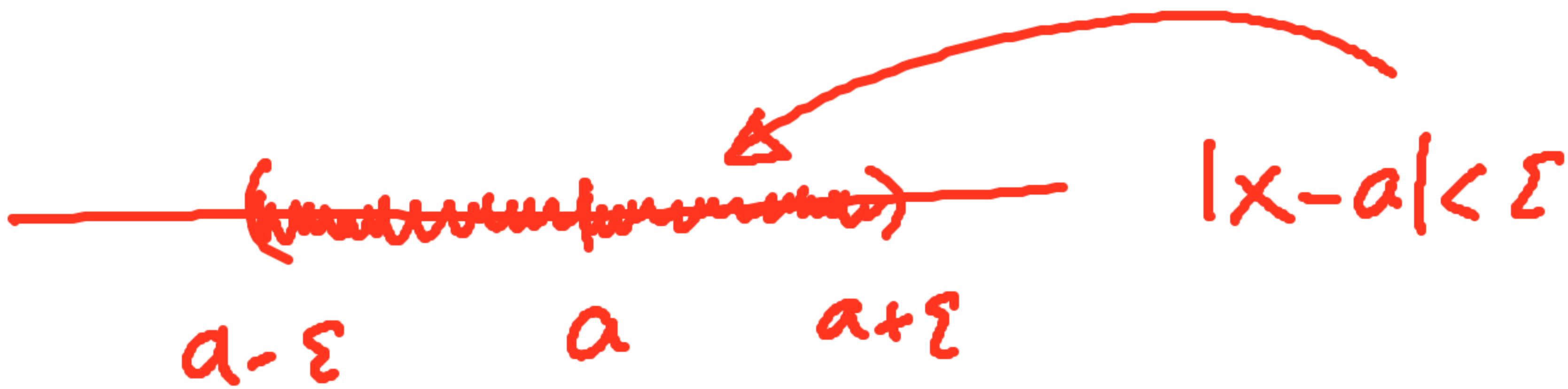
Equipped with this function, $\mathbb{R}$ is an example of a **normed space**. Normed space will be discussed at a later stage.

Theorem 6. (Properties of the Absolute Value)
If $x, y \in \mathbb{R}$, then

1. $|x| = \sqrt{x^2}$
2. $-|x| \leq x \leq |x|$
3. $|xy| = |x||y|$
4. $|x + y| \leq |x| + |y|$
5. $|x - y| \leq |x| + |y|$
6. $||x| - |y|| \leq |x - y|$

Remark: the following inequality will play a central role in the chapters to come:

$$|x-a|<\varepsilon \iff a-\varepsilon<x<a+\varepsilon.$$



We finish this section with an intriguing result about the distribution of rationals and irrationals among the reals.

2.1.4 – Density of $\mathbb{Q}$

Theorem 7. (Density of $\mathbb{Q}$)
Let $x, y \in \mathbb{R}$ be such that $x < y$. Then, $\exists r \in \mathbb{Q}$ such that $x < r < y$.

Proof. There are three distinct cases.

1. If $x < 0 < y$, then select $r = 0$.

2. If $0 \leq x < y$, then $y - x > 0$ and $\frac{1}{y-x} > 0$.

   By the Archimedean property, $\exists n \geq 1$ such that

$$n > \frac{1}{y-x} > 0.$$

By that same property, $\exists m \geq 1$ such that $m - 1 \leq nx < m$. Since $n(y - x) > 1$, then $ny - 1 > nx$ and $nx \geq m - 1$.

By transitivity of $<$, $ny - 1 > m - 1$, that is $ny > m$. But $m > nx$, so $ny > m > nx$ and $y > \frac{m}{n} > x$. Select $r = \frac{m}{n}$.

3. If $x < y \leq 0$, then $y - x > 0$ and $\frac{1}{y-x} > 0$. By the Archimedean property, $\exists n \geq 1$ such that
$$n > \frac{1}{y - x} > 0.$$
Note that $-nx > 0$. By that same property, $\exists m \geq 0$ such that $m < -nx \leq m + 1$ or $-m - 1 \leq nx < -m$.

Since $n(y - x) > 1$, then $ny - 1 > nx \geq -m - 1$, that is $ny > -m$. But $-m > nx$, so $ny > -m > nx$ and $y > -\frac{m}{n} > x$. Select $r = -\frac{m}{n}$. ■

Corollary. Let $x, y \in \mathbb{R}$ with $x < y$. Then, $\exists z \notin \mathbb{Q}$ such that $x < z < y$.

Proof. We will prove the case $xy > 0$, the other cases are left as an exercise.

According to the Density Theorem, $\exists r \neq 0 \in \mathbb{Q}$ such that

$$\frac{x}{\sqrt{2}} < r < \frac{y}{\sqrt{2}}.$$

Hence $x < r\sqrt{2} < y$. Set $z = r\sqrt{2}$. Then $z \notin \mathbb{Q}$ – indeed, if $z = r\sqrt{2} = \frac{p}{q} \in \mathbb{Q}$, then $\sqrt{2} = \frac{p}{qr} \in \mathbb{Q}$, a contradiction. ■

It is thus possible to find rationals and irrationals between any two real numbers $x < y$. In spite of this, $\mathbb{Q}$ is much "smaller" than $\mathbb{R} \setminus \mathbb{Q}$.

2.2 – Cardinality of Sets

In the set hierarchy $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$, the first three sets are of the same size, while the last one is "infinitely" larger.

For all $n \in \mathbb{N}^{\times}$, define the set $\mathbb{N}_n = \{1, 2, \ldots, n\}$.

A set S is **finite** if $S = \varnothing$ or if there exists a bijection $f : \mathbb{N}_n \to S$ for some $n \in \mathbb{N}^{\times}$. If S is not finite, it is **infinite**.

If S is infinite and there exists a bijection $f : \mathbb{N} \to S$, then S is **countable**. Otherwise, it is **uncountable**.

Note: in some references, finite sets are called **finitely countable** sets, and countable sets are called **infinitely countable** sets.

Consider two sets S_n and T_n, both with n distinct elements:

$$S_n = \{s_1, \ldots, s_n\}, \quad T_n = \{t_1, \ldots, t_n\}.$$

These two finite sets have the same size: there is a bijection $f : S_n \to T_n$, $f(s_i) = t_i$ for $1 \leq i \leq n$ (it is not the only such bijection).

In general, two sets S, T are said to have the same **cardinality**, denoted $|S| = |T|$, if there exists a bijection $f : S \to T$.

If S, T are finite, $|S| = |T|$ means that the two sets **have the same number of elements**: $|S| = |T| = |\mathbb{N}_n| = n$ for some $n \in \mathbb{N}$.

If S, T are infinite, the "number of elements" is not a well-defined, which can lead to counter-intuitive results.

Examples:

1. The set $2\mathbb{N} = \{2, 4, \ldots\}$ is countable because $f : \mathbb{N} \to 2\mathbb{N}$ defined by $f(n) = 2n$ is a bijection. We would then write $|\mathbb{N}| = |2\mathbb{N}| = \omega$.

2. The set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is countable since $f : \mathbb{Z} \to \mathbb{N}$ defined by
$$f(z) = \begin{cases} 2z, & z \geq 0 \\ -2z - 1, & z < 0 \end{cases}$$
is a bijection. Thus $|\mathbb{Z}| = |\mathbb{N}| = \omega$.

So two sets can have equal cardinality even when one is strictly contained in the other (this can only happen with infinite sets, however).

