2. Numbers

Calculus deals with properties of functions defined on the set of real numbers. We therefore must first discuss what we mean by a "(real) number."

This is surprisingly involved. In modern mathematics it is often not a good idea to ask "what is …" It is usually a better idea to ask, "what properties does … have". The reason is that at a fundamental level, many definitions run the risk of being circular.

Now, one might argue that a real number is simply something that can be expressed using a (possibly) infinite decimal expansion such as 0.212441091 … This begs the question what are the digits $0,1,2,4,9$ here? Why, you say, they are natural numbers. So yes, it is possible to define what a real number is, if one has the natural numbers at one's disposal. But then deriving the usual properties of real numbers from this definition is rather tedious. And it also not so easy to define what a natural number "is". Usually, though, the definition of real numbers is done using sequences of rational numbers rather than decimal expansions.

In this course, we will start with the real numbers and assume that you are familiar with their major properties. We will not precisely answer the question "what is a real number."

In the following few sections, we briefly discuss some of these issues. We will not always provide full details, but rather aim to give an idea of the ideas involved.

As before, sections labelled with a * are not strictly speaking material required for this course. They are meant for the interested, and may provide some background.

2.1 From the natural to rational numbers

2.1.1 The natural numbers

What is a natural number? That is largely a philosophical question, which we unfortunately cannot answer precisely in this course.

There are "definitions" of natural numbers in foundational set theory, using systems of axioms. But they may not be very intuitive, and more importantly, there may be several objects satisfying these axioms, not just the set of natural numbers. But one can show that they are all essentially equivalent.

But one fundamental property of natural numbers is that they are used for counting: when counting objects, there is a first, second, third[1], and so on. This can be formalized as follows:

Peano Axioms

P1 There is a natural number 1.

P2 For every natural number n, there is a *successor* $S(n)$ (also a natural number).

P3 $S(n) = S(m)$ only if $n = m$.

P4 $1 \neq S(n)$ for all n. (So 1 is not a successor of any natural number.)

[1] Of course, talking about a "first," "second," and "third" seems to assume some knowledge of numbers.

P5 If a set contains 1 and for every natural number n also contains $S(n)$, then it contains all natural numbers.

These properties encapsulate the basics of "counting" things. The "successor" $S(n)$ of a natural number n should be thought of as (and is not surprisingly equal to) $n + 1$.

P5 is known as the *Principle of Induction* (POI):

Principle of Induction (POI)
Let X be a set that contains 1 and for every natural number n contains its successor $S(n)$. Then X contains all natural numbers.

We write $\mathbb{N}$ for the set of natural numbers (but note that we did not prove the existence or uniqueness of such a set).

Remark
This set exists in modern set theory. In ZFC set theory (see 1.4.2) one can define the set of natural numbers as follows:

$$0 \coloneqq \emptyset$$
$$1 \coloneqq \{0\}$$
$$S(n) \coloneqq n \cup \{n\}$$

Thus, $2 = 1 \cup \{1\} = \{0,1\}$; $3 = 2 \cup \{2\} = \{0,1\} \cup \{2\} = \{0,1,2\}$. In fact, this pattern holds, and every n is a set that contains all natural numbers before it.
By the *Axiom of Infinity* (an axiom in ZF set theory) there is a set X containing all natural numbers. A set that contains $1 = \{\emptyset\}$ and with any element x also $S(x) = x \cup \{x\}$ is called *inductive*. Then $\mathbb{N}$ is defined as the intersection of all inductive sets. One can show that this set satisfies the Peano Axioms. EOR.

Using the Peano Axioms one *constructs* the usual arithmetic of natural numbers (that is, the usual order relation, addition, and multiplication). The POI is used to prove that these constructions make sense. For example, the addition is defined so that $S(n) = n + 1$.

The usual order of natural numbers is based on the definition that $n < S(n)$. One then shows by induction that this defines a well-defined total order (we will discuss total orders below) on all of $\mathbb{N}$. It has the property that if $n < m$ then also $S(n) < S(m)$ and there is no natural number "between" n and $S(n)$. That is, for all $n, m \in \mathbb{N}$, the statement $n < m < S(n)$ is false. All of this is tedious and not very interesting. We write $n \leq m$ if $n < m$ or $n = m$.

Once we have the order $<$ on $\mathbb{N}$, the POI has the following (equivalent) consequence/reformulations:

Well Ordering Principle (WOP)
$\mathbb{N}$ is *well ordered*. That is, any nonempty subset has a smallest element. EOP

The WOP should not be confused with the *Well Ordering Axiom* in set theory, which states that every set can be well-ordered (which means every set admits a so-called *total order* that is a well-ordering, i.e. where every nonempty set has a smallest element).

The Principle of Complete Induction (PCI)
Let S be a set of natural numbers with the following property:
If $k \in S$ for all natural numbers $k < n$, then $n \in S$.

Then $S = \mathbb{N}$. EOP.

Proof. We use P5 to prove that $S = \mathbb{N}$. For any natural number n, let $A(n)$ be the statement "$\forall k \leq n \in \mathbb{N}: k \in S$."

$1 \in S$ because the statemen "$\forall k < 1 \in \mathbb{N}: k \in S$" is true (as there are no natural numbers < 1). It follows that $A(1)$ is also true.

Next, suppose $A(n)$ is true for some natural number n. Then $k \in S$ for all natural numbers $k \leq n$, and therefore $k \in S$ for all natural numbers $k < n + 1$ (this uses that there are no natural numbers between n and $n + 1$). It follows that $n + 1 \in S$. But that means $A(n + 1)$ is true, and in particular $n + 1 \in S$. By P5 this means $S = \mathbb{N}$. QED.

The POI is at heart of *proofs by induction*. We postpone discussing them in greater detail until we have developed enough material that we have something to prove. See Section 2.5 below.

Related is also the concept of *recursive definition*. Those are definitions of mathematical objects A_n depending on a natural number n, where A_n is defined using the objects $A_1, A_2, \dots, A_{n-1}$ (and possibly other data). We will discuss them in 2.5.1 below.

2.1.2 *The arithmetic of natural numbers

We all know that we can add and multiply natural numbers, and that they are "ordered", meaning we have an order relation $<$ so that for any pair $n, m \in \mathbb{N}$ we have one and only one of $n < m$, or $n = m$, or $m < n$. Typically, we say "n is (strictly) less that m" if $n < m$. And "n is (strictly) greater than m" if x$m < n$. We also write $m > n$ if $n < m$, $n \leq m$ if $n = m$ or $n < m$, and $n \geq m$ if $n > m$ or $n = m$.

The point of this excursion is to show how one could define this order simply from the Peano Axioms. To do this, we will for each natural number n define a certain set G_n of natural numbers (which will be the set of all numbers strictly greater than n).

What would we expect from the order $<$? We would expect three properties:

1. It should be **transitive**: if $m < n$ and $n < p$, then also $m < p$.
2. For each pair m, n one and only one statement should be true: $m < n$, $m = n$, $n < m$.
3. $n < S(n)$
4. If $m < n$, then $S(m) < S(n)$.

The last one is a reflection of that later we will see $S(n) = n + 1$, and this is the natural definition. We are not precise here, and do not care whether one of those statements could be proved by the others. In fact 4 is a consequence of the rest.

If we had defined the order $<$ we would therefore expect that the set $G_n = \{ m \in \mathbb{N} \mid m > n \}$ has the following properties:

1. $n \notin G_n$
2. $S(n) \in G_n$
3. If $m \in G_n$, then also $S(m) \in G_n$

The last property would be a consequence of transitivity: $n < m$ and $m < S(m)$ should force $n < S(m)$.

It turns out we can also go the other way: if we have a set G_n with these three properties for all n, then we can define an order satisfying the above properties.

Proposition
For each $n \in \mathbb{N}$ there exists a unique subset $G_n \subset \mathbb{N}$ such that:

1. $n \notin G_n$ but $S(n) \in G_n$
2. If $m \in G_n$ then $S(m) \in G\_n$

EOP.

Proof. This is a proof by induction. Let S be the set of all natural numbers for which the proposition is true. We must show that $S = \mathbb{N}$.

$1 \in S$: Let $G_1 = \mathbb{N} \setminus \{1\}$. Then G_1 clearly satisfies 1. and 2. It is also unique with this property: Let T be any set satisfying 1. and 2. for $n = 1$. Then $T \cup \{1\} = \mathbb{N}$. Indeed, $1 \in T \cup \{1\}$. And if $m \in T \cup \{1\}$, then $m = 1$ or $m \in T$. If $m = 1$, then $S(m) \in T$ by 1. If $m \in T$, then $S(m) \in T$ by 2. Together $S(m) \in T \cup \{1\}$. By P5, this means $T \cup \{1\} = \mathbb{N}$. Since $1 \notin T$, this means $T = \mathbb{N} \setminus \{1\}$. It follows G_1 is the one and only set satisfying 1. and 2. for $n = 1$.

Induction step: suppose a given natural number n is an element of S. We must prove that also $S(n) \in S$.

For this observe that $S(n) \in G_n$ and. We define $G_{S(n)} \coloneqq G_n \setminus \{S(n)\}$, so we simply drop $S(n)$. Then $G_{S(n)}$ satisfies 1 and 2 with respect to $S(n)$:

$S(n) \notin G_{S(n)}$ because we dropped it. But $S(n) \in G_n$, and therefore $S\big(S(n)\big) \in G_n$, and therefore $S\big(S(n)\big) \in G_{S(n)}$ proving 1.

If $m \in G_{S(n)}$ then $m \in G_n$, and $S(m) \in G_n$. But $S(m) \neq S(n)$ because $m \neq n$, and therefore $S(m) \in G_{S(n)}$ proving 2.

It remains to show that this set is unique. Let H be a subset of $\mathbb{N}$ such that 1. and 2. are satisfied with respect to $S(n)$. We must show that $H = G_{S(n)}$.

Let $K = H \cup \{S(n)\}$. Then K is a set satisfying 1. and 2. for n. Indeed, $n \notin K$, for otherwise $n \in H$ and therefore $S(n) \in H$, a contradiction. $S(n) \in K$ by construction. If $m \in K$ then $S(m) \in H$: for if $m \in H$ this follows by the assumptions on H and if $m = S(n)$, then $S(m) \in H$ by 1 applied to H.

Since $n \in S$ this means $K = G_n$. But then it is clear that $H = G_n \setminus \{S(n)\} = G_{S(n)}$, and also $S(n) \in S$. QED.

We could now **define** an order $<$ on $\mathbb{N}$ as follows:

$n < m$ if $m \in G_n$.

One then needs to do several induction proofs to show that this does indeed define an order with the desired properties.

2.2 The fundamental properties of the real numbers

We will treat the set $\mathbb{R}$ of real numbers as a given and assume that you all are familiar with them. But it is important and interesting to analyze which properties of the real numbers we really need, and what is "fluff."

Is it important that real numbers can be expressed using a "decimal expansion"? Sometimes. Is it important that we know how to add and multiply decimal expansions explicitly (or how the addition and multiplication of real numbers is defined)? Not really, as far as mathematics is concerned.

On the other hand, we are used to so many important properties of real numbers that we forget they are far from "obvious" or given. For instance, why is the addition of real numbers commutative or associative? (We will define the meaning of these words below.)

We will not bother with defining what a real number "is" but list their most important properties. It turns out, just accepting these properties is enough to do everything you ever wanted to do with real numbers. At this point you do not need to know or care how they are defined.

This is certainly unsatisfactory. It would be much nicer, if we could simply say "a real number x is an object defined as follows…" We will see one possible definition of a real number a little later in the course. For now, we will just list the main things we know and assume as given about real numbers.

We will phrase these properties using "axioms", ie. a list of fundamental rules. There are many other systems satisfying some of these rules**. In the end we will arrive at a complete list of properties that completely characterize the real numbers**. Describing this list, is our first rule of business.

If you feel lost, it is always OK to substitute for any "F" below the set $\mathbb{R}$ of real numbers. However, it is a good practice to get used to more "abstraction" as this is at the heart of modern mathematics. We will phrase some results generally and not just as it applies to real numbers. Thus, you learn how useful it can be to use the axiomatic method (as any rules derived from some of the axioms may apply in a broader context than just the situation at hand), but also how little we must know about the real numbers in order to deduce most elementary facts that we are used to.

