I. Number Systems

A. The Natural Numbers, $\mathbb{N}$.

Mathematics has to start somewhere.

We will begin by assuming that we understand basic set theory, and by carefully describing the natural numbers.

Larger goal: We want to describe all of our familiar number systems:

$\mathbb{Z}$ = integers

$\mathbb{Q}$ = rationals

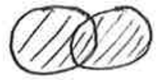
$\mathbb{R}$ = reals, and

$\mathbb{C}$ = complex numbers

in terms of $\mathbb{N}$. That is, we'll construct these systems from something well understood.

Basic set theory: A set is a collection of mathematical objects.

We can form unions $A \cup B$



and intersections $A \cap B$

We can ask whether an object is a member of a set (whether $x \in A$)

and form subsets of a known set ($A \subseteq B$)

or ordered pairs of elements from existing sets.

We describe $\mathbb{N}$ with the following axioms ("rules"):

Peano axioms for $\mathbb{N}$

1. There is an element $0 \in \mathbb{N}$.
2. There is a function $\sigma : \mathbb{N} \longrightarrow \mathbb{N} \setminus \{0\}$, called the successor function.
3. If $n, m \in \mathbb{N}$ satisfy $\sigma(n) = \sigma(m)$, then $n = m$.
   [That is, σ is injective or one-to-one.]
4. If S is a subset of $\mathbb{N}$ such that
   a) $0 \in S$, and b) whenever $n \in S$, also $\sigma(n) \in S$
   then $S = \mathbb{N}$. (the induction axiom)

Notation: With the Peano axioms, we have

$$\mathbb{N} = \{0, \sigma(0), \sigma(\sigma(0)), \sigma(\sigma(\sigma(0))), \ldots\}$$

but we'll usually write 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, and so forth. With this notation, we can write

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

Let's look at these Axioms more carefully. Axiom (1) is self-explanatory. Axioms (2) and (3) say that every element of $\mathbb{N}$ has a unique successor, and that every element except for 0 has a unique predecessor (or preimage of σ).

Axiom (4) may require more thought. Consider the following:

Anti-example: $\{2, 3, 4, \ldots\}$ fails to contain 0 (and is $\neq \mathbb{N}$)

Antiexample: $S = \{0, 1, 2, 3, 5, 6, 7, \ldots\}$ has $3 \in S$ but fails to have $\sigma(3) = 4$ in S. (and $S \neq \mathbb{N}$).

The crucial property of $\mathbb{N}$ is a consequence of Axiom (4) and gives a powerful method to prove statements involving $\mathbb{N}$.

<u>Theorem</u>: (Principle of Mathematical Induction)

Let $P_0, P_1, P_2, P_3, \ldots$ be a list of statements which may be true or false.

Suppose that i) P_0 is true, and

Write $P_n \Rightarrow P_{n+1}$ ii) Whenever P_n is true, also P_{n+1} is true.

Then all of the statements $P_0, P_1, P_2, P_3, \ldots$ are true.

<u>Proof</u>: (From Axiom (4))

Let $S := \{ n : P_n \text{ is true} \}$ be the set of all n such that P_n is true.

Then $S \subseteq \mathbb{N}$ (since we numbered the statements w/ $\mathbb{N}$)

and (i) says that $0 \in S$, while

(ii) says that whenever $n \in S$, also $n+1 \in S$.

Now Peano's Axiom (4) says that $S = \mathbb{N}$.

So all the statements are true, as was to be proved. ∎

Mathematical induction is a useful proof technique!

To demonstrate, let's assume for a moment that we know how to do arithmetic in $\mathbb{N}$. (We'll return to arithmetic later.)

<u>Example 1</u>: Show that $1+2+3+\ldots+n = \frac{n \cdot (n+1)}{2}$ for all positive natural numbers n.

<u>Solution</u>: (Expanded version, for 1st time induct-ors)

First, we identify our list of statements. P_n is the statement "$1+2+3+\ldots+n = \frac{n\cdot(n+1)}{2}$, or $n=0$."