Theorem 8. *If S is an infinite subset of a countable set A, then S is countable.*

Proof. As A is countable, we can list all its elements:

$$A = \{a_1, a_2, \ldots, \}.$$

Let $n_1, n_2, \ldots$ be integers obtained by the following algorithm:

- Set $K_1 = \{n \in \mathbb{N} \mid a_n \in S\}$. According to the Well-Ordering Principle, $\exists n_1 \in K_1$ which is minimal. Then $a_{n_1} \in S$ and $a_m \notin S$ for all $m < n_1$.
- Set $K_2 = K_1 \setminus K_1$. According to the WOP, $\exists n_2 \in K_2$ which is minimal, with $n_1 < n_2$. Then $a_{n_2} \in S$ and $a_m \notin S$ for all $m < n_1$ with $m \neq n_1$.
- etc.

Repeating this process, we obtain the set

$$S' = \{a_{n_1}, a_{n_2}, \ldots\}.$$

But every element of S must be in S' (why?), so $S = S'$. The function $f : \mathbb{N} \to S$ defined by $k \mapsto a_{n_k}$ is thus a bijection, and so S is countable. ■

General Remark: if you find it difficult to follow a proof, it is never a bad idea to try it with specific examples satisfying the hypotheses.

⚠ If you have to give a proof, an example only works if you are trying to show that some statement is **false**. A direct proof **never** uses examples.

The contrapositive of Theorem 8 gives a useful way to show that a set is uncountable: if $S \subseteq A$ is uncountable, then A is uncountable.

2.2.1 – Cardinality of $\mathbb{Q}$

Another way to think of countable sets is that they could be enumerated, at least conceptually, in an infinite list.

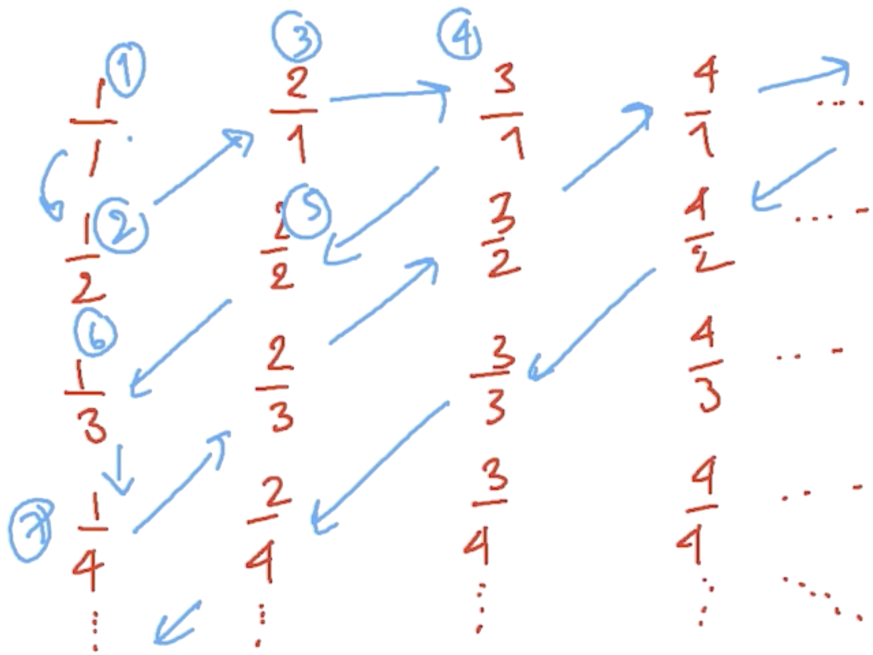
Theorem 9. *The set $\mathbb{Q}$ is countable.*

Proof. Write $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$, with the obvious notation. As there is a bijection $f : \mathbb{Q}^+ \to \mathbb{Q}^-$, $r \mapsto -r$, then $|\mathbb{Q}^+| = |\mathbb{Q}^-|$.

It is then sufficient to show that $|\mathbb{Q}^+| = \omega$. Indeed, if we can enumerate the elements of $\mathbb{Q}^+$, then then we can enumerate the elements of $\mathbb{Q}$ by starting with 0, and alternating from $\mathbb{Q}^-$ to $\mathbb{Q}^+$.

Every positive rational takes the form $\frac{m}{n}$, with $m, n \in \mathbb{N}^\times$.

Arrange all such fractions in an infinite array:



There is a bijection between $\mathbb{N}^\times$ and the set $F = \{\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{3}{1}, \frac{2}{2}, \ldots\}$, so $|F| = \omega$. But $\mathbb{Q}^+ \subseteq F$, so $\mathbb{Q}^+$ is countable since it is infinite ($\mathbb{N}^\times \subseteq \mathbb{Q}^+$). According to Theorem 8, $|\mathbb{Q}^+| = \omega$. This completes the proof. ■

2.2.2 – Cardinality of $\mathbb{R}$

We now show that a set which would seem to be much smaller than $\mathbb{Q}$ at a first glance is in fact much larger than $\mathbb{Q}$ from a cardinality perspective, using the celebrated **Cantor diagonal argument**.

Theorem 10. *The set $I = [0,1]$ is uncountable.*

Proof. Every number $x \in I$ has a (not necessarily unique) decimal representation of the form

$$x = 0.a_1a_2a_3\cdots , \quad a_i \in \{0,\ldots,9\}.$$

By convention, we write $1 = .0.99999\overline{9}$ and $0 = 0.00000\overline{0}$. When numbers have two decimal representations, such as $0.4000\overline{0} = 0.3999\overline{9}$, we only consider the representation with a tail of repeating 9s.

Assume that I is countable. Then it is possible to enumerate its elements:

$$I = \{x_1, x_2, \ldots\}.$$

Each of the $x_i \in I$ has a unique decimal representation (with the convention given earlier):

$$\begin{aligned}
x_1 &= 0.a_{1,1}a_{1,2}a_{1,3}\cdots a_{1,n}\cdots \\
x_2 &= 0.a_{2,1}a_{2,2}a_{2,3}\cdots a_{2,n}\cdots \\
&\vdots \\
x_n &= 0.a_{n,1}a_{n,2}a_{n,3}\cdots a_{n,n}\cdots \\
&\vdots
\end{aligned}$$

where $a_{i,j} \in \{0, \ldots, 9\}$ for all $ii, j \in \mathbb{N}^\times$.

Define the real number $y = 0.y_1y_2y_3\cdots$, where

$$y_i = \begin{cases} 2 & \text{if } a_{i,i} \geq 5 \\ 6 & \text{if } a_{i,i} \leq 4 \end{cases} \qquad \text{for } i \in \mathbb{N}^\times.$$

As $0 \leq y \leq 1$, we have $y \in I$. But for all $i \in \mathbb{N}^\times$, we also have $y \neq x_i$ in the list because $y_i \neq a_{i,i}$. Thus $y \notin I$, a contradiction.

Consequently, the assumption that I is countable is not valid. ■

Since $[0,1] \subseteq \mathbb{R}$, then $\mathbb{R}$ is also uncountable. What about $\mathbb{R} \setminus \mathbb{Q}$?

In general, is it possible for the union of two countable sets to be uncountable? Is the intersection of two uncountable sets uncountable?

2.3 – Nested Intervals Theorem

We end this chapter with an important result concerning nested intervals. In style and rigour, its proof is representative of analytical reasoning.

Theorem 11. (Nested Intervals)
For every integer $n \geq 1$, let $[a_n, b_n] = I_n$ be such that

$$I_1 \supseteq I_2 \supseteq \cdots I_n \supseteq I_{n+1} \supseteq \cdots$$

Then there exists $\psi, \eta \in \mathbb{R}$ such that $\psi \leq \eta$ and $\bigcap_{n\geq 1} I_n = [\psi, \eta]$.

Furthermore, if $\inf\{b_n - a_n \mid n \in \mathbb{N}\} = 0$, then $\psi = \eta$.