From now on, we assume that there is a set $\mathbb{R}$, equipped with operations $+$ and $\cdot$, called **addition** and **multiplication**, respectively. We call this the **field of real numbers**. An element of $\mathbb{R}$ is consequently called a **real number**.

We will assume that $\mathbb{R}$ contains the set $\mathbb{N}$ of natural numbers as a subset. We will see later how we could define a subset N of $\mathbb{R}$ satisfying the Peano Axioms. Here we remark only that $S(n) = n + 1$ for all $n \in \mathbb{N}$.

In the following, we will exhibit the properties we expect the set of real numbers has.

2.2.1 Fields

The real numbers form a field

A **field** is a mathematical structure (a **set** F together with two binary operations[2] called **addition** ("+") and **multiplication** ("· ") such that the following rules are satisfied:

F1. The addition is **associative**: $\forall x, y, z \in F: x + (y + z) = (x + y) + z$.

F2. The addition is **commutative**: $\forall x, y \in F: x + y = y + x$.

F3. There is an **identity element/neutral element** for the addition, denoted 0: $\forall x \in F: x + 0 = x$.

F4. Each element has an **additive inverse**: $\forall x \in F: \exists x': x + x' = 0$.

F5. The multiplication is **associative**: $\forall x, y, z \in F: x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

F6. The multiplication is **commutative**: $\forall x, y \in F: x \cdot y = y \cdot x$.

F7. There is an **identity element/neutral element** for the multiplication, denoted 1, and $1 \neq 0$: $\forall x \in F: 1 \cdot x = x$.

F8. Every element $x \neq 0$ has a **multiplicative inverse**: $\forall x \neq 0 \in F: \exists x': x \cdot x' = 1$.

F9. Addition and multiplication are connected by the **distributive law**: $\forall x, y, z \in F: x \cdot (y + z) = x \cdot y + x \cdot z$.

There are many fields other than the real numbers: for example, the set $\mathbb{Q}$ of rational numbers, or the set $\mathbb{C}$ of complex numbers form fields (if addition and multiplication are properly defined). As far as arithmetic is concerned, these are the fundamental properties. Everything else is a consequence, or (like the ordering below) an added on structure to gain additional insights in special cases.

Example

1. There are also more exotic examples: $\mathbb{F}_2 = \{0,1\}$ with addition and multiplication defined as $0 + 0 = 0, 0 + 1 = 1 + 0 = 0$, and $0 \cdot 1 = 1 \cdot 0 = 0, 1 \cdot 1 = 1$.
2. The field of rational "functions" $\mathbb{R}(x) = \left\{ \frac{p}{q} \,\middle|\, p, q \text{ polynomials in } x \text{ with } q \neq 0 \right\}$. Here a "polynomial in x" is an "expression[3]" $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ with $a_i \in \mathbb{R}$. Polynomials are added and multiplied in the obvious way. The expression $\frac{p}{q}$ here should be understood in the same way a rational number $\frac{n}{m}$ is understood. The condition $q \neq 0$ should not be confused with the condition $q(x) \neq 0$ for all x: $q \neq 0$ means that there is at least one value for x such that $q(x) \neq 0$. Equivalently, as we will see, at least one of the coefficients a_i must be nonzero.
3. Let us put $-\mathbb{N} = \{-n \mid n \in \mathbb{N} \subset \mathbb{R}\}$. Then $\mathbb{Z} \coloneqq -\mathbb{N} \cup \{0\} \cup \mathbb{N}$ is called the **ring of integers**. It is closed under addition and multiplication and contains $0,1$ (this needs a proof). It also contains additive inverses of all its elements, but it does not contain all multiplicative inverses. For example, 2 has no multiplicative inverse in $\mathbb{Z}$. (We of course know this, but it is surprisingly

[2] A **binary operation** on a set S is an operation (ie. function) $S \times S \to S$: its input are two elements of S, and its output is again an element of S. Often the output (that is, the image of $(s, t) \in S \times S$) is denoted by $s * t$ where "$*$" is some symbol (or occasionally no symbol at al

[3] This is not a precise definition. There is a way to formalize this and put it onto set theoretically sound foundations. But it would lead too far here.

difficult to prove just from the definition of $\mathbb{Z}$; we omit it for now, since we have not yet properly defined how the natural numbers sit inside $\mathbb{R}$.)

4. To remedy this problem, we define $\mathbb{Q} \coloneqq \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, b \neq 0 \right\} \subseteq \mathbb{R}$ and call this the **field of rational numbers**. It is closed under addition, multiplication, contains $0,1$ and with every element its negative and its multiplicative inverse (if nonzero). It is therefore a field in its own right. Subsets of $\mathbb{R}$ (or any field) with this property are called **subfields**.

EOE.

It turns out, however, for many results relating to fields, it is completely irrelevant *how* addition and multiplication are defined. It is only relevant that these operations satisfy the properties F1-F9.

Proposition

1. The additive and multiplicative identities in a field are unique.
2. The additive and multiplicative inverses of an element in a field are unique.

EOP.

Proof. Let F be a field. For 1. suppose there are elements a, b such that $x + a = x$ and $x + b = x$ for all $x \in F$. Then $a = a + b$ because b is an identity element for the addition. But $a + b = b + a = b$ because a is an additive identity element. Therefore $a = b$. So the zero element in a field is unique.

A similar argument shows that the multiplicative identity is unique. If $ex = x$ for all $x \in F$ and also $fx = x$ for all $x \in F$, then $e = fe = ef = f$, using F6 and the hypothesis that both e, f are identity elements for the multiplication.

For 2. Suppose $x + x' = 0 = x + x''$. Then

$$x' = x' + 0 = x' + (x + x'') = (x' + x) + x'' = (x + x') + x'' = 0 + x'' = x''$$

A similar argument shows that if $xx' = 1 = xx''$ (assuming $x \neq 0$), then $x' = x''$. We leave that as an exercise. QED.

Notation

Because of the uniqueness of inverses, we define $-x$ as the unique element of F such that $x + (-x) = 0$. Likewise, if $x \neq 0$, we define x^{-1} to be the unique element of F such that $x \cdot x^{-1} = 1$. We often also write $\frac{1}{x}$ for x^{-1}. EON.

In school you learned that $(-1)x = -x$, that $xy = 0$ only if $x = 0$ or $y = 0$, and several other statements about the arithmetic of real numbers. These properties are not special to the reals:

Theorem (Arithmetic in a field; AIF)

Let F be a field and $x, y, z \in F$. Then

1. $-(-x) = x$; and if $x \neq 0$, $(x^{-1})^{-1} = x$
2. If $x + z = y + z$, then $x = y$
3. If $z \neq 0$, and $xz = yz$, then $x = y$
4. $0z = 0$
5. $(-x)y = -(xy) = x(-y)$
6. $(-1)y = y$
7. $xy = 0$ only if $x = 0$ or $y = 0$

EOT.

Proof.

1. By definition of $-y$ for any $y \in F$, we have $x = -(-x)$ if and only if $x + (-x) = 0$, which is true by the definition of $-x$. For nonzero x the argument for $x = (x^{-1})^{-1}$ is similar.
2. Suppose $x + z = y + z$. Then adding $-z$ on both sides, gives
$$(x + z) + (-z) = (y + z) + (-z)$$
By the associative law, the left hand side is equal to $x + \big(z + (-z)\big) = x + 0 = x$, whereas the right hand side is equal to $y + \big(z + (-z)\big) = y + 0 = y$. It follows that $x = y$.
3. This is very similar to 2.: If $z \neq 0$, and $xz = yz$, we may multiply both sides by z^{-1} and get
$$(xz)z^{-1} = (yz)z^{-1}$$
Again, the left hand side is equal to $x(zz^{-1}) = x \cdot 1 = x$, and the right hand side is equal to y.
4. Note that by F3, $0 + 0 = 0$. Therefore $0z = (0 + 0)z$. By F9, this is equal to $0z + 0z$. We find
$$0z = 0z + 0z$$
Or, written differently $0 + 0z = 0z + 0z$. We may therefore cancel $0z$ on both sides because of 3.
5. To show that $(-x)y = -(xy)$ it is necessary and sufficient to verify that $xy + (-x)y = 0$. Now $xy + (-x)y = \big(x + (-x)\big)y = 0y = 0$ by 4. Now $x(-y) = (-y)x = -(yx) = -(xy)$ by what we just proved (you could also prove it directly again).
6. This is the 5. applied to the case $x = 1$ (which uses F7: $1y = y$).
7. Suppose $xy = 0$. If $x \neq 0$, let $c = x^{-1}$. Then $xy = 0$ means $c(xy) = c0 = 0$ by 4. On other hand, $c(xy) = (cx)y = 1y = y$. Thus, if $x \neq 0$, then $y = 0$, which is what we needed to show.

QED.

Notation
In any field F, we write $a - b$ instead of $a + (-b)$.
For a natural number n and $x \in F$, we put $x^n = \underbrace{xx \cdots x}_{n \text{ factors}}$.

EON.

Exercise

1. For each of the statements in AIF, verify which field axioms (F1-F9) were used at each step in the proof.
2. Verify the following statements for all a, b in a field F: $-(a + b) = -a - b$, $-(a - b) = b - a$.
3. Let us define an operation $\ominus$ on F as $a \ominus b \coloneqq a - b$. Is this an associative operation? That is, is it true that for all $a, b, c \in F$, $(a \ominus b) \ominus c = a \ominus (b \ominus c)$?
4. Show that in any field F the usual rules of adding and multiplying fractions apply: If $a, b, c, d \in F$ and $b, d \neq 0$, then $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

EOE.

2.2.2 Ordered fields

As we have seen there are many distinct fields. Therefore, the real numbers are not completely characterized by the fact that they form a field. An additional important property is the following:

The real numbers form an ordered field.

Definition
A field F together with a subset P is called **ordered**, if P has the following properties
OF1. $\forall x \in F$ exactly one property is true: $x \in P, -x \in P$, or $x = 0$.
OF2. $\forall x, y \in P$, $x \cdot y \in P$ and $x + y \in P$
Strictly speaking, the pair (F, P) is called an ordered field as a field may a priori allow several different subsets P with this property.
EOD.

You should think of P as the **set of positive** elements, and we define $x \in F$ to be **positive** if $x \in P$ and **negative** if $-x \in P$.

One then defines a **total order** on F as

$$x < y : \Leftrightarrow y - x \in P$$

We write $x > y$ if $y < x$. In addition, we write $x \leq y$ if $x < y$ or $x = y$. Similarly, $x \geq y$ if $x > y$ or $x = y$.

From the definition above it follows immediately that $x > 0 \Leftrightarrow x \in P$.

Example
The most important examples of ordered fields are $\mathbb{Q}$ and $\mathbb{R}$. But here is another one: the field $\mathbb{R}(x)$ discussed above can be turned into an ordered field by defining $x > a$ for all $a \in \mathbb{R}$. To be precise: $P = \left\{ \frac{p}{q} \,\middle|\, L(p), L(q) > 0 \right\}$, where for a polynomial $p = a_n x^n + a_{n-1} x^n + \cdots + a_0$ with $a_n \neq 0$, we write $L(p) = a_n$. EOE.

Proposition (Useful facts about orders; UFO)
In an ordered field F the following holds:

1. $\forall x, y \in F$, one and only one statement holds: $x < y$, $x = y$, $y < x$.
2. $\forall x, y, z \in F$: $x < y$ and $y < z \Rightarrow x < z$. This is referred to as the order being **transitive**.
3. $\forall x, y, z \in F$: If $x < y$, then $x + z < y + z$.
4. $\forall x, y, z \in F$: If $x < y$ and $z \in P$, then $zx < zy$.
5. $\forall x, y, z \in F$: If $x < y$ and $-z \in P$, then $zx > zy$.
6. $\forall x \in F$: If $x > 0$, then $x^{-1} > 0$.
7. $\forall x, y \in F$: If $x < y$, then $-x > -y$.
8. $\forall x, y \in F$: If $x, y \neq 0$ and $x < y$ then $x^{-1} > y^{-1}$.
9. $\forall x, y \in F, \forall\, n \in \mathbb{N}$: If $0 < x, y$, then $x < y$ if and only if $x^n < y^n$.
10. $\forall x \in F$: If $x \neq 0$ then $x^2 > 0$.
11. $\forall x, y \in F$: If $x, y \in P$, then $(-x)(-y) \in P$ and $-(xy) = (-x)y = x(-y) \notin P$.