So P_1 means "$1 = \frac{1\cdot 2}{2}$", P_2 means "$1+2 = \frac{2\cdot 3}{2}$", and so forth.

Notice that P_1 is obviously true, and P_0 is immediate.

These (P_0 and P_1) form the <u>base case</u> for our induction

(The base case corresponds to (i), and in this case "$P_0 \Rightarrow P_1$" in the Principle of Mathematical Induction)

Now we show that $P_n \Rightarrow P_{n+1}$ for $n \geq 1$: (the inductive step, (ii) in PoMI).

Inductive step $P_n \Rightarrow P_{n+1}$

If P_n is true, then

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

Now add $n+1$ to both sides of the equation:

$$\begin{aligned} 1+2+\dots+n+(n+1) &= \frac{n\cdot(n+1)}{2} + (n+1) \\ &= \left(\frac{n}{2}+1\right)\cdot(n+1) \\ &= \frac{(n+2)\cdot(n+1)}{2} \end{aligned}$$

and we conclude that P_{n+1} is also true.

By the Principle of Mathematical Induction, P_n is true for all n. ∎

There are three important parts in the above solution to Example 1:

We say how we're using induction, (easy)

prove a base case, (PoMI (i)) (easy)

and show an inductive step (PoMI (ii)) (less easy).

After a little more experience, you'll write the same solution more shortly:

<u>Solution to Example 1:</u> (Short version, for experts)

We proceed by induction on n.

<u>Base case:</u> <u>$n=1$</u>: $1 = \frac{1\cdot(1+1)}{2}$ holds. ✓

<u>Inductive step:</u> <u>$P_n \Rightarrow P_{n+1}$</u>:

Since (by inductive assumption of P_n)

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

also

$$\begin{aligned} 1+2+\dots+n+(n+1) &= \frac{n\cdot(n+1)}{2} + (n+1) \\ &= \left(\frac{n}{2}+1\right)(n+1) = \frac{(n+2)}{2}\cdot(n+1) \end{aligned}$$ ✓ ∎

Example 2: Show that $5^n - 4n - 1$ is a natural number multiple of 16 for any $n \in \mathbb{N}$.

Solution: (Short form only)

We proceed by induction on n.

Base case: $n=0$: $\quad 5^0 - 4\cdot 0 - 1 = 1 - 0 - 1 = 0 = 0\cdot 16$ ✓

Inductive step:

We can assume by induction that, for some $k \in \mathbb{N}$,

$$5^n - 4n - 1 = 16\cdot k \qquad (\text{"}P_n\text{"})$$

Then we break down the "P_{n+1}" into something related to "P_n":

$$\begin{aligned} 5^{n+1} - 4(n+1) - 1 &= 5\cdot 5^n - 4n - 4 - 1 \\ &= 5\cdot(5^n - 4n - 1) + 16n \\ &= 5\cdot 16\cdot k + 16n \\ &= 16\cdot(5k+n) \end{aligned}$$

and since $k, n \in \mathbb{N}$, also $5k+n \in \mathbb{N}$. ✓ ∎

Ordering $\mathbb{N}$:

Two elements of $\mathbb{N}$ are equal if they are obtained from 0 by the same number of applications of σ (that is, if they are identical).

Write $n = m$ if n and m are equal.

Also, write $n < m$ if m is some successor of n and $n \leq m$ if $n < m$ or $n = m$.

Eg: $2 < 4$, since $4 = \sigma(\sigma(\sigma(\sigma(0))))$
and $2 = \sigma(\sigma(0))$
so that $4 = \sigma(\sigma(2))$.

The relation $\leq$ on $\mathbb{N}$ is an example of a "partial order" and moreover of a "linear order", as some of you will see in DM-I. There are many examples of linear orders.

An unusual property of $\leq$ on $\mathbb{N}$ is the following:

<u>Theorem</u>: Every nonempty subset of $\mathbb{N}$ has a least element wrt $\leq$.