Proof. Since $I_n \subseteq I_1$ for all $n \geq 1$, the set $S = \{a_1, \ldots, a_n\}$ is bounded above by b_1. But $S \neq \varnothing$, so $\psi = \sup S$ exists by completeness of $\mathbb{R}$, and thus

$$a_n \leq \psi, \quad \text{for all } n \geq 1.$$

Fix $n \geq 1$ and let $k \geq 1$ be an integer:

- if $k \geq n$, then $I_n \supseteq I_k$ and $a_k \leq b_k \leq b_n$;
- if $k < n$, then $I_n \subseteq I_k$ and $a_k \leq a_n \leq b_n$.

In both cases, $a_k \leq b_n$ for all $k \geq 1$. Thus b_n is an upper bound of S for all $n \geq 1$. As $\psi = \sup S$, $\psi \leq b_n$ for all $n \geq 1$.

Combining these results, we have $a_n \leq \psi \leq b_n$, for all $n \geq 1$.

Since $I_n \subseteq I_1$ for all $n \geq 1$, the set $T = \{b_1, \ldots, b_n\}$ is bounded below by a_1. But $T \neq \varnothing$, so $\eta = \inf T$ exists by completeness of $\mathbb{R}$, and thus

$$b_n \geq \eta, \quad \text{for all } n \geq 1.$$

Fix $n \geq 1$ and let $k \geq 1$ be an integer:

- if $k \geq n$, then $I_n \supseteq I_k$ and $a_n \leq a_k \leq b_k$;
- if $k < n$, then $I_n \subseteq I_k$ and $a_n \leq b_n \leq b_k$.

In both cases, $a_n \leq b_k$ for all $k \geq 1$. Thus a_n is an lower bound of T for all $n \geq 1$. As $\eta = \inf T$, $\eta \geq a_n$ for all $n \geq 1$.

Combining these results, we have $a_n \leq \eta \leq b_n$, for all $n \geq 1$.

(In general, we avoid repeating nearly identical proof segments, using generic statements like "Similarly, we can show that $a_n \leq \inf\{b_i \mid i \geq 1\} \leq b_n$, for all $n \geq 1$" while leaving the details to be worked out by the reader).

But ψ is also a lower bound of T since $\psi \leq b_n$ for all $n \geq 1$. Since η is the largest such lower bound, $\psi \leq \eta$, which is to say:

$$a_n \leq \psi \leq \eta \leq b_n, \quad \text{for all } n \geq 1,$$

and so $[\psi, \eta] \subseteq I_n$ for all $n \geq 1$. Consequently,

$$[\psi, \eta] \subseteq \bigcap_{n \geq 1} I_n.$$

Now, suppose that $\gamma \in I_n$ for all $n \geq 1$. Then $a_n \leq \gamma \leq b_n$ for all $n \geq 1$, and so γ is an upper bound of S and a lower bound of T.

But ψ is the smallest upper bound of S, so $\psi = \sup S \leq \gamma$, and η is the largest lower bound of T, so $\gamma \leq \inf T \leq \eta$, and so $\gamma \in [\psi, \eta]$. Thus

$$\bigcap_{n \geq 1} I_n \subseteq [\psi, \eta] \implies \bigcap_{n \geq 1} I_n = [\psi, \eta].$$

Finally, suppose that $\inf\{b_n - a_n \mid n \geq 1\} = 0$. Let $\varepsilon > 0$. By definition, $\exists k \geq 1$ such that $0 \leq b_k - a_k < \varepsilon$, otherwise $\varepsilon > 0$ would be a lower bound of the set, which would contradict the assumption that 0 is the largest such upper bound.

We have seen that $b_k \geq \eta$ and that $a_k \leq \psi$, so

$$\varepsilon > b_k - a_k \geq \eta - \psi \geq 0.$$

Thus, for all $\varepsilon > 0$, we have $0 \leq \eta - \psi < \varepsilon$, which is to say $\eta - \psi = 0$. ■

Why can we conclude that $\eta - \psi = 0$ if $0 \leq \eta - \psi < \varepsilon$ for all $\varepsilon > 0$?

In general, if $a \leq x < a + \varepsilon$ for all $\varepsilon > 0$, then $x = a$. If $x \neq a$, $\exists \delta > 0$ such that $x = a + \delta$. Thus, if $\varepsilon = \delta$, which is possible since ε can take on any positive value, we would have $\delta = x - a < \varepsilon = \delta$, a contradiction.

Example: If $I_n = [1 - \frac{1}{n}, 1 + \frac{1}{n}]$ for $n \geq 1$, then the conditions of the Nested Intervals Theorem are satisfied, and so $\bigcap_{n \geq 1} I_n = [\psi, \eta]$. As $\inf\{b_n - a_n \mid n \geq 1\} = \inf\{\frac{2}{n} \mid n \geq 1\} = 0$, we have

$$\psi = \sup\{1 - \tfrac{1}{n}\} = 1 = \inf\{1 + \tfrac{1}{n}\} = \eta, \implies [\psi, \eta] = \{1\}.$$

⚠ We can only use a theorem if the hypotheses are satisfied (even though the conclusion may hold nonetheless). The intervals $I_n = (1 - \frac{1}{n}, 1 + \frac{1}{n})$, $n \geq 1$ are such that their intersection is $\{1\}$, but not because of the NVT.

2.4 – Exercises

1. Let $a, b \in \mathbb{R}$ and suppose that $a \leq b + \varepsilon$ for all $\varepsilon > 0$. Show that $a \leq b$.
2. Let $c > 0$ be a real number.
   (a) If $c > 1$, show that $c^n \geq c$ for all $n \in \mathbb{N}$ and that $c^n > 1$ if $n > 1$.
   (b) If $0 < c < 1$, show that $c^n \leq c$ for all $n \in \mathbb{N}$ and that $c^n < 1$ if $n > 1$.
3. Let $c > 0$ be a real number.
   (a) If $c > 1$ and $m, n \in \mathbb{N}$, show that $c^m > c^n$ if and only if $m > n$.
   (b) If $0 < c < 1$ and $m, n \in \mathbb{N}$, show that $c^m > c^n$ if and only if $m < n$.
4. Let $S_2 = \{x \in \mathbb{R} \mid x > 0\}$. Does S_2 have lower bounds? Does S_2 have upper bounds? Does $\inf S_2$ exist? Does $\sup S_2$ exist? Prove your statements.
5. Let $S_4 = \left\{1 - \frac{(-1)^n}{n} \mid n \in \mathbb{N}\right\}$. Find $\inf S_4$ and $\sup S_4$.
6. Let $S \subseteq \mathbb{R}$ be non-empty. Show that if $u = \sup S$ exists, then for every number $n \in \mathbb{N}$ the number $u - \frac{1}{n}$ is not an upper bound of S, but the number $u + \frac{1}{n}$ is.
7. If $S = \left\{\frac{1}{n} - \frac{1}{m} \mid m, n \in \mathbb{N}\right\}$, find $\inf S$ and $\sup S$.

8. Let X be a non-empty set and let $f : X \to \mathbb{R}$ have bounded range in $\mathbb{R}$. If $a \in \mathbb{R}$, show that

$$\sup\{a + f(x) : x \in X\} = a + \sup\{f(x) : x \in X\}$$
$$\inf\{a + f(x) : x \in X\} = a + \inf\{f(x) : x \in X\}.$$

9. Let A and B be bounded non-empty subsets of $\mathbb{R}$, and let

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

Prove that $\sup(A + B) = \sup A + \sup B$ and $\inf(A + B) = \inf A + \inf B$.