EOP.

Statements 1 and 2 are the definition of a **total order** (on any set). Statements 1, 2, 3, and 4 are also called the **Order Axioms** for ordered fields. One can define an ordered field also as a field with a relation $<$ satisfying these 4 properties (of course for 4. one must replace the condition $c \in P$ with $c > 0$).

Proof (of the Proposition). Here we will show only selected statements and leave the rest as an exercise.

1. By definition, we have exactly one of $y - x \in P$, $y - x = 0$, or $-(y - x) \in P$. The first means $x < y$, the second $x = y$, and the last $x - y \in P$, ie. $y < x$.
2. Suppose $x < y$ and $y < z$. Then $y - x \in P$ and $z - y \in P$. It follows that $z - x = (z - y) + (y - x) \in P$. Hence, $x < z$.
3. If $y - x \in P$ then also $(y + z) - (x + z) = y - z \in P$.
4. If $x < y$ then $y - x \in P$ so if $z \in P$ then also $z(y - x) \in P$, so $zy - zx \in P$, ie. $zx < zy$.
5. Suppose $x < y$, and $-z \in P$. By UFO4 $(-z)x < (-z)y$. By AIF5 $(-z)x = -(zx)$ and $(-z)y = -(zy)$. Thus $-zx < -zy$, that is $-zy - (-zx) \in P$, that is $zx - zy \in P$ (see also Exercise 2. in 2.2.1). But that means $zx > zy$.
6. Suppose $x > 0$. If $x^{-1} < 0$, then UFO4 guarantees that $xx^{-1} < x0 = 0$. But then $1 < 0$. But $1 = 1^2 > 0$ because of UFO10. We must have $x^{-1} > 0$.
7. If $0 < x < y$, then $y - x \in P$, and so $-(x - y) = (-x) - (-y) \in P$, so $= -x > -y$.
8. If $0 < x < y$, then $x^{-1} > y^{-1}$. Indeed, then $x \neq y$, so $x^{-1} \neq y^{-1}$. Both are positive by UFO6. But if $x^{-1} < y^{-1}$, then $1 = xx^{-1} < xy^{-1} < yy^{-1}$ (applying UFO4 twice).
9. This needs a proof by induction. But first observe that if $c \in P$, then $c^n \in P$ for any natural number n (again, this would need a proof by induction; do it as an exercise).
   Base case ($n = 1$): Obvious, as $x < y$ if and only if $x^1 < x^1$.
   Inductions step: Suppose for a given natural number n, the assertion is true: $x < y$ if and only if $x^n < y^n$.
   We must verify that $x < y$ if and only if $x^{n+1} < y^{n+1}$.
   Suppose $x < y$: Note that by UFO4, $x \cdot x^n < x \cdot y^n$. By UFO4 again $x \cdot y^n < y \cdot y^n$ because $y^n > 0$. Transitivity (UFO2) gives that $x^{n+1} < y^{n+1}$.
   Suppose that $x^{n+1} < y^{n+1}$. Then clearly $x \neq y$. Also, if $x > y$, we just proved that $y^{n+1} < x^{n+1}$. Therefore $x < y$, as needed.
10. Note that if $x > 0$ then $x^2 > 0$, as $x^2 \in P$. If $-x \in P$, then $(-x)^2 = (-1)^2x^2 = x^2 \in P$.
11. Suppose $x, y \in P$. Then $(-x)(-y) \in P$, as $(-x)(-y) = -(-xy) = xy \in P$. Similarly, as $xy \in P$, $-(xy) = (-x)y = x(-y) \notin P$.

QED.

Remark
Convince yourself that UFO11 is true. It then shows that the old helper "negative times negative = positive" and "negative times positive = negative" holds even in this more abstract setting. EOR.

Note that UFO9 implies that $1 = 1^2 > 0$ in any ordered field. In the field $\mathbb{C}$ of complex numbers there is an element (in fact two) i such that $i^2 = -1$. **Thus $\mathbb{C}$ cannot be ordered because in an ordered field, -1 is never positive.**

2.2.3 The natural numbers

In this course we treat $\mathbb{R}$ as the fundamental set (whose existence and properties we will assume as given). This leaves us with a problem: what "is" a natural number? Which set inside $\mathbb{R}$ should play the role of natural numbers?

Definition
Let F be a field and $S \subseteq F$ a subset. We say S is **inductive** if S has the following two properties:

1. $1 \in S$

2. $\forall x \in S: x + 1 \in S$

EOD.

In particular, this means an inductive set is never empty.

One can show that the intersection of all inductive subsets of $\mathbb{R}$ is again inductive (exercise). This is what we will call the set of natural numbers.

Definition
The set of natural numbers $\mathbb{N}$ is defined as the intersection of all inductive subsets of $\mathbb{R}$. EOD.

You may now forget (in theory, please don't) any preconceived notion you had about natural numbers and work only with this definition.

Proposition
Let $\mathbb{N}$ be defined as above. For $n \in \mathbb{N}$ define $S(n) \coloneqq n + 1$. Then $S(n) \in \mathbb{N}$ and $\mathbb{N}$ together with this successor function satisfies the Peano Axioms. EOP.

Proof. We have remarked that $\mathbb{N}$ is inductive. Therefore $1 \in \mathbb{N}$ and P1 is satisfied.

Next, because $\mathbb{N}$ is inductive, $S(n) = n + 1$ is again a natural number for all $n \in \mathbb{N}$. Obviously also this gives us P2.

If $S(n) = S(m)$ then $n + 1 = m + 1$ and therefore $n = m$ by AIF2. Hence P3 holds.

The set $\mathbb{R}_{>0} = \{ x \in \mathbb{R} \mid x > 0 \}$ is inductive. By the definition of $\mathbb{N}$, it is a subset of all inductive subsets of $\mathbb{R}$, and hence a subset of $\mathbb{R}_{>0}$. Therefore $1 - 1 = 0$ is not a natural number, and 1 is not the successor of a natural number. This gives P4.

Finally, let $S \subseteq \mathbb{N}$ be a set that contains 1 and for every $n \in S$ contains $S(n) = n + 1$. Then S is an inductive set, and by definition we must also have $\mathbb{N} \subseteq S$, and therefore $S = \mathbb{N}$, proving P5. QED.

We have now concretely identified a subset $\mathbb{R}$ that satisfies the Peano Axioms. It also has an order relation (inherited from $\mathbb{R}$) and it turns out it is the same order relation one could also define using the Peano Axioms.

Let $H_n = \{ m \in \mathbb{N} \mid m > n \}$. Then $H_n = G_n$ as defined before (using only the Peano axioms). Indeed, $n \notin H_n$ but $n + 1 \in H_n$. And if $m \in H_n$ then $m + 1 > m > n$, so $m + 1 \in H_n$.

Facts
1. 1 is a minimum for $\mathbb{N}$: $1 \leq n$ for all $n \in \mathbb{N}$.
2. $\mathbb{N}$ is closed under addition and multiplication of real numbers.

Proof. The first statement follows from the fact that $\mathbb{R}_{\geq 1} = \{ x \in \mathbb{R} \mid x \geq 1 \}$ is inductive, and therefore contains $\mathbb{N}$.

The second statement requires a proof by induction: We first deal with the addition.

Let $A(n)$ be the statement: $m + n \in \mathbb{N}$ for all $m \in \mathbb{N}$.

The set $S = \{n \in \mathbb{N} \mid A(n)\}$ is inductive: $1 \in S$ by construction. If $n \in S$, then $m + n \in \mathbb{N}$ for all m. But then also $(m + n) + 1 = m + (n + 1) \in \mathbb{N}$ as $\mathbb{N}$ is inductive. Therefore $n + 1 \in S$. It follows $S = \mathbb{N}$.

For the multiplication we proceed in the same way. Here we put $T = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N}: mn \in \mathbb{N}\}$. Then T is inductive: $1 \in T$ as $m1 = m$ for all m. If $n \in T$, then $m(n+1) = mn + m$. Now $mn \in \mathbb{N}$ since $m \in T$, and $mn + m \in \mathbb{N}$ since $\mathbb{N}$ is closed under addition. Again, it follows that $T = \mathbb{N}$. QED.

One should now work to show that the addition and multiplication inherited from the real numbers is the one that one could also construct from the Peano Axioms. We will omit that.

We will make one final observation:

Let n be any natural number. Then there is no natural number m such that $n < m < n + 1$.

Indeed, let $S \subseteq \mathbb{N}$ be the set $S = \{\, n \in \mathbb{N} \mid \nexists m \in \mathbb{N}: n < m < n + 1 \,\}$. Then S is inductive.

To see this we need the following claim.

Claim
Every natural number except 1 is a successor.

Proof. Let $T \subseteq \mathbb{N}$ be the set of successors, that is $T = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}: m + 1 = n\}$. Then $T \cup \{1\}$ is inductive and hence $T \cup \{1\} = \mathbb{N}$. QED.

Returning to the argument above, $1 \in S$. Indeed if $1 < m < 2$, then m cannot be the successor of any natural number as $m - 1 < 1$ is not a natural number. Next, suppose $n \in S$, and let $1 < n + 1 < m < n + 2$. If m is a natural number, then $m > 1$, and so it is a successor. But then $n < m - 1 < n + 1$ contradicts the fact that $n \in S$. Therefore m cannot be a natural number and $n + 1 \in S$.

We conclude that $S = \mathbb{N}$.

2.2.4 The set $\mathbb{Z}$ of integers

We define the set $\mathbb{Z}$ of **integers** as the set $\mathbb{N} \cup \{0\} \cup -\mathbb{N}$ where $-\mathbb{N}$ is the set $\{\, n \in \mathbb{R} \mid -n \in \mathbb{N} \,\}$.

Exercise

1. Show that $\mathbb{Z}$ is an inductive subset of $\mathbb{R}$.
2. Show that $\mathbb{Z}$ is closed under addition, multiplication, contains 0 and 1.
3. Show that $\mathbb{Z}$ is closed under taking additive inverses: for every $n \in \mathbb{Z}$: $-n \in \mathbb{Z}$.
4. Show that $\mathbb{Z}$ is **not** closed under taking multiplicative inverses, that is there are integers $n \neq 0$ such that the real number $\frac{1}{n} \notin \mathbb{Z}$.

***Lemma**
Let $n \neq 0$ be an integer. If $n^{-1} \in \mathbb{Z}$ then then $n = \pm 1$. EOL.

Proof. Suppose first that $n > 0$. Then $n \geq 1$, so $n^{-1} \leq 1$. We also know by some UFO (which one?) that $\frac{1}{n} > 0$. If $n \neq 1$, then $0 < \frac{1}{n} < 1$, and therefore $\frac{1}{n}$ is not an integer (see the definition above).

Now let $n < 0$. Then $-n \in \mathbb{Z}$ (in fact $-n \in \mathbb{N}$). If $n \neq -1$, then $0 \neq -\frac{1}{n} \notin \mathbb{N}$ by the discussion above. But then $\frac{1}{n} \notin \mathbb{Z}$. QED.

This seemingly obvious statement is mentioned to see how we can argue just from definitions.

2.2.5 The set $\mathbb{Q}$ of rational numbers

The set of **rational numbers** is defined as $\mathbb{Q} = \{ ab^{-1} \mid a, b \in \mathbb{Z}, b \neq 0 \}$.

Exercise
Verify the claim made earlier, that $\mathbb{Q}$ is a subfield of $\mathbb{R}$. EOE.