<u>Remark</u>: A linear order with the above property — that every nonempty subset has a least element — is called a <u>well-ordering</u>. So this theorem could be stated as "$\mathbb{N}$ is well-ordered by $\leq$."

<u>Proof (of Theorem)</u> Suppose that $A \subseteq \mathbb{N}$ is a subset having no least element. We'll show that A is empty.

Define $B = \mathbb{N} \setminus A$. Showing A empty is the same as showing $B = \mathbb{N}$.

Now we notice:

i) $0 \in B$, as 0 would certainly be least in A.

ii) If $0, 1, 2, \ldots, n \in B$, then also $n+1 \in B$ (as otherwise $n+1$ would be least in A.)

By the Principle of Mathematical Induction, we see $B = \mathbb{N}$, so $A = \emptyset$. ∎

<u>Arithmetic in $\mathbb{N}$:</u>

<u>Definitions</u>: $+$: For $n, m \in \mathbb{N}$, define $n+m := \underbrace{\sigma(\sigma(\cdots\sigma}_{m \text{ times}}(n)\cdots))$

$\cdot$: For $n, m \in \mathbb{N}$, define

$$n \cdot m := \underbrace{n+n+\cdots+n}_{m \text{ times}}$$

Similarly, define exponentiation via $n^m := \underbrace{n \cdot n \cdot \cdots \cdot n}_{m \text{ times}}$.

<u>Properties of Arithmetic on $\mathbb{N}$:</u> For $n, m, \ell \in \mathbb{N}$

i) $n+m \in \mathbb{N}$, $n \cdot m \in \mathbb{N}$ (closure)

ii) $n+m = m+n$, $n \cdot m = m \cdot n$ (commutativity)

iii) $(n+m)+\ell = n+(m+\ell)$, $(n \cdot m) \cdot \ell = n \cdot (m \cdot \ell)$ (associativity)

iv) $n+0 = 0+n = n$, and (additive identity)
$n \cdot 1 = 1 \cdot n = n$ (multiplicative identity)

v) $n \cdot (m+\ell) = nm + n\ell$ (distributivity)

The $+$ operation gives a nice alternative way to write σ,
as $n+1 = \sigma(n)$.

The operations $+$ and $\cdot$ have <u>limited inverses</u> in $\mathbb{N}$,
which we write with $-$ and $\div$.
An <u>inverse</u> of $+$ is an operation that "undoes" $+$,
and <u>limited</u> means that sometimes the inverse operation
is well-defined (e.g. $5-2$)
while sometimes it is not (e.g. $2-5$).
Define $n-m$ to be the mth predecessor of n if $m \leq n$
(otherwise, leave it to be undefined).
<u>Eg:</u> $5-2=3$, since $\sigma(\sigma(3)) = 3+2 = 5$.

Similarly, define n/m to be the value x s.t. $x \cdot m = n$
if a <u>unique</u> such $x \in \mathbb{N}$ exists.
(and otherwise leave it undefined).
Alternative notation $n \div m$. (Less Common).
<u>Eg:</u> $6/3 = 2$, but $5/3$ and $6/0$ are undefined here.

Our next step will be to <u>complete</u> $\mathbb{N}$ to its closure under $-$.
That is, we'll extend $\mathbb{N}$ to a larger number system
so that $-$ is always defined.

(Later, we'll do a similar completion with respect to $\div$.)

B. The Integers, $\mathbb{Z}$

We noticed that $\mathbb{N}$ is closed under $+$ and $\cdot$
(i.e., that $n+m \in \mathbb{N}$ and $n \cdot m \in \mathbb{N}$ whenever $n, m \in \mathbb{N}$)
but not under $-$. (E.g., $2-5$ is undefined over $\mathbb{N}$.)
The smallest set containing $\mathbb{N}$ and closed under $-$ is
that of the integers $\mathbb{Z}$.