10. Let X be a non-empty set and let $f, g : X \to \mathbb{R}$ have bounded range in $\mathbb{R}$. Show that

$$\sup\{f(x) + g(x) \mid x \in X\} \leq \sup\{f(x) \mid x \in X\} + \sup\{g(x) \mid x \in X\}$$
$$\inf\{f(x) \mid x \in X\} + \inf\{g(x) \mid x \in X\} \leq \inf\{f(x) + g(x) \mid x \in X\}.$$

11. Let X and Y be non-empty sets and let $h : X \times Y \to \mathbb{R}$ have bounded range in $\mathbb{R}$. Let $F : X \to \mathbb{R}$ and $G : Y \to \mathbb{R}$ be defined by

$$F(x) = \sup\{h(x,y) \mid y \in Y\} \quad \text{and} \quad G(y) = \sup\{h(x,y) \mid x \in X\}.$$

Show that

$$\sup\{h(x,y) \mid (x,y) \in X \times Y\} = \sup\{F(x) \mid x \in X\} = \sup\{G(y) \mid y \in Y\}.$$

12. Show there exists a positive real number u such that $u^2 = 3$.
13. Show there exists a positive real number u such that $u^3 = 2$.
14. Let $S \subseteq \mathbb{R}$ and suppose that $s^* = \sup S$ belongs to S. If $u \notin S$, show that $\sup(S \cup \{u\}) = \sup\{s^*, u\}$.
15. Show that a non-empty finite set $S \subseteq \mathbb{R}$ contains its supremum.
16. If $S \subseteq \mathbb{R}$ is a non-empty bounded set and $I_S = [\inf S, \sup S]$, show that $S \subseteq I_S$. Moreover, if J is any closed bounded interval of $\mathbb{R}$ such that $S \subseteq J$, show that $I_S \subseteq J$.

17. Prove that if $K_n = (n, \infty)$ for $n \in \mathbb{N}$, then $\bigcap_{n \in \mathbb{N}} K_n = \varnothing$.
18. If S is finite and $s^* \notin S$, show $S \cup \{s^*\}$ is finite.
19. Show directly that there exists a bijection between $\mathbb{Z}$ and $\mathbb{Q}$.
20. Using only the field axioms of $\mathbb{R}$, show that the multiplicative identity of $\mathbb{R}$ is unique.
21. Using only the field axioms of $\mathbb{R}$, show that $(2x-1)(2x+1) = 4x^2 - 1$.
22. Using only the order axioms, usual arithmetic manipulations, and inequalities between concrete numbers, prove that if $x \in \mathbb{R}$ satisfies $x < \varepsilon$ for all $\varepsilon > 0$, then $x \leq 0$.
23. Show that there exists some $x \in \mathbb{R}$ satisfying $x^2 + x = 5$.
24. Consider a set S with $0 \leq \sup S = A < \infty$ and $A \notin S$. Show that for all $\varepsilon > 0$, $S \cap [A - \varepsilon, A] \neq \varnothing$. Using this fact, conclude that $S \cap [A - \varepsilon, A]$ is infinite.
25. Somebody walks up to you with a proof by induction of the statement "*For any integer $N \in \mathbb{N}$, all collections of N sheep are the same colour*," as follows:
    - **Notation:** Let $x_1, x_2, \ldots,$ be the colours of all sheep in the world, in some order.
    - **Base Case:** Obviously the first sheep is a single colour, x_1.

- **Induction Step:** Assume that the statement is true up to some integer n.

  By the induction hypothesis, the collection of the first n sheep $\{x_1, \ldots, x_n\}$ are one colour (label this "colour 1'), and the collection of the last n sheep $\{x_2, \ldots, x_{n+1}\}$ are also one colour (label this "colour 2" - note that we haven't yet shown it is the same colour as the first collection).

  Since $\{x_2, \ldots, x_n\}$ are in both sets, we must have that "colour 1" and "colour 2" are the same, and so $\{x_1, \ldots, x_{n+1}\}$ are all one colour.

Explain why this "proof" fails by identifying/explaining a (significant) false statement.

Solutions

1. **Proof.** Suppose that $a > b$. Let $\varepsilon_0 = \frac{a-b}{2} > 0$. Then

$$\begin{aligned} a &> b \\ \therefore a + a &> a + b \quad \text{(see Theorem, in class)} \\ \therefore a = \frac{a+a}{2} &> \frac{a+b}{2} = b + \varepsilon_0 \quad \text{(same thing)} \end{aligned}$$

   Hence, $a > b + \varepsilon_0$, which contradicts the hypothesis that $a \leq b + \varepsilon$ for all $\varepsilon > 0$. Consequently, the assumption $a > b$ is false, that is, $a \not> b$ or $a \leq b$ by trichotomy of the order on $\mathbb{R}$. ■

2. **Proof.** The statement is clearly not true if $n = 0$: as a result, we must interpret $\mathbb{N}$ to stand for the set $\mathbb{N} = \{1, 2, 3, \ldots\}$, without the 0. Generally, we use whatever "version" of $\mathbb{N}$ is appropriate.

   (a) If $c > 1$, $\exists x \in \mathbb{R}$ such that $x > 0$ and $c = 1 + x$. Let $n \in \mathbb{N}$. First note that $n - 1 \geq 0$ and so $(n-1)x > 0$.

   Then, by Bernoulli's Inequality,

   $$c^n = (1+x)^n \geq 1 + nx = 1 + x + (n-1)x \geq 1 + x = c.$$

   Furthermore, $n - 1 > 0$ and $(n-1)x > 0$ if $n > 1$.

   In that case, the last inequality above is strict and so $c^n > c > 1$, which implies $c^n > 1$ by transitivity of $>$.

(b) If $0 < c < 1$, there exists $b > 1$ such that $c = \frac{1}{b}$. Indeed, $\frac{1}{c}$ is such that $c \cdot \frac{1}{c} = 1$. As $c > 0$, then $\frac{1}{c} > 0$ since the product $c \cdot \frac{1}{c} = 1$ is positive.

But $c < 1$, so that $1 = c \cdot \frac{1}{c} < \frac{1}{c}$.

In particular, if we let $b = \frac{1}{c}$, then $b > 1$ and so we can apply part (a) of this question to get $b^n \geq b$ for all $n \in \mathbb{N}$ and $b^n > 1$ if $n > 1$.

Let $n \in \mathbb{N}$. Then

$$\frac{1}{c^n} = b^n \geq b = \frac{1}{c}$$

so that $c \geq c^n$ and

$$\frac{1}{c^n} = b^n > 1$$

so that $1 > c^n$ if $n > 1$. ■

3. **Proof.**

(a) It is sufficient to show that if $m \geq n$, then $c^m \geq c^n$.

If $m = n$, the result is clear. So we consider $m > n$. In this case, $\exists k \geq 1$ such that $m = n + k$. An easy induction exercise shows that $c^{n+k} = c^n c^k$ for for all integers n and k (from this point on, we will assume and apply freely all the usual techniques of algebra).

In particular, using the previous problem,

$$c^m = c^{n+k} = c^n c^k \geq c^n \cdot c > c^n \cdot 1 = c^n$$

and so $c^m > c^n$.

(b) This can be shown from part (a) using the technique from the previous question. ■

4. **Proof.**

Does S_2 have lower bounds? Yes.
By definition, any negative real number is a lower bound (so is 0).

Does S_2 have upper bounds? No.
Assume that it does. By the completeness of $\mathbb{R}$, $\alpha = \sup \mathbb{R}$ exists. In particular, $\alpha \geq n$ for all $n \in \mathbb{N}$, which contradicts the Archimedean Property of $\mathbb{R}$. Hence S_2 has no upper bound.