2.2.6 Characteristic of a field.

Let F be a field. We can construct a special *function*[4] $f: \mathbb{N} \to F$ such that $f(ab) = f(a)f(b)$ and $f(a+b) = f(a) + f(b)$ by "adding 1":

Indeed, we define $f(1) = 1$ (where the right hand 1 is the 1 in F). Then $f(2) \coloneqq 1 + 1$, $f(3) = 1 + 1 + 1$, and so on. So formally $f(n) = \underbrace{1 + 1 + 1 + \cdots + 1}_{n \text{ summands}}$.

To be precise, we should phrase it as a recursive definition:

1. $f(1) = 1$.
2. $f(n+1) = f(n) + 1$

And then prove by induction (see below) that this is a well defined function satisfying $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

Definiton
Let F be a field. The **characteristic** of F is the *smallest* natural number p such that $f(p) = 0$ in F. If no such number exists, we say the characteristic of F is **zero**. EOD.

One can show that the characteristic of F is always a prime number or zero. For example, in $\mathbb{F}_2$, $1 + 1 = 0$, and $1 \neq 0$, so it is a field of characteristic 2. The characteristic of $\mathbb{R}$ is obviously 0.

In fact, a finite field cannot be ordered either:

Lemma (Characteristic)
Let F be an ordered field. Then the characteristic of F is zero. EOL.

Proof. We show by induction that for all $n \in \mathbb{N}$ we always have $f(n) > 0$, and therefore we never have $f(n) = 0$. Indeed, the base case is clear $f(1) = 1 \neq 0$ by F7 and UFO9. Suppose for a given n, we have $f(n) > 0$. Then $f(n+1) = f(n) + 1 > 0$: in F we have $1 > 0$ and hence $f(n) + 1 > f(n) + 0 = f(n) > 0$. This uses UFO3. QED.

If a field has characteristic zero, it contains a "copy" of $\mathbb{N}$. Indeed, the function f is one-one (injective): $f(n) = f(m)$ if and only if $n = m$: indeed, suppose $f(n) = f(m)$. If $n = m$, this is clear. Suppose $n > m$ (the case $n < m$ is similar). Let $k = n - m$. Then $f(m + k) = f(m) + f(k) = f(n)$, which forces $f(k) = 0$. But F has characteristic 0, so this is impossible.

We may thus think of $\mathbb{N}$ as a subset of F (by identifying $n \in \mathbb{N}$ with $f(n) \in F$). This identification respects the arithmetic operations in $\mathbb{N}$, and is in fact order preserving (if $n < m$, then $f(n) < f(m)$).

[4] We will properly define functions below.

Since every element in F has an additive inverse, for every $n \in \mathbb{N}$, there is an element $-f(n) \in F$. Thus, we may think of $\mathbb{Z}$ as a subset of F as well. But then nonzero integers have a mutiplicative inverse and so $\mathbb{Q}$ can be thought of as a subset of F. (One should formally prove this, but the proof does not provide further insights. You will see such proofs in e.g. MATH 227, 228, or 326.)

2.2.7 Supremum and infimum of a set

Definition (Intervals)
Let F be an ordered field and $a \leq b \in F$. We define

$$(a,b) \coloneqq \{x \in F \mid a < x < b\}$$
$$[a,b] \coloneqq \{x \in F \mid a \leq x \leq b\}$$
$$(a,b] \coloneqq \{x \in F \mid a < x \leq b\}$$
$$[a,b) \coloneqq \{x \in F \mid a \leq x < b\}$$

The first two sets are referred to as the **open**, resp. **closed** interval defined by a, b. The last two are called **half-open intervals**. EOD.

If $a < b$, these intervals are never empty. This is clear for the last three as these always contain a, or b, or both.

But even the first one is not empty.

Lemma (Existence of Average)
Let $a < b$. Then $a < \frac{a+b}{2} < b$. EOL.

The element $\frac{a+b}{2}$ is often called the **average** or **mean** of a and b.

Proof. Note that $\frac{a+b}{2}$ is a well-defined element of F, since we may think of $\mathbb{Q}$ (and hence $\mathbb{N}$) as a subset of F as discussed above. Therefore $\frac{1}{2} \in F$. Now since $a < b$ we have (by UFO 4) that $2a < 2b$, since $2 \in P$. On the other hand, the distributive law F9 says that $2a = a + a$ and $2b = b + b$. Then UFO 3 guarantees $2a = a + a < a + b < b + b = 2b$. UFO 4 again then gives $\frac{1}{2}(2a) < \frac{a+b}{2} < \frac{1}{2}(2b)$ and the associative law F5 translates that into $a < \frac{a+b}{2} < b$. QED.

In particular, between any two real (or rational) numbers there is another real (or rational) number.

Definition (SUP)
Let X be a totally ordered set (think $X = F$, where F is an ordered field), and let $S \subseteq X$ be a subset.
We say S is **bounded above** if $\exists x \in X$ such that $x \geq s \forall s \in S$. S is **bounded below**, if $\exists x \in X$ such that $x \leq s \forall s \in S$. S is **bounded** if it is both, bounded above and below.
An **upper (resp. lower) bound** of S is an element $x \in X$ such that $x \geq s$ (resp. $x \leq s$) for all $s \in S$.
A **least upper bound** or **supremum** for S is an upper bound x_0 such that if x is *any* upper bound then $x_0 \leq x$.
Similarly, a **greatest lower bound** or **infimum** is a lower bound x_0 such that if x is *any* lower bound, then $x \leq x_0$.
An upper bound u of a set S is called the **maximum** of S if $u \in S$. It is denoted $\max S$. Similarly, a lower bound ℓ of S is called the **minimum** of S, if $\ell \in S$. It is denoted $\min S$. EOD.

Exercise and example
Let A be nonempty subset of an ordered field. Suppose $a \in A$ is an upper bound for A.
Show that $a = \sup A$. EOE.

A set does not have to have a maximum or minimum even if it is bounded.

Lemma (SUP is unique)
Any supremum or infimum is unique (if it exists). EOL.

Proof. We show the case of a supremum. Let x_0, x_1 be suprema for S. As both are upper bounds we have $x_0 \leq x_1$ because x_0 is a least upper bound. Likewise, $x_1 \leq x_0$ because x_1 is a least upper bound. But that means $x_0 = x_1$. The case for infima is similar. QED.

Note that a set S has a maximum if and only if it has a supremum and $\sup S \in S$. Then the supremum and maximum coincide.

We write $s = \sup S$ if s is the unique supremum of S. Similarly, we write $i = \inf S$ if i is the unique infimum of S (if either exists).

A supremum need not exist: for example, in $\mathbb{R}$ the empty set has many upper bounds (any real number is an upper bound), but no least upper bound.

If $a < b \in F$, then $\sup(a, b) = b$ and $\inf(a, b) = a$. (a, b) has no maximum and no minimum.

To see this observe that b is an upper bound. Let $s \in F$ be an upper bound and suppose $s < b$. Note that $m = \frac{a+b}{2} \in (a, b)$, and therefore $a < m \leq s < b$. Therefore $s \in (a, b)$. But then also $s < \frac{s+b}{2} \in (a, b)$ and s is not an upper bound. The argument for $\inf(a, b) = a$ is similar.

2.2.8 Archimedean Fields

The real numbers form an Archimedean field
An ordered field is called **Archimedean** if it doesn't have any "infinite" element. That is, there is no element x such that $x > n$ for all $n \in \mathbb{N}$.

Formally, an Archimedean field satisfies:

AF. For every $x \in F$: $\exists n \in \mathbb{N}$: $x < n$.

Examples of Archimedean fields are $\mathbb{R}$ and $\mathbb{Q}$.

An Archimedean field also does not contain any "infinitesimal" elements. An element x is called **infinitesimal** if $0 < x < \frac{1}{n}$ for all $n \in \mathbb{N}$. Indeed, if $0 < x < \frac{1}{n}$ for all n, then $x^{-1} > n$ for all n by UFO8, a contradiction.

A consequence of AF is the fact that if $x > 0 \in F$ and $m \in \mathbb{N}$, then there is $n \in \mathbb{N}$ such that $nx > m$. Otherwise, $x \leq \frac{m}{n}$ for all n and hence $\frac{x}{m} \leq \frac{1}{n}$ for all n. But that means $\frac{x}{m}$ is an infinitesimal element (as "$=$" can hold for at most one n, and then $\frac{x}{m}$ is not $< \frac{1}{n+1}$). Note the fact that $m \in \mathbb{N}$ is not needed. It is enough that $m > 0 \in F$.

Lemma ($\mathbb{Q}$ is dense)
Let F be an Archimedean field and let $a < b \in F$. Then $(a, b) \cap \mathbb{Q}$ is never empty. EOL.

Proof. Recall that $(a, b) = \{x \in F \mid a < x < b\}$. Let $n_0 \in \mathbb{N}$ such that $n_0(b - a) > 1$. This exists, as $b - a$ cannot be infinitesimal. If $(n_0 a, n_0 b)$ contains a rational number r, so does (a, b) (namely $\frac{r}{n_0}$), so we may assume that $b - a > 1$. Thus, $a < a + 1 < b$. Choose $m \in \mathbb{N}$ such that $a + m > 1$. Such an m exists, as there is a natural number $> 1 - a$. Now let $n \in \mathbb{N}$ be minimal[5] such that $a + m < n$. Then $n \leq a + m + 1$. Indeed, as $a + m + 1 > 2$, if $n > a + m + 1 > 2$, then $n - 1$ is a natural number (n is a successor), and $n - 1 > a + m$, contradicting the minimality of n. And thus $n \in (a + m, b + m)$ and hence the rational number $n - m$ is contained in (a, b). QED.

Later we will see that this means we can "approximate" any element in F[6] by rational numbers.

Example
The ordered field $\mathbb{R}(x)$ of rational functions we discussed above is not Archimedian. Indeed, the element $x > n$ for all $n \in \mathbb{N}$. Thus, x is an "infinite" element. EOE.

Any Archimedian field F contains a copy of the rational numbers, and the rational numbers meet any "interval" in F.

We have seen that the empty set has no supremum in an Archimedean field. While this may seem like an artificial example, here is a more serious one:

Lemma (No SUP)
Let F be an Archimedean field. Let $S = \{r \in \mathbb{Q} \mid r^2 \leq 2\}$. Suppose $s = \sup S$ exists. Then $s^2 = 2$. EOL.

Proof. S is bounded above. Indeed, $r \leq 2$ for all $r \in S$ because if $r > 2$, then $r^2 > 2^2 = 4 > 2$. If $s^2 < 2$, then there is $n \in \mathbb{N}$ such that $\left(s + \frac{1}{n}\right)^2 \leq 2$. Indeed, $\left(s + \frac{1}{n}\right)^2 = s^2 + \frac{2s}{n} + \frac{1}{n^2}$. Let $t = 2 - s^2 > 0$. It suffices to find n such that $\frac{2s}{n} + \frac{1}{n^2} \leq t$. There is $n \in \mathbb{N}$ such that $nt > 2s + 1$. Then $t > \frac{2s}{n} + \frac{1}{n} > \frac{2s}{n} + \frac{1}{n^2}$. Now the interval $\left(s, s + \frac{1}{n}\right)$ contains a rational number r. But then $r^2 < \left(s + \frac{1}{n}\right)^2 < 2$. As a consequence, $r \in S$ and that means s is no upper bound.

If on the other hand $s^2 > 2$, a similar argument shows that there is $n \in \mathbb{N}$ such that $\left(s - \frac{1}{n}\right)^2 > 2$. For this we must find $n \in \mathbb{N}$ such that $s^2 - \frac{2s}{n} + \frac{1}{n^2} > 2$, or $\frac{2s}{n} - \frac{1}{n^2} < t \coloneqq s^2 - 2$. Again, for large enough n, we have $\frac{2s}{n} + \frac{1}{n^2} < t$ as above, and then also $\frac{2s}{n} - \frac{1}{n^2} < t$. Note that $s - \frac{1}{n} > 0$ as $s > 1$. But then $s - \frac{1}{n} < s$ is also an upper bound: if $r \in S$, then $r \leq 0$ means $r \leq s - \frac{1}{n}$ and if $r > 0$, then UFO9 forces $r < s - \frac{1}{n}$, and therefore s is not the supremum. QED.