We construct $\mathbb{Z}$ from $\mathbb{N}$ by the "Method of Ordered Pairs".
We consider the set of all ordered pairs of natural numbers
(n, m). ($\leftarrow$ think of as "$n-m$")
and identify all pairs of $n, m \in \mathbb{N}$ of the form
$(n+k, n)$ for a fixed $k \in \mathbb{N}$, or
$(n, n+k)$ - - - - - - .

E.g.: $(2,0) = (3,1) = (4,2) = \dots$ will be the object we call 2
and $(0,2) = (1,3) = (2,4) = \dots$ will be the object we call -2.

More generally, for $n, k \in \mathbb{N}$, we have the correspondences
1) $(n+k, n) \longleftrightarrow k$ (embedding $\mathbb{N}$ in $\mathbb{Z}$)
2) $(n, n+k) \longleftrightarrow -k$.

We order $\mathbb{Z}$ by

$$(n_1, m_1) < (n_2, m_2) \text{ when } n_1 + m_2 \overset{\text{in } \mathbb{N}}{<} n_2 + m_1$$

(You should convince yourself that this yields the usual order on $\mathbb{Z}$.)
As usual, $x \leq y$ means "$x < y$ or $x = y$".

Remark: The identification of many ordered pairs to a common element of $\mathbb{Z}$ is an example of "quotienting by an equivalence relation", which is a framework for checking that the identification makes sense!

Notice that $\leq$ on $\mathbb{Z}$ is <u>not</u> a well-ordering.
E.g., $\mathbb{Z}$ itself has no least element.

<u>Arithmetic in $\mathbb{Z}$:</u>

<u>Definition:</u> For $x_1 = (n_1, m_1)$ and $x_2 = (n_2, m_2) \in \mathbb{Z}$,
define $x_1 + x_2 = (n_1, m_1) + (n_2, m_2) := (n_1 + n_2, m_1 + m_2)$
(entry-wise)
and $x_1 \cdot x_2 = (n_1, m_1) \cdot (n_2, m_2) := (n_1 n_2 + m_1 m_2, n_1 m_2 + n_2 m_1)$

Remember that we identify $n \in \mathbb{N}$ with $(n, 0) \in \mathbb{Z}$
and notice that arithmetic in $\mathbb{N}$ is compatible with that in $\mathbb{Z}$:

$$(n, 0) + (m, 0) = (n+m, 0)$$
$$(n, 0) \cdot (m, 0) = (n \cdot m + 0, 0 + 0).$$

The following properties now follow from the Arithmetic Prop for $\mathbb{N}$. (<u>Exercise:</u> Check these!)

<u>Properties of $\langle \mathbb{Z}, +, \cdot \rangle$:</u>

i) $\mathbb{Z}$ is closed under $+, \cdot$ (and $-$).
ii) $+$ and $\cdot$ are commutative (but $-$ is not commutative).
iii) $+$ and $\cdot$ are associative.
iv) there is a multiplicative identity 1 and an additive identity $0 \neq 1$.
v) For every $n \in \mathbb{Z}$, there is some $n^* \in \mathbb{Z}$ so that $n + n^* = n^* + n = 0 \in \mathbb{Z}$ (additive inverses)
vi) $\mathbb{Z}$ is distributive.

(See p7 for meanings of commutative, associative, identity, distributive.)

Sets with operations satisfying similar properties are common in mathematics, and we pause to introduce a name:

A set G with a binary operation $\oplus$ is a <u>group</u> if

i) G is closed under $\oplus$

ii) $\oplus$ is associative

iii) G has an identity 0 for $\oplus$
(so, for any $g \in G$, we get $0 \oplus g = g \oplus 0 = g$.)

iv) Every $g \in G$ has an inverse $g^* \in G$ under $\oplus$
(so, $g \oplus g^* = g^* \oplus g = 0$).

Thus, $\langle \mathbb{Z}, + \rangle$ is a group.
But notice that $\langle \mathbb{Z}, \cdot \rangle$ is <u>not</u> a group. Why not?