Does $\inf S_2$ exist? Yes.
Consider the set $-S_2 = \{x \in \mathbb{R} \mid -x \in S_2\} = \{x \in \mathbb{R} \mid x < 0\}$. By construction, 0 is an upper bound of $-S_2$. Note furthermore that neither S_2 nor $-S_2$ are empty.

By completeness of $\mathbb{R}$, $\sup(-S_2)$ exists. Right?

One definition of completeness is that any non-empty bounded subset of $\mathbb{R}$ has a supremum. But $-S_2$ is only bounded above, not below. How can we conclude that $\sup(-S_2)$ exists?

That definition is one particular version of the Completeness Property of $\mathbb{R}$. An **equivalent** way of stating it is: *The ordered set F is* ***complete*** *if for any $\varnothing \neq S \subset F$, S has a supremum in F whenever S is bounded above and an infimum in F whenever S is bounded below.*

But $\sup(-S_2) = -\inf S_2$. Indeed, let $u = \sup(-S_2)$. Then $u \geq -x$ for all $-x \in -S_2$ and if v is another upper bound of $-S_2$ then $u \leq v$.

Note that if v is an upper bound of $-S_2$, then $v \geq -x$ for all $-x \in -S_2$, **i.e.** $-v \leq x$ for all $x \in S_2$: as a result, $-v$ is a lower bound of S_2.

Similarly, if $-v$ is a lower bound of S_2, v is automatically an upper bound of $-S_2$. Then any lower bound of S_2 is of the form $-v$, where v is an upper bound of $-S_2$.

Then, $-u \leq x$ for all $x \in S_2$ and $-v \leq -u$ whenever $-v$ is a lower bound of S_2. Hence $-u = \inf S_2$ and so $u = -\inf S_2$.

As $\sup(-S_2) = -\inf S_2$ exists, so does $\inf S_2$.

Does $\sup S_2$ exist? No.
See second item. ■

5. **Proof.** The first few elements of S_4 are

$$2, \frac{1}{2}, \frac{4}{3}, \frac{3}{4}, \frac{6}{5}, \frac{5}{6}, \ldots .$$

This gives us the idea that S_4 is bounded above by 2 and below by $\frac{1}{2}$. To show that this is indeed the case, note that $(-1)^n$ only takes on the values -1 and 1, whatever the integer n.

Technically, this also has to be shown. One proceeds by induction.

The **base case** is clear: when $n = 1$, $(-1)^1 = -1 \in \{1, -1\}$.

Now, on to the **induction step**: suppose $(-1)^k \in \{1, -1\}$.

Then

$$(-1)^{k+1} = (-1)^k(-1) = \begin{cases} 1(-1) = -1 \\ (-1)(-1) = 1 \end{cases}.$$

Hence $(-1)^{k+1} \in \{1, -1\}$.

By induction, $(-1)^n \in \{-1, 1\}$ for all $n \in \mathbb{N}$.

Thus $-1 \leq (-1)^n \leq 1$ for all $n \geq 1$. (In practice, we need only show it once and refer to the result if we need it in the future.)

For any $n \geq 2$, we then have $-n \leq -1 \leq (-1)^n$ and $\frac{n}{2} \geq 1 \geq (-1)^n$, that is

$$-n \leq (-1)^n \leq \frac{n}{2}.$$

A quick check shows the inequalities also hold for $n = 1$.

Then, for $n \geq 1$,

$$
\begin{aligned}
-n \leq (-1)^n &\leq \frac{n}{2} \\
\therefore -1 \leq \frac{(-1)^n}{n} &\leq \frac{1}{2} \\
\therefore 1 \geq -\frac{(-1)^n}{n} &\geq -\frac{1}{2} \\
\therefore 2 \geq 1 - \frac{(-1)^n}{n} &\geq \frac{1}{2}.
\end{aligned}
$$

Hence $2 \geq s \geq \frac{1}{2}$ for all $s \in S_4$, *i.e.* 2 is an upper bound and $\frac{1}{2}$ is a lower bound of S_4.

By completeness of $\mathbb{R}$, S_4 possesses a supremum and an infimum in $\mathbb{R}$. If $u = \sup S_4 < 2$, there is a contradiction as $u \not\geq s$ for all $s \in S_4$ (it "misses" the element 2 in S_4).

Thus, $\sup S_4 \geq 2$. But 2 is already an upper bound so $\sup S_4 \leq 2$. Consequently $\sup S_4 = 2$. Similarly, $\inf S_4 = \frac{1}{2}$. ■

6. **Proof.** Let $n \geq 1$. Then $\frac{1}{n} > 0$ and $u < u + \frac{1}{n}$. Since $s \leq u$ for all $s \in S$, $s < u + \frac{1}{n}$ for all $s \in S$ by transitivity of $<$. Consequently, $u + \frac{1}{n}$ is an upper bound of S.

   Furthermore, $u - \frac{1}{n} < u$. Since u is the least upper bound, $u - \frac{1}{n}$ cannot be an upper bound (as it would then be lesser upper bound than u, a contradiction). This completes the proof. Or does it?

   We haven't used the hypothesis $S \neq \varnothing$. Where does it fit?

   The definition of an upper bound implies that every real number is an upper bound of the empty set. Indeed, if $v \in \mathbb{R}$, then $v \geq s$ for all $s \in \varnothing$ automatically as there is **no** $s \in \varnothing$.

   The proof rests on the fact that $u = \sup S$. But $\sup \varnothing$ does not exist as we just discussed. OK. Now it's the end for real. ■

7. **Proof.** The set $S=\left\{\frac{1}{n}-\frac{1}{m}\mid n,m\in\mathbb{N}\right\}$ is bounded above by 1 and below by -1 since

$$\frac{1}{n}\leq 1\leq 1+\frac{1}{m}\quad\text{and}\quad\frac{1}{m}\leq 1\leq 1+\frac{1}{n}\implies -1\leq\frac{1}{n}-\frac{1}{m}\leq 1,\quad\forall m,n\in\mathbb{N}.$$

Note that S is not empty as $0=\frac{1}{2}-\frac{1}{2}$ is in S, say.

By completeness of $\mathbb{R}$, S thus has a supremum and an infimum.

By definition, $s^*=\sup S\leq 1$. Suppose that $s^*<1$. Then $\exists\varepsilon>0$ such that $s^*=1-\varepsilon$. Furthermore,

$$\frac{1}{n}-\frac{1}{m}\leq 1-\varepsilon,\quad\forall m,n\in\mathbb{N}.$$

In particular, if $n = 1$, then

$$1 - \frac{1}{m} \leq 1 - \varepsilon, \quad \forall m \in \mathbb{N}.$$

Equivalently, $\varepsilon \leq \frac{1}{m}$ for all integers m so that $\frac{1}{\varepsilon}$ is an upper bound for $\mathbb{N}$.

This contradicts the Archimedean Property of $\mathbb{R}$. Hence $s^* \not< 1$ and so $s^* = 1$.

To prove that $\inf S = -1$, proceed along the same lines. $\blacksquare$

8. **Proof.** Let $f(X) = \{f(x) \mid x \in X\}$. By hypothesis, $f(X)$ is bounded and not empty and so has a supremum in $\mathbb{R}$, say u^*.

   We need to show $\sup\{a + f(x); x \in X\} = a + u^*$.

   To do so, first note that $a+u^*$ is an upper bound of $\sup\{a+f(x) \mid x \in X\}$ since $u^* \geq f(x)$ for all $x \in X$; as a result $a + u^* \geq a + f(x)$ for all $x \in X$.

   (By completeness of $\mathbb{R}$, this means that $\sup\{a + f(x) \mid x \in X\}$ does indeed have a supremum.)

   Next, we need to show that $a + u^*$ is the smallest upper bound of $\{a + f(x) \mid x \in X\}$.