Since there is no rational number with square equal to 2, $\sup S$ does not exist if $F = \mathbb{Q}$!

---

[5] This uses the Well Ordered Principle of $\mathbb{N}$.
[6] We will discuss this if $F = \mathbb{R}$, but it is true in any Archimedean field.

2.2.9 Complete fields (a.k.a the real numbers)

The real numbers form a complete field

This is what really sets the real numbers apart from the rational numbers and in fact most Archimedean fields.

Definition

An ordered field F is called **complete** if every nonempty set that is bounded above has a supremum. EOD.

The real numbers therefore satisfy the additional axiom

CF Every nonempty set bounded above has a supremum.

Exercise

Show that in a complete field every nonempty set bounded below has an infimum. EOE.

Lemma (Complete implies Archimedian)

A complete ordered field is always Archimedian. EOL.

Proof. Indeed, suppose there is $x \in F$ such that there is no $n \in \mathbb{N}$ such that $n > x$. Then $x \geq n$ for all n, and therefore $x > n$ for all $n \in \mathbb{N}$. Then $\mathbb{N}$ is bounded above and hence has a supremum s, say. So $n \leq s$ for all $n \in \mathbb{N}$, and there is $n \in \mathbb{N}$ such that $n > s - 1$. But then $n + 1 > s$, a contradiction. QED.

As a consequence, we can conclude:

Theorem

Let $a > 0$ be a positive real number. Then a has a square root, that is, there is $r \in \mathbb{R}$ such that $r^2 = a$. EOT.

Proof. Let $S = \{x \in \mathbb{R} \mid x^2 < a\}$. This set is nonempty ($0 \in S$), and bounded above ($a + 1$ is an upper bound, why?). Thus, there exists $s \coloneqq \sup S$. Similar arguments as in the above Lemma No SUP show that $s^2 = a$. QED.

Exercise

Fill in the details in the above proof. EOE.

We close by mentioning that we will assume the set $\mathbb{R}$ is a complete ordered field, and observing that this singles out $\mathbb{R}$ and completely characterizes it (for our purposes).

2.2.10 *Excursion: Why is $\mathbb{R}$ characterized by being a complete ordered field?

Let F be an Archimedian ordered field. We will construct a function $f: F \to \mathbb{R}$ which is injective (one-to-one), and respects addition and multiplication (and the order).

For $a \in F$, let $S_a \coloneqq \{r \in \mathbb{Q} \mid r < a\}$. This set is never empty, since $(a - 1, a)$ always contains a rational number. We may think of S_a as a subset of $\mathbb{R}$. Now put $f(a) \coloneqq \sup S_a \in \mathbb{R}$. This exists, because S_a as a subset of $\mathbb{R}$ is bounded above. Indeed, any rational number in $(a, a + 1)$ is an upper bound.

One now has to work a bit to show: for $a, b \in F$ we have $f(ab) = f(a)f(b)$ and $f(a + b) = f(a) + f(b)$. Furthermore, $a < b$ if and only if $f(a) < f(b)$, and $f(1) = 1$.

Finally, f is one-to-one: suppose $f(a) = 0$. Indeed, if $a > 0$, then there is a rational number in $(0, a)$. And if $a < 0$ there is a rational number in $(a, 0)$. In both cases, $0 \neq f(a)$.

So if $f(a) = f(b)$ then $f(a - b) = 0$, and therefore $a = b$.

This means that we can essentially think of Archimedean ordered fields as subsets of the field $\mathbb{R}$ of real numbers (it does not matter whether we perform computations in F or in its image in $\mathbb{R}$ because we can use f as a "dictionary" to translate between results). For example the result z of the computation $ab + c$ in F is determined by the condition $f(z) = f(a)f(b) + f(c)$.

The upshot is that $\mathbb{R}$ is the only field satisfying

F1 – F9

OF1 – OF2

CF

It then also automatically satisfies AF.

This is technically not quite a correct statement: it is the only field up to (canonical) isomorphism. Every other field is indistinguishable from $\mathbb{R}$ by purely arithmetic properties.

2.2.11 *Excursion: Dedekind cuts

It is worth mentioning a property of the real numbers that historically was very important.

Definition
A **Dedekind[7] cut** of $\mathbb{R}$ denoted $(A \mid B)$ is the following data: $A, B \subset \mathbb{R}$ are nonempty subsets such that

1. $A \cup B = \mathbb{R}$
2. $\forall a \in A, \forall b \in B: a < b$

An element $s \in \mathbb{R}$ is called a **separating number** for $(A \mid B)$ if $a \leq s \leq b$ for all $a \in A$ and all $b \in B$.
EOD.

Note that if $s \in \mathbb{R}$ and $A = \{x \in \mathbb{R} \mid x < s\}$ and $B = \{x \in \mathbb{R} \mid x \geq s\}$, then $(A \mid B)$ is a Dedekind cut with separating number s.

The Completeness Axiom CF is equivalent to the Cut Axiom

DC Every Dedekind cut of $\mathbb{R}$ has one and only one separating number.

Indeed, suppose $(A \mid B)$ is a Dedekind cut. Since B is nonempty, there is $b \in B$ and this is an upper bound for A. Therefore $s := \sup A$ exists by CF. Since *every* element of B is an upper bound for A, and s is the least upperbound, we have $s \leq b$ for all $b \in B$. We then must have $a \leq s \leq b$ for all $a \in A$ and all $b \in B$. Therefore s is a separating number.

Let t be any separating number. Then t is an upper bound for A. If $u < t$ is an upper bound for A, then the interval (u, t) contains at least one element c (e.g. the average). Then $c \in B$ because $c > u$. But $c \in A$ because $c < t$. Therefore u cannot exist, and $t = \sup A$.

[7] Julius Wilhelm Richard Dedekind (1831 – 1916)

Conversely, suppose we know DC holds in $\mathbb{R}$. Then CF becomes provable: indeed, let A be any nonempty subset of A that is bounded above. Let $B = \{x \in \mathbb{R} \mid \forall a \in A: x \geq a\}$. B is not empty because A is bounded above.

Let $C = \mathbb{R} \setminus B$. Then C is not empty. Indeed, A is not empty, so pick $a \in A$. Then $a - 1 \in \{x \in \mathbb{R} \mid x < a\} \subset C$.

Moreover $C \cup B = \mathbb{R}$ by construction. Now let $c \in C$ and $b \in B$. If $c \geq b$, c is an upper bound for A because b is. But then $c \in B$, a contradiction. Therefore $c < b$ must be true for all $c \in C$ and $b \in B$.

We have shown that $(C \mid B)$ is a Dedekind cut. By CD there exists a unique separating number s. If $s \in C$, s is not an upper bound for A. Thus, there is at least one $a \in A$ with $a > s$. But then $a \in B$ and therefore a is an upper bound. Since $a \in A$ this means a is the supremum of A (see Exercise and Example in 2.2.7).

We may therefore assume that s is an upper bound. But then $s = \sup A$, because any $t < s$ is an element of C and therefore not an upper bound of A. Therefore, CF and DC are equivalent.

CF is more practical. This is why we chose it in our characterization of real numbers.

Remark
It is possible to use (a modified) notion of Dedekind cuts to *define* the field $\mathbb{R}$ once the field $\mathbb{Q}$ is defined. For this consider the following definition:
A Dedekind cut of $\mathbb{Q}$ is roughly the same as defined above with the set $\mathbb{R}$ replaced by $\mathbb{Q}$ everywhere: $A, B \subset \mathbb{Q}$ are nonempty subsets such that

1. $A \cup B = \mathbb{Q}$
2. $\forall a \in A, \forall b \in B: a < b$
3. A has no maximum (no upper bound of A is an element of A)

It is again denoted $(A \mid B)$. Then $\mathbb{R}$ is defined as the set of all Dedekind cuts of $\mathbb{Q}$. This may be hard to swallow and is best left for a more advanced class.
But note, it makes sense to identify the rational number r with the Dedekind cut $(A \mid B)$ where

$$A = \{x \in \mathbb{Q} \mid x < r\}$$
$$B = \{x \in \mathbb{Q} \mid x \geq r\}$$

Indeed, its separating number is exactly r. It is possible to define the usual arithmetic on the set of all such Dedekind cuts of $\mathbb{Q}$, and arrive at a complete ordered field, which then necessarily must be essentially $\mathbb{R}$. By the way, probably the simplest thing to define is the order, $(A \mid B) < (C \mid D)$ if $A \subsetneq C$, or equivalently $(A \mid B) > 0$ if A contains a positive rational number (prove this!). We will not go down that road but rather stick to our original plan to treat the real numbers as given. EOR.

2.3 Order and absolute value

In the following let F be an ordered field (but you may think $F = \mathbb{R}$ throughout).

Definition
The **absolute value** $|a|$ of $a \in F$ is defined as

$$|a| := \vdash \begin{cases} a & a \geq 0 \\ -a & a < 0 \end{cases}$$

Note that $a < b$ does not necessarily mean $|a| < |b|$. For instance, $-2 < 1$ but $|-2| = 2 > 1 = |1|$.

In general, $|a| < L$ (where $L \in F$) if and only if $-L < a < L$.

Note if $L \leq 0$ this is always false.

Later, we will often compare absolute values. For example, we will say a and b are "close" to each other, if $|a - b|$ is "small".

So, let $\varepsilon, a, b \in F$, then $|a - b| < \varepsilon$ if and only if $b - \varepsilon < a < b + \varepsilon$.

Indeed, $|a - b| < \varepsilon$ is equivalent to $-\varepsilon < a - b < \varepsilon$. Now add b on all sides.

The absolute value has the following properties that we often use implicitly:

AV1 $|a| \geq 0$ for all $a \in F$; $|a| = 0$ if and only if $a = 0$.
AV2 $|ab| = |a| \cdot |b|$ for all $a, b \in F$.
AV3 $|a + b| \leq |a| + |b|$ for all $a, b \in F$.

The last property is known as the *triangle inequality*. It is the only of these properties that is not completely obvious.

Triangle Inequality
Let $a, b \in F$, then $|a + b| \leq |a| + |b|$. EOL.

Proof. By the above we must show that $-(|a| + |b|) \leq a + b \leq |a| + |b|$. Since $x \leq |x|$ for all $x \in F$ we also have $-|x| \leq x$, and the result follows (using some UFOs). QED.

From AV2 and AV3 one deduces by induction that for all $n \in \mathbb{N}$ and all $a_1, a_2, \ldots, a_n \in F$ we have

$$|a_1 a_2 \cdots a_n| = |a_1||a_2| \cdots |a_n|$$

and

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

If $b \neq 0$ then

$$\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$$

Indeed, $|b^{-1}| = |b|^{-1}$ (either directly from the definition, or from the fact that $1 = |1| = |bb^{-1}|$ and AV2). But then AV2 says

$$\left|\frac{a}{b}\right| = |ab^{-1}| = |a||b^{-1}| = |a||b|^{-1} = \frac{|a|}{|b|}$$

A little more involved is the following statement about subtraction.

Proposition
We always have

$$\big||a| - |b|\big| \leq \min\{|a - b|, |a + b|\}$$

EOP.

Proof. Note that $|a| = |a - b + b| \leq |a - b| + |b|$ and hence $|a| - |b| \leq |a - b|$. Similar reasoning applied to $b = b - a + a$ shows that $|b| - |a| \leq |b - a| = |a - b|$.

Taken together we get $\big||a| - |b|\big| \leq |a - b|$. This holds for all $a, b \in F$. In particular, it applies when b is replaced with $-b$.

Thus, $\big||a| - |b|\big| = \big||a| - |-b|\big| \leq |a - (-b)| = |a + b|$. QED.

The absolute value is often used to define a **distance function**: here the **distance** between a and b in F is defined as $d(a, b) \coloneqq |b - a|$.

2.4 Interlude: some more set theory

We will need some additional concepts from set theory.