<u>Summary</u>: We have just embedded $\mathbb{N}$ in a larger structure $\mathbb{Z}$ in which subtraction is always defined.
Our next step will be to do similarly for $\div$.

<u>C. The Rationals, $\mathbb{Q}$:</u>

We construct $\mathbb{Q}$ from $\mathbb{N}$ in two steps, both using the "Method of Ordered Pairs".

First, we construct $\mathbb{Q}^{\geq 0}$, the set of non-negative rationals.
We consider the set of all ordered pairs
(n,m) such that $m,n \in \mathbb{N}$ and $m > 0$.
We'd like to think of such an ordered pair as "$\frac{n}{m}$",
so we identify pairs
(n_1, m_1) and (n_2, m_2)
when $n_1 m_2 = n_2 m_1$

Eg: $(1,2)=(2,4)=(3,6)=\dots$ will be the object we call $1/2$
$(2,3)=(4,6)=(6,9)=\dots$ will be the object we call $2/3$
and so forth

Compare with our procedure to construct $\mathbb{Z}$!

We order $\mathbb{Q}^{\geq 0}$ by $(n_1,m_1)<(n_2,m_2)$ when $n_1 m_2 \overset{\text{in } \mathbb{N}}{<} n_2 m_1$
and extend to $\leq$ as usual. ("$<$ or $=$").

We define Arithmetic in $\mathbb{Q}^{\geq 0}$ by
$$(n_1, m_1) + (n_2,m_2) := (n_1 m_2 + n_2 m_1, m_1 m_2)$$
and $$(n_1,m_1)\cdot(n_2,m_2) := (n_1 n_2, m_1 m_2)$$

We embed $\mathbb{N}$ in $\mathbb{Q}^{\geq 0}$ by associating $n \in \mathbb{N}$ with $(n,1) \in \mathbb{Q}^{\geq 0}$

All of this is entirely similar to the extension from $\mathbb{N}$ to $\mathbb{Z}$.
You should verify that our construction of $\mathbb{Q}^{\geq 0}$ agrees w/ your previous experiences in the non-negative rationals.

Finally, we extend from $\mathbb{Q}^{\geq 0}$ to $\mathbb{Q}$
by another application of the Method of Ordered Pairs,
exactly as we did for $\mathbb{N}$ to $\mathbb{Z}$.
(Take ordered pairs (a,b) where $a,b \in \mathbb{Q}^{\geq 0}$
identify pairs w/ the same difference,
define order and arithmetic).
Since the details are very similar to the construction of $\mathbb{Z}$,
we omit them.

Properties of $\langle \mathbb{Q}, +, \cdot \rangle$

A) $\langle \mathbb{Q}, + \rangle$ is a group.

B) $\langle \mathbb{Q} \setminus \{0\}, \cdot \rangle$ is a group.

(But 0 has no multiplicative inverse)

and

i) $+, \cdot$ are commutative

ii) $\langle \mathbb{Q}, +, \cdot \rangle$ is distributive.

These can be verified from properties of $\mathbb{N}$ with a little work (going through 2 applications of MoP.)

Remark: We could have also constructed $\mathbb{Q}$ directly from $\mathbb{Z}$. As that still uses 2 instances of MoP, though, it's not really simpler, and the signs are inconvenient when defining $<$ on $\mathbb{Q}$.

That is, our constructions so far may be diagrammed as

$$\begin{tikzcd} \mathbb{N} \arrow[r, squiggly, "\text{MoP}, \cdot"] \arrow[d, squiggly, "\text{MoP}, +"'] & \mathbb{Q}^{\geq 0} \arrow[d, squiggly, "\text{MoP}, +"] \\ \mathbb{Z} \arrow[r, squiggly, "\text{MoP}, \cdot"'] & \mathbb{Q} \end{tikzcd}$$

D. The Real Numbers, $\mathbb{R}$

Although the rational numbers $\mathbb{Q}$ are "dense" and closed under $+, \cdot$ and their inverses they still are not complete in an important sense – there are "holes", or missing numbers.