   Suppose v is another upper bound of $\{a + f(x) \mid x \in X\}$. Then $v \geq a + f(x)$ for all $x \in X$; in particular, $v - a$ is an upper bound of $f(X)$.

By hypothesis, $v - a \geq u^*$, hence $v \geq a + u^*$. Consequently, $a + u^*$ is the least upper bound of $\{a + f(x) \mid x \in X\}$, i.e.

$$\sup\{a + f(x) \mid x \in X\} = a + u^*.$$

The proof for the other equality proceeds in a similar manner. ■

9. **Proof.** A and B are bounded and non-empty.

By completeness, they have infimums (in $\mathbb{R}$), say a_* and b_*, respectively. Then $a_* \leq a$ and $b_* \leq b$ for all $a \in A$, $b \in B$.

The real number $a_* + b_*$ is a lower bound of $A + B$ since $a_* + b_* \leq a + b$ for all $a \in A$, $b \in B$.

By completeness of $\mathbb{R}$, $A + B$ has an infimum as it is also not empty. We show that this infimum is indeed $a_* + b_*$.

Let w be a lower bound of $A + B$. Then, $w \leq a + b$ for all $a \in A$ and $b \in B$, or $w - b \leq a$ for all $a \in A$ and $b \in B$.

Thus, $w - b$ is a lower bound of A for all $b \in B$, *i.e.* $w - b \leq a_*$ for all $b \in B \implies w - a_* \leq b$ for all $b \in B$, so $w - a_*$ is a lower bound of B.

hence $w - a_* \leq b_*$. As a result, $w \leq a_* + b_*$, which concludes the proof. The other equality is shown in the same manner. ■

10. **Proof.** Let $f(X) = \{f(x) \mid x \in X\}$ and $g(X) = \{g(x) \mid x \in X\}$. By hypothesis, $f(X)$ and $g(X)$ are both bounded and not empty, so they each have a supremum in $\mathbb{R}$, say u^* and v^* respectively.

    Since $f(x) \leq u^*$ and $g(x) \leq v^*$ for all $x \in X$, then $f(x)+g(x) \leq u^*+v^*$ for all $x \in X$.

    Hence $\{f(x) + g(x) \mid x \in X\}$ has a supremum in $\mathbb{R}$, as it is a bounded non-empty subset of $\mathbb{R}$. Let w^* be that supremum, i.e. the smallest upper bound of $\{f(x) + g(x) \mid x \in X\}$.

    Since $u^* + v^*$ is also an upper bound of that set, it's automatically larger than w^*. Note that we can not in general say more: it is **not** true, in general, that $w^* = u^* + v^*$.

Indeed, take $X = [1, 2]$ and let f and g be defined by

$$f(x) = \frac{1}{x} \quad \text{and} \quad g(x) = -\frac{1}{x}, \quad \forall x \in X.$$

Then $f(X) = \{\frac{1}{x} \mid x \in X\}$, $g(X) = \{-\frac{1}{x} \mid x \in X\}$ and $u^* = 1$, $v^* = -\frac{1}{2}$ and $w^* = 0$ (you should show these results!), and $w^* \leq u^* + v^*$ but $w^* \neq u^* + v^*$.

(Compare this result with the one from the previous question; what is the difference?)

The other inequality is tackled in a similar manner. ∎

11. **Proof.** Let $h(X,Y) = \{h(x,y) \mid (x,y) \in X \times Y\}$. By definition, $h(X,Y)$ is bounded and not empty, so it has a supremum in $\mathbb{R}$, and F and G are well-defined.

    Let $\alpha = \sup h(X,Y)$. Then $\alpha \geq h(x,y)$ for all $x \in X$ and $y \in Y$. In particular, if $x \in X$ is fixed, $\alpha \geq h(x,y)$ for all $y \in Y$. But $F(x)$ is the smallest upper bound of $\{h(x,y) \mid y \in Y\}$, so $\alpha \geq F(x)$.

    But x was arbitrary, so $\alpha \geq F(x)$ for all $x \in X$. Hence α is an upper bound of $\{F(x) \mid x \in X\}$; by completeness, $\{F(x) \mid x \in X\}$ has a supremum in $\mathbb{R}$, say β. Then $\alpha \geq \beta$, by definition of the supremum.

    Again, fix $x \in X$. Then $\beta \geq F(x) \geq h(x,y)$ for all $y \in Y$. Hence, for any $x \in X$, $\beta \geq h(x,y)$ for all $y \in Y$. As a result, β is an upper bound of $h(X,Y)$. Then $\beta \geq \alpha$, by definition of the supremum.

    Combining these two results yields $\alpha = \beta$ (now do the other). $\blacksquare$

12. **Proof.** We first show that u is not rational (even though that wasn't part of the question, it will be informative).

Suppose the equation $r^2 = 3$ has a positive root r in $\mathbb{Q}$. Let $r = p/q$ with $\gcd(p, q) = 1$ be that solution. Then $p^2/q^2 = 3$, or $p^2 = 3q^2$. Hence p^2 is a multiple of 3, and so p is also a multiple of 3.

(Indeed, if p is not a multiple of 3, then neither is p^2. Let $p = 3k + 1$ or $p = 3k + 2$. Then $p^2 = 3(3k^2 + 2k) + 1$ or $p^2 = 3(3k^2 + 4k + 1) + 1$, neither of which is a multiple of 3.)

Set $p = 3m$. Then $(3m)^2 = 3q^2$, which is the same as $3m^2 = q^2$. Then q^2 is a multiple of 3, and so q is also a multiple of 3.

Consequently, p and q are both divisible by 3, which contradicts the hypothesis $\gcd(p, q) = 1$. The equation $r^2 = 3$ cannot then have a solution in $\mathbb{Q}$.

But we haven't shown yet that the equation has a solution in $\mathbb{R}$.

Consider the set $S = \{s \in \mathbb{R}^+ : s^2 < 3\}$, where $\mathbb{R}^+$ denotes the set of positive real numbers.

This set in not empty as $1 \in S$. Furthermore, S is bounded above by 3. (Indeed, if $t \geq 3$, then $t^2 \geq 9 > 3$, whence $t \notin S$.)

By completeness of $\mathbb{R}$, $x = \sup S \geq 1$ exists. It will be enough to show that neither $x^2 < 3$ and $x^2 > 3$ can hold. The only remaining possibility will be that $x = \sqrt{3}$.

- If $x^2 < 3$, then $\frac{2x+1}{3-x^2} > 0$. By the Archimedean property, $\exists n > 0$ such that $\frac{2x+1}{3-x^2} < n$. By re-arranging the terms, we get

$$0 < \frac{1}{n}(2x+1) < 3 - x^2.$$

Then

$$\left(x+\frac{1}{n}\right)^2 = x^2+\frac{2x}{n}+\frac{1}{n^2} \le x^2+\frac{2x}{n}+\frac{1}{n}$$
$$= x^2+\frac{1}{n}(2x+1) < x^2+3-x^2 = 3.$$

Since $(x+\frac{1}{n})^2 < 3$, $x+\frac{1}{n} \in S$. But $x < x+\frac{1}{n}$; x is then not an upper bound of S, which contradicts the fact that $x = \sup S$. Thus $x^2 \not< 3$.

- If $x^2 > 3$, then $\frac{2x}{x^2-3} > 0$. By the Archimedean property, $\exists n > 0$ such that $\frac{2x}{x^2-3} < n$. By re-arranging the terms, we get

$$0 > -\frac{2x}{n} > 3 - x^2.$$

Then

$$\left(x - \frac{1}{n}\right)^2 = x^2 - \frac{2x}{n} + \frac{1}{n^2} > x^2 - \frac{2x}{n} > x^2 + 3 - x^2 = 3.$$

Since $(x - \frac{1}{n})^2 > 3$, $x - \frac{1}{n}$ is an upper bound of S. But $x > x - \frac{1}{n}$; x can not then be the supremum of S, which is a contradiction. Thus $x^2 \not> 3$.