2.4.1 Tuples and Cartesian products

Definition

Let X, Y be sets. A **tuple** of elements of X and Y is a pair (x, y) where $x \in X$ and $y \in Y$. The set of all such tuples is denoted by $X \times Y$ and referred to as the Cartesian[8] product of X and Y.
More generally, if $X_1, X_2, \dots, X_n$ are n sets, an ***n*-tuple** with elements from $X_1, X_2, \dots, X_n$ is a an object $(x_1, x_2, \dots, x_n)$ where $x_1 \in X_1, x_2 \in X_2, \dots, x_n \in X_n$. The set of all such n-tuples is denoted by $X_1 \times X_3 \times \dots \times X_n$. EOD.

The existence of the set of tuples follows from the axioms of set theory. It should be noted that

$$(x_1, x_2, \dots, x_n) = (y_1, y_2, \dots, y_n)$$

if and only if $x_1 = y_1$, $x_2 = y_2$,..,$x_n = y_n$.

***Remark**

There are several ways to define $X_1 \times X_2 \times \cdots \times X_n$. All are largely equivalent for our purposes. They always boil down to use a *recursive definition*.
One way would be, assuming Cartesian products of two sets have been defined, and assuming that $X_1 \times X_2 \times \cdots \times X_n$ has been defined, to define $X_1 \times X_2 \times \dots \times X_{n+1}$ as

$$X_1 \times X_2 \times \dots \times X_{n+1} \coloneqq (X_1 \times X_2 \times \dots \times X_n) \times X_{n+1}$$

For us, formally, an n-tuple will be a *function* $f: D_n \to X_1 \cup X_2 \cup \dots \cup X_n$ such that $f(i) \in X_i$. We will discuss functions at great lengths below. EOR.

If $X_1 = X_2 = \cdots = X_n$, then we denote $X_1 \times X_2 \times \dots \times X_n$ often by X^n.

For example,$\mathbb{R}^2 = \{\, (a, b) \mid a, b \in \mathbb{R} \,\}$.

In this case it is important to note that a tuple $(x_1, x_2, \dots, x_n)$ of elements in X is a *different* notion from a set $\{x_1, x_2, \dots, x_n\}$ of elements in X. The former is an ordered sequence, whereas the order of elements for the latter plays no role.

---

[8] René Descartes, latinized as Renatus Cartesius (1596 – 1650) (yes, “cogito ergo sum”, “I think, therefore I am.”)

2.4.2 Power set

The axioms of set theory assert that if S is any set, then so is $\mathcal{P}(S)$, the set of all subsets of S, which is usually referred to as the **power set** of S.

For example, if $S = \{1,2\}$, then $\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

Always remember: an **element** of the power set of a set S is a **subset** of the original set S.

The power set is an important set theoretic tool.

2.5 Proofs by induction and examples

Proofs by induction are an immensely powerful tool. They arise in many ways and contexts.

Often, we want to prove a statement for each natural number n. The problem is, that there are infinitely many natural numbers! We cannot possibly give a proof for each natural number individually. Proofs by induction solve this conundrum: we do not have to prove the statement for each natural number individually, we just have to make sure that the set of natural numbers for which the statement is true is an inductive subset of $\mathbb{N}$ (and then it is equal to $\mathbb{N}$).

Therefore, a proof by induction that a statement $A(n)$ is true for all $n \in \mathbb{N}$ has usually two parts:

A **base case**: Here one has to show that $A(1)$ is true.

An **induction step**: under the assumption that $A(n)$ is true for a given n (the so called **induction hypothesis** or **assumption**), one has to show that $A(n+1)$ is true.

Then the $S = \{n \in \mathbb{N} \mid A(n)\}$ of all natural numbers n for which $A(n)$ is true is inductive, and hence equal to $\mathbb{N}$ because it is also a subset of $\mathbb{N}$.

2.5.1 Recursive definitions

A *recursive definition* is a definition of a mathematical object depending on a natural number n, based on the objects defined for all natural numbers $< n$.

The most basic example is that of a power: When we write a^3 what does that mean? We read it as "multiply a 3times with itself." Again, what does that mean, and what does it mean for arbitrary n "to multiply a n times with itself". A formal recursive definition would be

$$a^1 \coloneqq a$$

and $a^{n+1} = a \cdot a^n$. The Recursive Definition Theorem below asserts that this defines a^n completely.

But note that we had a choice. We could equally well have defined $a^{n+1} = a^n \cdot a$. But by the commutative law of the multiplication, this results in the same.

Example

Let $n \in \mathbb{N}$, the symbol $n!$ (read "n factorial") is defined recursively as:

1. $1! = 1$.
2. $(n+1)! = (n+1)n!$.

In addition, we define $0! = 1$. EOE.

A heuristic and imprecise formulation of the idea is the following:

Suppose we want to define an object A_n for each natural number n.

To do this we show

A_1 is defined; and
If $A_1 A_2, \dots, A_n$ have been defined, then so is A_{n+1}.

By the POI (or complete induction) we then conclude A_n is defined for all natural numbers n.

For all practical purposes this is exactly what we will be doing. But to apply the POI, technically we must have that $\{n \in \mathbb{N} \mid A_n \text{ is defined}\}$ is a set. That depends on the actual definition of A_n, and it is rather tedious to make a general statement.

Suffices to say that any specific rule that can be expressed in usual set theoretic terms to compute A_{n+1} from $A_1, A_2, \dots, A_n$ works. So A_{n+1} must be unambiguously defined by $A_1, A_2, \dots, A_n$.

A formal proof of this idea can be found in *van der Waerden*, Algebra I (unfortunately, this text seems to be available only in German). Below is an excursion that also formalizes the idea.

2.5.2 Some general examples of proofs by induction

Theorem (Cardinality Theorem)
As set S with n elements has 2^n elements. EOT.

For now, we leave aside the rather involved question what the "number of elements" in a set is and adopt the obvious intuitive notion of what that should mean. In set theory the *cardinality* (that is the number of elements in a set) is a well defined concept. Formally, S has n elements if there is a *bijection* $D_n = \{1,2, \dots, n\} \to S$.

Proof. We proceed by induction. The base case here is $n = 0$: the empty set has only one subset, namely the empty set. Now 2^0 is defined as 1, and therefore the base case holds.

Now suppose that for a given integer $n \geq 0$, the assertion is correct, and suppose S is a subset with $n + 1$ elements. In particular there is at least one element, s_0, say, in S. Let S' be the set obtained by removing s_0: $S' = S \setminus \{s_0\}$. Then S' has n elements, and therefore S' has 2^n subsets.

If $T \subseteq S$ is any subset, it falls into one of two categories: $s_0 \in T$ or $s_0 \notin T$.

Let P_1 be the set of subsets of S that do not contain s_0. Any element of P_1 is a subset of S' (and vice versa). Therefore P_1 has exactly 2^n elements.

Let P_2 be the set of subsets that do contain s_0. If $U \in P_1$ then $U \cup \{s_0\} \in P_2$. Conversely, if $V \in P_2$ then $V \setminus \{s_0\} \in P_1$. This defines a one-to-one correspondence between P_1 and P_2, so that P_2 also has 2^n elements.

Taken together, S has $2 \cdot 2^n = 2^{n+1}$ subsets. QED.

We can also use induction to generalize some of the UFOs:

Lemma
Let $n \in \mathbb{N}$. Let $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n \in \mathbb{R}$ such that $x_i < y_i$ for all i. Then,

$$x_1 + x_2 + \cdots + x_n < y_1 + y_2 + \cdots + y_n$$

If in addition all $x_i, y_i > 0$, then

$$x_1 x_2 \cdots x_n < y_1 y_2 \cdots y_n$$

EOL.

Proof. If $n = 1$ there is nothing to show. Suppose for a given n the claims are true, and let $x_1, x_2, \ldots, x_{n+1}, y_1, y_2, \ldots, y_{n+1}$ be numbers with $x_i < y_i$.

Then $x_1 x_2 \cdots x_n < y_1 y_2 \cdots y_n$ (if all $x_i, y_i > 0$) and $x_1 + x_2 + \cdots + x_n < y_1 + y_2 + \cdots + y_n$.

Applying UFO3 (twice!) we get

$$x_1 + x_2 + \cdots + x_n + x_{n+1} < (y_1 + y_2 + \cdots + y_n) + x_{n+1} < (y_1 + y_2 + \cdots + y_n) + y_{n+1}$$

Applying UFO4 (twice!) we find

$$(x_1 x_2 \cdots x_n) x_{n+1} < (y_1 y_2 \cdots y_n) x_{n+1} < (y_1 y_2 \cdots y_n) y_{n+1}$$

QED.

Exercise
Show that the lemma remains true if $<$ everywhere is replaced by $\leq$. EOE.

Lemma (Bernoulli's Inequality)[9]
Let $n \in \mathbb{N}$ and $a \geq -1 \in \mathbb{R}$. Then $(1 + a)^n \geq 1 + na$. EOL.

Proof. Again, this is best done by induction.

Let $n = 1$. Then the assertion is trivial: $(1 + a)^1 \geq 1 + 1 \cdot a$, which is actually an equality.

Now suppose that Bernoulli's Inequality has been shown for a specific $n \in \mathbb{N}$. We now show it also holds for $n + 1$. $(1 + a)^{n+1} = (1 + a)(1 + a)^n \geq (1 + a)(1 + na)$ by the induction assumption (and some UFOs). It is here that we use $a \geq -1$ (why?). But $(1 + a)(1 + na) = 1 + a + na + na^2 = 1 + (n + 1)a + na^2 \geq 1 + (n + 1)a$ because $na^2 \geq 0$. QED.

Exercise
Show that Bernoulli's Inequality is *strict* if $n > 1$ and $a \neq 0$. EOE.

Definition
Let $n, k \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$. We define $0! \coloneqq 1$ and use the definition for $n!$ given above. The **binomial coefficient** $\binom{n}{k}$ (pronounced "n choose k") is defined as 0 if $k > n$ and as

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

if $n \geq k$. EOD.

Remark
Note that $\binom{n}{k}$ is always an element of $\mathbb{N}_0$. This can be shown for example using combinatorics as the binomial coefficient describes the number of subsets with exactly k elements in a set of n elements, so it represents the number of ways to "choose" k elements out of n. Here is a somewhat non very

[9] Jakob Bernoulli (1654 – 1705).

rigorous proof: Let us label the elements of our set by $1,2,\dots,n$. So we want to pick k elements out of $\{1,2,\dots,n\}$. Let us do that in sequence. We pick a first element, a second element, and so on.
For the first element we have n choices. For the second element we then have $n-1$ choices, since we must pick a *different* element from the first. Continuing we see that we have $n(n-1)(n-2)\dots(n-k+1)$ ways of picking a first, second,…, kth element. But many of those choices result in the same subset. For example, if $k=3$, then the ordered choices $2,4,1$ and $1,4,2$ result in the same subset (as subsets are not ordered). There are precisely $k!$ reorderings of our k elements, all resulting in the same subset. Thus the number of subsets is $\frac{n(n-1)\cdots(n-k+1)}{k!}=\frac{n!}{k!(n-k)!}=\binom{n}{k}$. To make this precise one would have to formalize what an orderd "choice" is and use induction on n. EOR.

Fact
The binomial coefficients have the following properties:

1. $\binom{n}{0}=\binom{n}{n}=1$
2. $\binom{n}{1}=\binom{n}{n-1}=n$
3. $\binom{n}{k}=\binom{n}{n-k}$
4. For $k\geq 1$: $\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}$

EOF.

Proof. 1. – 3. are left as exercises. For 4. we observe that if $n\geq k$, then

$$\binom{n}{k}+\binom{n}{k-1}=\frac{n!}{k!\,(n-k)!}+\frac{n!}{(k-1)!\,(n-k+1)!}=\frac{(n-k+1)\cdot n!+k\cdot n!}{k!\,(n-k+1)!}=\frac{(n+1)!}{k!\,\big((n+1)-k\big)!}$$

The right hand side is $\binom{n+1}{k}$. If $n<k$, then all three binomial coefficients in 4. are 0 unless $n=k-1$. In this case, however, the left hand side is $0+1$, and the right hand side is 1. QED.

Lemma (Binomial Theorem)
Let $a,b\in\mathbb{R}$ and $n\in\mathbb{N}$. Then

$$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\binom{n}{2}a^{n-2}b+\cdots+\binom{n}{n-1}ab^{n-1}+b^n$$

EOL.

For any real number x, we define $x^0=1$.

Here we define for every pair of integers $n,k\geq 0$

$$\binom{n}{k}\coloneqq\frac{n!}{k!\,(n-k)!}$$

with the understanding that $0!=1$, and $\binom{n}{k}=0$ if $k>n$. This is called the **binomial coefficient** and pronounced "n choose k".

A more compact notation for the statement of the lemma would be

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

Proof. We proceed by induction on n. For $n=1$ the right hand side is equal to

$\binom{1}{0}a^1b^0 + \binom{1}{1}a^0b = a + b.$

The left hand side is $(a+b)^1$, which is obviously equal.

Induction assumption: Let us assume now that the binomial theorem is true for a given n.

Then $(a+b)^{n+1} = (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$ by the induction assumption.

This is equal to

$$\sum_{k=0}^{n}\binom{n}{k}a^{n-k+1}b^k + \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1}$$

In the right hand sum, the exponents of b run from 1 to $n+1$. So we can rewrite this as

$$\sum_{k=0}^{n}\binom{n}{k}a^{n-k+1}b^k + \sum_{\ell=1}^{n+1}\binom{n}{\ell-1}a^{n-\ell+1}b^{\ell}$$

where we substituted $\ell = k+1$. We may choose to relabel the index k in the first sum also as ℓ and get

$$a^{n+1} + \sum_{\ell=1}^{n}\left(\binom{n}{\ell}a^{n+1-\ell}b^{\ell} + \binom{n}{\ell-1}a^{n+1-\ell}b^{\ell}\right) + b^{n+1}$$

where we separated a^{n+1} and b^{n+1} out so that the sums have the same range of indices.

But then by the 4. Fact about binomial coefficients, this becomes

$$a^{n+1} + \sum_{\ell=1}^{n}\binom{n+1}{\ell}a^{n+1-\ell}b^{\ell} + b^{n+1}$$

Finally, since $\binom{n+1}{0} = \binom{n+1}{n+1} = 1$, we may rewrite this as

$$\sum_{\ell=0}^{n+1}\binom{n+1}{\ell}a^{n+1-\ell}b^{\ell}$$

Therefore the binomial theorem also holds for the case of $n+1$. QED.

Corollary

Let $m < n \in \mathbb{N}$. Then $\left(1+\frac{1}{m}\right)^m < \left(1+\frac{1}{n}\right)^n$.

Proof. First note that for any $2 \le k \le n$ we have $\frac{1}{n^k}\binom{n}{k} > \frac{1}{m^k}\binom{m}{k}$. Note that $\frac{n-i}{n} > \frac{m-i}{m}$ for any $1 \le i \le m$. If $k > m$, this is clear. Suppose $2 \le k \le m$.

$$\frac{1}{n^k}\binom{n}{k} = \frac{1}{n^k}\frac{n!}{(n-k)!\,k!} = \frac{1}{k!}\frac{n(n-1)\cdots(n-k+1)}{n^k} > \frac{1}{k!}\frac{m(m-1)\cdots(m-k+1)}{m^k}$$

because $\frac{n-i}{n} > \frac{m-i}{m}$ for $i = 1,2,\ldots k-1$.

For $k = 0,1$, $\frac{1}{n^k}\binom{n}{k} = \frac{1}{m^k}\binom{n}{k} = 1$. By the Binomial Theorem,

$$\left(1+\frac{1}{m}\right)^m = \sum_{k=0}^{m}\binom{m}{k}\frac{1}{m^k} \leq \sum_{k=0}^{m}\binom{n}{k}\frac{1}{n^k} < \sum_{k=0}^{n}\binom{n}{k}\frac{1}{n^k} = \left(1+\frac{1}{n}\right)^n$$

by the above. QED.

2.6 Elementary properties of real numbers

Now we focus on the set of real numbers.

2.6.1 Some additional notations

We have seen that as $\mathbb{R}$ is Archimedean, the rational numbers sit *dense*, that is, every interval (a, b) with $a < b$ contains a rational number.

It follows that for every $\varepsilon > 0$, and any $a \in \mathbb{R}$ there is $r \in F$ such that $|r - a| < \varepsilon$. Indeed, there is some $r \in \mathbb{Q} \cap (a - \varepsilon, a + \varepsilon)$. In that sense every element of F can be "approximated" by rational numbers. And since we can choose ε "small" (e.g. $\varepsilon = \frac{1}{n}$ for "large" $n \in \mathbb{N}$), this is often useful.

If $S \subseteq \mathbb{R}$ is nonempty and bounded above, then it has a unique supremum. If it is unbounded above, we write $\sup S = \infty$ (or $+\infty$). Note that ∞ is not a number but merely a symbol expressing the fact that there is no real number that is greater than all elements of S.

Similarly, if S is not bounded below, we write $\inf S = -\infty$.

We occasionally say that the supremum (resp. infimum) is an **improper** supremum (resp. infimum) if it is equal to ∞ (resp. $-\infty$), and then call the "finite" version the **proper** supremum (resp. infimum).

.It is sometimes convenient to write $\overline{\mathbb{R}} \coloneqq \mathbb{R} \cup \{\pm\infty\}$, the set of real numbers together with two arbitrarily chosen elements. We then write $\infty > x$ for all $x \in \mathbb{R} \cup \{-\infty\}$ and $-\infty < x$ for all $x \in \mathbb{R} \cup \{\infty\}$. We also adopt the convention that $\infty + x = \infty$ and $-\infty + x = -\infty$ for all $x \in \mathbb{R}$. Likewise, $\infty \cdot x = \infty$ and $-\infty \cdot x = -\infty$ if $x > 0$ is a real number (and $\infty \cdot x = -\infty$ and $(-\infty) \cdot x = \infty$ if $x < 0$). Finally, $\infty \cdot (\pm\infty) = \pm\infty$ and $(-\infty) \cdot (-\infty) = \infty$.

Note we do not give any meaning to $0 \cdot (\pm\infty)$, nor do we define $\infty + (-\infty)$. And it has to be re-iterated that this is purely symbolic and does not assume any special meaning of "infinity".

2.6.2 Roots

We have already seen that any positive real number has a square root. In fact we are ready to look at solutions of more general equations such as $x^n - a = 0$ where $a \geq 0$.

Theorem (nth roots exist)
Let $a \geq 0$, and $n \in \mathbb{R}$. Then there is a unique real number $r \geq 0$ such that $r^n = a$. EOT.

Proof. We use the ideas discussed when we showed that every positive real number has a square root.

Let $S = \{x \in \mathbb{R} \mid x^n < a\}$. Then S is nonempty: it contains 0. It is also bounded above: $1 + a$ is an upper bound. Indeed, by Bernoulli's Inequality $(1 + a)^n \geq 1 + na \geq a$.

It then follows that S has a (proper) supremum $r \geq 0$. We will show that $r^n = a$. We will do this by showing that the assumptions $r^n < a$ and $r^n > a$ yield contradictions.

Suppose $r^n < a$. Then also $(r+\varepsilon)^n < a$ for some $\varepsilon > 0$. But that means $r + \varepsilon > r \in S$, a contradiction. To see this note that by the Binomial Theorem,

$$(r+\varepsilon)^n = \sum_{k=0}^{n} \binom{n}{k} r^{n-k} \varepsilon^k$$

For sufficiently small $\varepsilon > 0$, it is clear that

$$\sum_{k=1}^{n} \binom{n}{k} r^{n-k} \varepsilon^k = \varepsilon \sum_{k=1}^{n} \binom{n}{k} r^{n-k} \varepsilon^{k-1} < a - r^n$$

Indeed, let $\varepsilon = \frac{1}{m}$ for $m \in \mathbb{N}$, then

$$\sum_{k=1}^{n} \binom{n}{k} r^{n-k} \varepsilon^{k-1} = \sum_{k=1}^{n} \binom{n}{k} r^{n-k} \left(\frac{1}{m}\right)^{k-1} \leq \sum_{k=1}^{n} \binom{n}{k} r^{n-k} =: A$$

For m large enough $\frac{A}{m}$ is smaller than $a - r^n$.

Now suppose $r^n > a$. Again we find that for $\varepsilon = \frac{1}{m}$ with $m \in \mathbb{N}$ large enough we have

$$(r-\varepsilon)^n = \sum_{k=0}^{n} \binom{n}{k} r^k (-1)^k \varepsilon^k = r^n + \varepsilon \sum_{k=1}^{n} \binom{n}{k} r^k (-1)^k \varepsilon^{k-1} > a$$

With $B \coloneqq \sum_{k=1}^{n} \binom{n}{k} r^k (-1)^k \varepsilon^{k-1}$, we have $|B| \leq \sum_{k=1}^{n} \binom{n}{k} r^k =: C$ (triangle inequality; and $\frac{1}{m} < 1$), and hence $\frac{|B|}{m} \leq \frac{C}{m} < r^n - a$ if m is large enough. We may assume that $r - \varepsilon > 0$ by increasing m further if necessary. But then $r - \varepsilon < r$ is another upper bound of S, a contradiction.

The upshot is that $r^n = a$.

To show that r is unique, suppose $s \geq 0$ also satisfies $s^n = a$. QED.

Remark
We have found *one* solution of the equation $x^n = a$ (if $a \geq n$). This is not the same as *solving* the equation $x^n = a$, which usually refers to finding *all* solutions of the equations.
But here, we are close: we have actually shown that r (as constructed in the proof) is the *only* nonnegative solution. It turns out that if n is even and $a > 0$, there exists exactly one other (real) solution, namely $-r$. EOR.

Exercise
Show that if $a > 0$ and n is even there are exactly two solutions of $x^n = a$, one of them (r, say), positive. Show that that the other solution must be $-r$.
Show that if $a < 0$ and n is even, then $x^n - a = 0$ has no real solution.

Show that if $a < 0$ and n is odd, then $x^n - a = 0$ has precisely one solution, and the solution is negative EOE.

2.6.3 Rational powers

Let a be a **positive** real number, and r be a rational number. We want to define a^r.

If $r = n \in \mathbb{N}$, then a^n is as we have seen defined recursively by

1. $a^1 = a$
2. $a^{n+1} = a \cdot a^n$

If $r = -n$, we put $a^r := \frac{1}{a^n}$. Together with $a^0 = 1$ we obtain a definition of a^r for all $r \in \mathbb{Z}$.

One then shows that for any $r, s \in \mathbb{Z}$, one has $a^{r+s} = a^r a^s$ and $(a^r)^s = a^{rs}$.

Finally, let $r = \frac{p}{q}$ with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. Then

$$a^r = a^{\frac{p}{q}} = \sqrt[q]{a^p}$$

Remark

1. $a^r = \sqrt[q]{a^p} = \left(\sqrt[q]{a}\right)^p$. Indeed, both numbers on the right are (positive) solutions of the equation $x^q = a^p$, and therefore must be equal.
2. The value of a^r does not depend on the choice of representation of r as $\frac{p}{q}$.
3. For all $r, s \in \mathbb{Q}$, we have $a^{r+s} = a^r a^s$ and $(a^r)^s = a^{rs}$.

EOR.

Exercise

Prove 2. And 3.

In addition, show that for all $r, s \in \mathbb{Q}$ and all $a, b > 0$:

$\frac{a^r}{a^s} = a^{r-s}$, $a^r b^r = (ab)^r$, $\frac{a^r}{b^r} = \left(\frac{a}{b}\right)^r$. EOE.

2.6.4 Arithmetic mean

The **arithmetic mean** (or **average**) of two elements a, b in F is defined as

$$\frac{a+b}{2}$$

We always have

$$\min\{a, b\} \leq \frac{a+b}{2} \leq \max\{a, b\}$$

The arithmetic mean is a special case of the **weighted arithmetic mean** defined as follows:

Let $w_1, w_2, \dots, w_n > 0$ and $a_1, a_2, \dots, a_n \in \mathbb{R}$. Then the weighted arithmetic mean is defined as

$$\frac{w_1 a_1 + w_2 a_2 + \cdots + w_n a_n}{w_1 + w_2 + \cdots + w_n}$$

The usual arithmetic mean corresponds to the case $w_i = \frac{1}{n}$ for all n.