That leaves only one alternative (since we know that $x \in \mathbb{R}$): $x^2 = 3$, whence $x = u = \sqrt{3} > 0$. ■

13. **Proof.** Consider the set $S = \{s \in \mathbb{R}^+ : s^3 < 2\}$, where $\mathbb{R}^+$ denotes the set of positive real numbers.

This set in not empty as $1 \in S$. Furthermore, S is bounded above by 2. (Indeed, if $t \geq 2$, then $t^3 \geq 8 > 2$, whence $t \notin S$.)

By completeness of $\mathbb{R}$, $x = \sup S \geq 1$ exists. It will be enough to show that neither $x^3 < 2$ and $x^3 > 2$ can hold. The only remaining possibility will be that $x = \sqrt[3]{2}$.

- If $x^3 < 2$, then $\frac{3x^2+3x+1}{2-x^3} > 0$. By the Archimedean property, $\exists n > 0$ such that $\frac{3x^2+3x+1}{2-x^3} < n$. By re-arranging the terms, we get

$$0 < \frac{1}{n}(3x^2 + 3x + 1) < 2 - x^3.$$

Then

$$\left(x+\frac{1}{n}\right)^3 = x^3+\frac{3x^2}{n}+\frac{3x}{n^2}+\frac{1}{n^3} \leq x^3+\frac{3x^2}{n}+\frac{3x}{n}+\frac{1}{n}$$
$$= x^3+\frac{1}{n}(3x^2+3x+1) < x^3+2-x^3 = 2.$$

Since $(x+\frac{1}{n})^3 < 2$, $x+\frac{1}{n} \in S$. But $x < x+\frac{1}{n}$; x is then not an upper bound of S, which contradicts the fact that $x = \sup S$. Thus $x^3 \not< 2$.

- If $x^3 > 2$, then $\frac{3x^2+1}{x^3-2} > 0$. By the Archimedean property, $\exists n > 0$ such that $\frac{3x^2+1}{x^3-2} < n$. By re-arranging the terms, we get

$$0 > -\frac{(3x^2+1)}{n} > 2-x^3.$$

Then

$$\left(x-\frac{1}{n}\right)^3 = x^3 - \frac{3x^2}{n} + \frac{3x}{n^2} - \frac{1}{n^3} \geq x^3 - \frac{3x^2}{n} - \frac{1}{n^3} \geq x^3 - \frac{3x^2}{n} - \frac{1}{n}$$
$$= x^3 - \frac{1}{n}(3x^2+1) > x^3 + 2 - x^3 = 2.$$

Since $(x-\frac{1}{n})^3 > 2$, $x-\frac{1}{n}$ is an upper bound of S. But $x > x - \frac{1}{n}$; x can not then be the supremum of S, which is a contradiction. Thus $x^3 \not> 2$.

That leaves only one alternative (since we know $x \in \mathbb{R}$): $x^3 = 2$ or, equivalently, $x = u = \sqrt[3]{2} > 0$.

(We could also show it is irrational, but we'll leave it as an exercise.) ■

14. **Proof.** In this case, we do not need to verify if s^* exists, as that is one of the hypotheses.

Set $v = \sup\{s^*, u\}$. Then, v is an upper bound of $S \cup \{u\}$ since $v \geq u$ and $v \geq s^* \geq s$ for all $s \in S$.

Furthermore, $v \in S \cup \{u\}$.

Hence, any upper bound of $S \cup \{u\}$ must be $\geq v$: consequently, v is the smallest upper bound of $\sup(S \cup \{u\})$. ■

15. **Proof.** We use induction on the cardinality of S to show the result.

Base case: if $|S| = 1$, then $S = \{s_1\}$ for some $s_1 \in \mathbb{R}$. Clearly, $s_1 = \sup S \in S$.

Induction step: Suppose that the result holds for any set whose cardinality is $n = k$. Let S be any set with $|S| = k + 1$, say

$$S = \{s_1, \ldots, s_k, s_{k+1}\}.$$

Write $S = T \cup \{s_{k+1}\}$, with $T = \{s_1, \ldots, s_k\}$. Note that we can assume that $s_{k+1} \notin T$ (otherwise $|S| = k$).

Then T is non-empty and bounded since it is finite (exercise: a finite set is bounded); by completeness, $t^* = \sup T$ exists.

However, $|T| = k$. By the induction hypothesis, then, $\sup T \in T$, i.e. $t^* = s_j$ for some $j \in \{1, \dots, k\}$.

According to the preceding problem,

$$\sup S = \sup(T \cup \{s_{k+1}\}) = \sup\{t^*, s_{k+1}\} \in T \cup \{s_{k+1}\} = S.$$

By induction, any non-empty finite set contains its supremum (and infimum too – it's the same idea). ■

16. **Proof.** As S is non-empty and bounded, $\sup S$ and $\inf S$ exist by the completeness of $\mathbb{R}$.

Since $\inf S \leq s \leq \sup S$ for all $s \in S$, then $\inf S \leq \sup S$ and so the interval $I_S = [\inf S, \sup S]$ is well-defined.

Furthermore, the string of inequalities above also shows that $S \subseteq I_S$.

Now, let $J = [a, b]$ be a closed interval containing S. Then $a \leq s \leq b$ for all $s \in S$. Thus, a is a lower bound and b is an upper bound of S.

By definition,

$$a \leq \inf S \leq \sup S \leq b,$$

and so $I_S = [\inf S, \sup S] \subseteq [a, b] = J$. ■

17. **Proof.** Suppose $x \in \bigcap K_n$. Then $x \in K_n$ for all n, i.e. $x > n$ for all $n \in \mathbb{N}$. This implies x is an upper bound of $\mathbb{N}$, which contradicts the Archimedean property. Hence, $\bigcap K_n = \varnothing$.

If you do not like contradiction proofs, here is the same proof, but presented as a direct proof.

Let $x \in \mathbb{R}$. We will show that $x \notin \bigcap K_n$; as x is arbitrary, this implies $\bigcap K_n = \varnothing$.

By the Archimedean property, there is a positive integer N such that $N > x$. Hence $x \notin K_n$ for all $n \geq N$. The conclusion follows. ■

18. **Proof.** If $S = \varnothing$, then $S \cup \{s^*\} = \{s^*\}$ is finite as the function $f : \mathbb{N}_1 \to \{s^*\}$ defined by $f(1) = s^*$ is a bijection.

Now, suppose $S \neq \varnothing$. As S is finite, there exist an integer k and a bijection $f : \mathbb{N}_k \to S$.

Define the associated function $\tilde{f} : \mathbb{N}_{k+1} \to S \cup \{s^*\}$ by

$$\tilde{f}(i) = \begin{cases} f(i) & \text{if } 1 \leq i \leq k \\ s^* & \text{if } i = k+1 \end{cases}.$$

As $s^* \notin S$, $\tilde{f}$ is a bijection. Hence $S \cup \{s^*\}$ is finite. ■

19. **Proof.** Write $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n > 0, \gcd(m, n) = 1\}$, where $\gcd(m, n)$ is the greatest common divisor of m, n. Define the map $f : \mathbb{Q} \to \mathbb{Z}$ by $f(\frac{m}{n}) = m$. To see that this is surjective, note that for all $m \in \mathbb{Z}$, $\frac{m}{1} \in \mathbb{Q}$ and $f(\frac{m}{1}) = m$.