We have the following inequality:

$$\min\{a_1, a_2, \dots, a_n\} \leq \frac{w_1 a_1 + w_2 a_2 + \cdots + w_n a_n}{w_1 + w_2 + \cdots + w_n} \leq \max\{a_1, a_2, \dots, a_n\}$$

Indeed, WLOG we may assume that $a_1 \leq a_2 \leq \cdots \leq a_n$. Let $W = w_1 + w_2 + \cdots + w_n$. Then

$$a_1 = \frac{1}{W}(w_1 a_1 + w_1 a_1 + \cdots + w_n a_1) \leq \frac{1}{W}(w_1 a_1 + w_1 a_2 + \cdots + w_n a_n)$$

$$\leq \frac{1}{W}(w_1 a_n + w_2 a_n + \cdots + w_n a_n) = a_n$$

QED.

2.6.5 The geometric mean

The **geometric mean** of two real numbers $a, b \geq 0$ is defined as $\sqrt{ab}$.

More generally, the geometric mean of numbers $a_1, a_2, \dots, a_n \geq 0$ is defined as

$$\sqrt[n]{a_1 a_2 \cdots a_n}$$

Note we always have

$$\sqrt{ab} \leq \frac{a+b}{2}$$

that is, the geometric mean is always less than or equal to the arithmetic mean.

Proof. By UFO9 it is enough to show that $ab \leq \frac{(a+b)^2}{4} = \frac{1}{4}(a^2 + 2ab + b^2)$, or equivalently that

$$\frac{1}{4}(a^2 - 2ab + b^2) = \frac{1}{4}(a-b)^2 \geq 0$$

But this is a square so always nonnegative. QED.

This inequality generalizes to

$$\sqrt[n]{a_1 a_2 \cdots a_n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n}$$

We leave the proof (which can be done by induction) as an exercise.

2.6.6 *The cardinality of $\mathbb{R}$

The *cardinality* of a set refers to its "size." This can be made precise using ordinals, but we will not go into that. We say two sets S, T have the same cardinality if there is a bijection $f: S \to T$. A **bijection** is a one-to-one correspondence. What we mean by that is, we can relabel the elements of T using the elements of S so that every element of T gets a unique label, and every element of S is used as a label.

The sets $\{1,2,3\}$ and $\{4, -2, 11\}$ have the same cardinality, because we can label 4 by 1, -2 by 2, and 11 by 3.

$\{1,2,3\}$ and $\{4,-2\}$ do not have the same cardinality because no matter how we label the elements in $\{4,-2\}$, we will only use two elements of $\{1,2,3\}$ as labels. If we turn it around, and try to label the elements of $\{1,2,3\}$ with those of $\{4,-2\}$ we must use one label twice.

Definition
A set S is called **finite**, if it is empty or has the same cardinality as $\{1,2,\dots,n\}$ for some natural number n.
A set that is not finite is called **infinite**.
S is called **countably infinite** (or **countable** for short), if it has the same cardinality as $\mathbb{N}$.
S is called **uncountably infinite** if it is infinite but not countable. EOD.

Example
Both $\mathbb{Z}$ and $\mathbb{Q}$ are countably infinite. EOE.

Theorem
$\mathbb{R}$ is uncountably infinite. EOT.

The proof as given here uses the notion of *decimal expansion*, which we have not discussed yet, and which is impossible to do without a firm grasp on *limits*. However, you have seen decimal expansions in school and use them everyday, so we will assume familiarity with them. We will discuss the details later on.

Proof. The argument given here is usually referred to as *Cantor's diagonal argument*. It goes as follows: suppose the real numbers form a countably infinite set (it is clear that $\mathbb{R}$ is infinite, as it contains $\mathbb{N}$). Then any subset of $\mathbb{R}$ is finite or countably infinite.

In particular, this must apply to the interval $[0,1)$. Suppose we can label every number in $[0,1)$ by a natural number (we can "count" them).Then we can write down an infinite list $x_1, x_2, \dots, x_n, \dots$ of the all the numbers in $(0,1)$. Each number x_i has a *decimal expansion*[10]. Let x_{ik} denote the kth decimal place of x_i (if $x_4 = .78932\dots$, say, then $x_{42} = 8$). As all numbers are in $(0,1)$ we do not need to keep track of the places before the decimal point.

Now let us write down the numbers in $[0,1)$ in a table: in the ith row we list the digits of x_i. Of course, this table will have infinitely many rows and columns.

We define a real number y as follows: its kth decimal place is given by

$$y_k = \vdash \begin{cases} 0 & x_{kk} \neq 0 \\ 1 & x_{kk} = 0 \end{cases}$$

Such a decimal expansion corresponds to a unique real number $y \in [0,1)$. We therefore must have $y = x_n$ for some (unique) n. After all, y must appear in our list!

But for each n, y and x_n differ in at least the nth decimal place: $y_n \neq x_{nn}$ by construction. Therefore y cannot appear on our list, and we have a contradiction. QED.

Remark
This result is interesting. We observed that in $\mathbb{Q}$ we cannot solve the equation $x^2 - 2 = 0$. So we "threw in" a solution and called it $\sqrt{2}$. Even if we do that with *all* polynomial equations that have no solution in

[10] We will discuss these later, but for now we assume you are familiar with that fact.

$\mathbb{Q}$ but have a solution in $\mathbb{R}$, we would still end up with a countable set (the so called *field of real algebraic numbers*). Therefore $\mathbb{R}$ must contain elements that are not easily describable as the solution of a specific equation, and in fact the vast "majority" of them must be.
It came as a shock to many mathematicians (and philosophers and theologists) that there are different "kinds" of infinity. In fact, a similar argument applied to ordinals shows that there is no "largest" infinity. There are infinitely many cardinalities of infinite sets!
While there is no largest cardinality, one might ask is there anything "between" countable and uncountably infinite? This is known as the *Continuum Hypothesis*: it states that there should be no set "smaller" than $\mathbb{R}$ and "larger" than $\mathbb{N}$. Only in 1940 Goedel showed that the continuum hypothesis cannot be disproved from the axioms of set theory (ZFC). Later Cohen[11] showed that the continuum hypothesis also cannot be proved using only these axioms. This shows that the continuum hypothesis is independent from ZFC set theory (meaning it cannot be proved or disproved using only these axioms).

2.7 Functions

Ultimately, calculus is the theory of functions on the real line, that is, quantities that "depend" on a real number. How can we formalize this idea?

2.7.1 The definition of a function

Definition 1
Let X, Y be sets. A **function** $f: X \to Y$ is a **rule** that associates to each $x \in X$ one and only one element $y = f(x)$ of Y.
The set X is called the **domain** of f, and Y is called the **codomain**. The **range** or image of f is the set $f(X)$ of all values of f, ie. $f(X) = \{ y \in Y \mid y = f(x) \text{ for some } x \in X \} = \{f(x) \mid x \in X\}$.
Two functions $f: X \to Y$ and $g: Z \to W$ are equal if $X = Z$ and $Y = W$ and in addition $f(x) = g(x)$ for all $x \in X$. EOD.

Remark
For two functions to be equal we require that their domains and codomains coincide. While the first is always necessary, we sometimes treat two functions as equal if their domains and values are equal. Consider the following example: Let $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$, $g: \mathbb{R} \to \mathbb{R}_{\geq 0}$, defined by $g(x) = x^2$, and finally $h: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ also defined by $h(x) = x^2$.
It is often useful to treat f and g as equal. This causes no problems as long as we don't discuss invertibility (see below). However, neither f nor g are equal to h. In fact, strictly speaking h is the **restriction** of g to $\mathbb{R}_{\geq 0}$. EOR.

Examples

1. If X is any set, the **identity map** is the function $f: X \to X$ defined by $f(x) = x$.
2. If X, Y are sets and $y \in Y$ is a fixed element, there is a **constant** function $f: X \to Y$ that assigns to each x the value $f(x) = y$.
3. Now let $X = Y = \mathbb{R}$. Then for any $n \in \mathbb{N}$, and $c \in \mathbb{R}$ we obtain a function $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = cx^n$. Such a function is called a **monomial function**.
4. Generalizing the previous example, given numbers $c_0, c_1, \dots, c_n$ we can define a **polynomial function** $f: \mathbb{R} \to \mathbb{R}$ by $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$.

[11] Paul J. Cohen (1934 – 2007)

5. Not every function is given by an arithmetic rule: the *Dirichlet[12]-function* $\chi_{\mathbb{Q}}: \mathbb{R} \to \mathbb{R}$ is the *characteristic function* of $\mathbb{Q}$ defined as
$$\chi_{\mathbb{Q}} = \begin{cases} 1 & \text{if } x \in \mathbb{Q} \\ 0 & \text{if } x \notin \mathbb{Q} \end{cases}$$
This is an example of a function that exists, but is impossible to compute at a specific x in general, because for most x we don't know whether they are rational or not (depending on how x is given).

EOE.

In large parts of mathematics, all objects are sets. We should define a function as a certain set, which would solve all our problems.

Definition 2
Let X, Y be sets. A **function** $f: X \to Y$ is a subset $\Gamma \subseteq X \times Y = \{(x, y) \mid x \in X, y \in Y\}$ with the following properties:

1. $\forall x \in X: \exists y \in Y: (x, y) \in \Gamma$
2. $\forall x \in X: (x, y), (x, y') \in \Gamma \Rightarrow y = y'$

If f is such a function denote $y \in Y$ such that $(x, y) \in \Gamma$ by $f(x)$ and call it the **value** of f at x. The set Γ is also called the **graph** of f. EOD.

Strictly speaking we should incorporate X, Y into the definition. While X can be recovered from Γ, Y cannot in general. So technically f is a triple (X, Y, Γ).

Here, we avoid any talk of "rules" or "formulas". The only condition is that Γ has to be a set.

Example

1. The identity map $f: X \to X$ corresponds to $\Gamma = \{(x, x) \mid x \in X\}$, so the so-called *diagonal* in $X \times X$.
2. A function $f: \mathbb{R} \to \mathbb{R}$ corresponds to a set $\Gamma \subseteq \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, the Euclidean plane. Drawing it using an x- and y-axis, the possible functions correspond exactly to those subsets which have no "duplicates" over any point on the x-axis. For example, any line which is *not* vertical corresponds to a function.
3. The Dirichlet function $\chi_{\mathbb{Q}}$ defined above corresponds to the set $\Gamma = \mathbb{Q} \times \{0\} \cup (\mathbb{R} \setminus \mathbb{Q}) \times \{1\}$.

2.7.2 Injective and surjective functions

Definiton
A function $f: X \to Y$ is called **injective** (or **one-one**) if for all $x, y \in X : f(x) = f(y)$ only if $x = y$.
f is called **surjective** (or **onto**) if $f(X) = Y$, or in other words, for each $y \in Y$ there is $x \in X$ such that $f(x) = y$.
f is called **bijective** (also a **one-to-one correspondence**) if it is both injective and surjective. EOD.

These notions may take some time to get used to.

Example

1. $f: X \to X$, $f = \mathrm{id}_X$. Then f is bijective. Indeed, if $x \in X$, then $f(x) = x$, so f is surjective. If $f(x) = f(y)$, then $f(x) = x = y = f(y)$.

[12] Johann Peter Gustav Lejeune Dirichlet (1805 – 1859)

2. $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ is neither surjective nor injective: for example, there is no $x \in \mathbb{R}$ such that $f(x) = x^2 = -1$; so f is not surjective. Also $f(1) = f(-1)$ but $1 \neq -1$, so f is not injective either.
3. For any function $f: X \to Y$, we may modify the co-domain to be equal to the range $f(X) \subset Y$. Let us call the modified function by $\bar{f} : X \to f(X)$. Then $\bar{f}$ is surjective. Often, we do not distinguish between f and $\bar{f}$ even though we should.