    Next, we define the map $g : \mathbb{Z} \to \mathbb{Q}$ according to three cases: for numbers of the form

    (a) $2^a 3^b$ with $a, b \in \{0, 1, 2, \ldots\}$, set $g(2^a 3^b) = \frac{a}{b}$.
    (b) $-2^a 3^b$ with $a, b \in \{0, 1, 2, \ldots\}$, set $g(-2^a 3^b) = -\frac{a}{b}$.
    (c) every other type n, set $g(n) = 0$.

    We need to check that g is well-defined, and then that it is surjective. To see that it is well-defined, we note that integers have unique prime decompositions, and $2, 3$ are prime.

This means that every number can have *at most* one decomposition of the form $\pm 2^a 3^b$, so every number is in *at most* one case. It is also clear that every number n must be in *at least* one case. Thus, every number belongs to *exactly one case*, so it is well-defined.

To check that g is surjective, we consider some $\frac{m}{n} \in \mathbb{Q}$ and again consider three cases:

(a) $\frac{m}{n} > 0$: $g(2^m 3^n) = \frac{m}{n}$.
(b) $\frac{m}{n} < 0$: $g(-2^m 3^n) = \frac{m}{n}$.
(c) $\frac{m}{n} = 0$: $g(5) = \frac{m}{n}$.

This completes the proof (there are other bijections). ■

20. **Proof.** Let a, b be two multiplicative identities in a field. Since a is a multiplicative identity,

$$ab = b.$$

Since b is a multiplicative identity,

$$ab = a.$$

Combining these two equations,

$$b = ab = a.$$

This completes the proof. ■

21. **Proof.** Each equality is labeled with the field axiom used:

$$\begin{aligned}
(2x-1)(2x+1) &\overset{\text{D1}}{=} 2x(2x+1)+(-1)(2x+1) \\
&\overset{\text{D1}}{=} (2x)(2x)+(1)2x+(-1)(2x)+(-1)(1) \\
&\overset{\text{D1}}{=} (2x)(2x)+(1+(-1))2x+(-1)(1) \\
&\overset{\text{A4}}{=} (2x)(2x)+(-1)(1) \overset{\text{A3}}{=} (2x)(2x)-1 \\
&\overset{\text{M1}}{=} ((2)(2))(x^2)-1 = ((1+1)(1+1))(x^2)-1 \\
&\overset{\text{D1}}{=} (1(1+1)+1(1+1))x^2-1 \\
&\overset{\text{M3}}{=} 4x^2-1.
\end{aligned}$$

This completes the proof. ■

22. **Proof.** Assume first that $x > 0$. By O4 (and the fact that $0 < \frac{1}{2} < 1$), this means

$$\left(\frac{1}{2}\right) x > \left(\frac{1}{2}\right) \cdot 0 = 0$$

as well. By O3, since $\frac{x}{2} > 0$,

$$\frac{x}{2} < \frac{x}{2} + \frac{x}{2} = x.$$

Putting together these two sequences of inequalities, we have

$$0 < \frac{x}{2} < x.$$

But then we have found some number $\varepsilon = \frac{x}{2} > 0$ so that $x > \varepsilon$; this contradicts the original assumption. Thus, we conclude that our original assumption $x > 0$ is false; by O1, we conclude $x \leq 0$. ■

23. **Proof.** Consider the interval $I = [0, 10]$, define $S = \{x \in I : x^2 + x < 5\}$, and define $A = \sup S$. Note that for $x \in [0, 1]$,

$$x^2 + x - 5 \leq 1^2 + 1 - 5 = -3 < 0,$$

so $A \geq 1$. Similarly, for $x \in [9, 10]$,

$$x^2 + x - 5 \geq 9^2 + 9 - 5 > 0,$$

so $A \leq 9$.

Claim: $A^2 + A = 5$. This is shown in two parts: first we show that $A^2 + A \leq 5$, then we show that $A^2 + A \geq 5$.

We show that $A^2 + A \leq 5$ by contradiction. Let us assume $A^2 + A > 5$.

Then, by previous exercise, there exists some $0 < \varepsilon < 1$ so that $A^2 + A > 5 + \varepsilon$. But then for all $0 < \delta < \frac{\varepsilon}{100}$, we have

$$\begin{aligned}(A-\delta)^2 + (A-\delta) &= A^2 - 2A\delta + \delta^2 + A - \delta \\ &\geq A^2 - (2)(10)(\delta) + A - \delta \\ &\geq A^2 + A - 21\delta \\ &> A^2 + A - \varepsilon > 5.\end{aligned}$$

Furthermore, since $A \geq 1$ and $\delta \leq 0.01$, we know that $A - \delta \in I$. Thus, in this case $A - \frac{\varepsilon}{100} < A$ is also an upper bound on S, contradicting the fact that A is defined to be the least upper bound on S.

We conclude that $A^2 + A \leq 5$.

Next, we show that $A^2 + A \geq 5$ by contradiction. Let us assume $A^2 + A < 5$. Then, by a previous exercise, there exists some $0 < \varepsilon < 1$ so that $A^2 + A < 5 - \varepsilon$. But then for all $0 < \delta < \frac{\varepsilon}{100}$, we have

$$\begin{aligned}(A+\delta)^2 + (A+\delta) &= A^2 + A + (2A + 1 + \delta)\delta \\ &\leq A^2 + A + 22\delta \\ &< A^2 + A - \varepsilon > 5.\end{aligned}$$

$Furthermore$, since $A \leq 9$ and $\delta \leq 0.01$, we know that $A + \delta \in I$. Thus, in this case $A + \frac{\varepsilon}{100} \in S$ and $A + \frac{\varepsilon}{100} > A$, contradicting the fact that A is defined to be an upper bound on S. We conclude that $A^2 + A \leq 5$.

Since $A^2 + A \leq 5$ and $A^2 + A \geq 5$, we conclude that $A^2 + A = 5$. ■

24. **Proof.** We prove the first claim by contradiction.

Assume there exists some $\varepsilon > 0$ so that $S \cap [A - \varepsilon, A]$ is empty. Since A is an upper bound for S, we also know that $S \cap (A, \infty)$ is empty.

Thus, $S \cap [A - \varepsilon, \infty)$ is empty. But this means that $A - \varepsilon < A$ is an upper bound for s, contradicting the fact that A is the least upper bound for S.

We conclude that in fact $S \cap [A - \varepsilon, A]$ is not empty.

We also prove the second part by contradiction.

Assume there exists some $\varepsilon > 0$ so that $S \cap [A - \varepsilon, A]$ is finite. Then we can enumerate its elements, $\{b_1, \ldots, b_n\}$. Let $B = \max(b_1, \ldots, b_n\}$.

Since $A \notin S$, we know that $b_1, \ldots, b_n < A$. Since B is a maximum of finitely many elements, this means that $B < A$ as well.

But then $A > A - \frac{A-B}{2} > B$, so $[A - \frac{A-B}{2}, A] \cap S$ is empty. But this is impossible, by the first part of the question.

This completes the proof. ■

25. **Solution.** The critical error is in the following part of the argument, in the case $n = 1$:

> "the collection of the first n sheep $\{x_1, \ldots, x_n\}$ are one colour, and the collection of the last n sheep $\{x_2, \ldots, x_{n+1}\}$ are also one (possibly different) colour. Since $\{x_2, \ldots, x_n\}$ are in both sets, both sets must in fact be the same colour, and so $\{x_1, \ldots, x_{n+1}\}$ are all one colour."

Consider the case $n = 1$. Then the collection $\{x_2, \ldots, x_n\}$ is actually empty, and so we cannot conclude that the two sets $\{x_1\}, \{x_2\}$ share any sheep, and so we cannot conclude that they are the same colour. ■