<u>Example</u> (Pythagoreans ~500 BCE)

The equation $x^2 = 2$ has no solution in $\mathbb{Q}$ (or in $\mathbb{Q}^{\geq 0}$)

<u>Proof:</u> Suppose that $\frac{n^2}{m^2} = 2$ for some $n, m \in \mathbb{N}$ with $m > 0$.

That is, $n^2 = 2 \cdot m^2$.

Without loss of generality (wlog), we can assume that n, m share no common factor $k \in \mathbb{N}$. (Otherwise, divide both by k).

If n is a multiple of 2, then n^2 is a multiple of 4,

so m^2 is a multiple of 2.

As 2 is not divisible by any integer > 1,

m is a multiple of 2.

But this violates our no-common-factor assumption! #

So n is not a multiple of 2.

But then n^2 is not a multiple of 2, either.

But $2m^2$ is a multiple of 2. #.

As n is either a multiple of 2, or not, the original supposition that $\frac{n^2}{m^2} = 2$ must be false. ∎

This means you can't "walk" from 1 to 2 in $\mathbb{Q}$,

since you'd have to pass through $\sqrt{2} = 1.414\ldots$

$\mathbb{Q}$ has a "hole" where $\sqrt{2}$ should be.

Of course, we can find rational numbers whose square is arbitrarily close to 2:

<u>Consider</u> 1.4, 1.41, 1.414, 1.4142, ...

This last observation leads to a method for completing $\mathbb{Q}$ to $\mathbb{R}$,

(an idea of Dedekind, from 1858).

It's more convenient to first construct $\mathbb{R}^{\geq 0}$, the set of all nonnegative reals.

<u>Definition</u> A <u>(Dedekind) cut</u> for $\mathbb{Q}^{\geq 0}$ is an ordered pair (A, B) of subsets of $\mathbb{Q}^{\geq 0}$, such that

i) $A \cup B = \mathbb{Q}^{\geq 0}$ (cover)

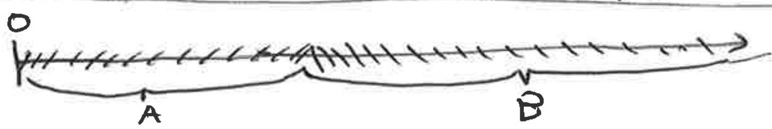
ii) If $a \in A$ and $b \in B$, then $a < b$

iii) A contains no largest element, and B is nonempty.

<u>Eg</u>: • $([0,3), [3,\infty))$ is an (uninteresting) cut for $\mathbb{Q}^{\geq 0}$

• $(\{x \in \mathbb{Q}^{\geq 0} : x^2 < 2\}, \{x \in \mathbb{Q}^{\geq 0} : x^2 \geq 2\})$ is a more interesting example.

<u>Picture of a cut:</u>



We'll use the notation $A \mid B$ for a cut, and will sometimes use a letter like $\alpha = A \mid B$.

We now define $\mathbb{R}^{\geq 0}$ to be the set of all cuts for $\mathbb{Q}^{\geq 0}$.

Now, $\mathbb{Q}^{\geq 0}$ embeds into $\mathbb{R}^{\geq 0}$ by the association

$$\frac{n}{m} \longleftrightarrow [0, \tfrac{n}{m}) \mid [\tfrac{n}{m}, \infty).$$

Notice that cuts of this form have a least element for B. Moreover, if B has a least element, then this least element is a rational $\frac{n}{m}$, and then $A \mid B$ is the cut associated with $\frac{n}{m}$.

Cuts $A \mid B$ where B has no least element produce a new construct, conceptually filling a hole at the "missing" least element.

Example: 2, considered as a number in $\mathbb{R}^{\geq 0}$, corresponds to the Dedekind cut $[0,2) \mid [2,\infty)$.

ie, as the set of all nonnegative rational numbers <2

together with " " " " " " " ≥ 2.

Remark: Writing this Dedekind cut as $[0,2) \mid [2,\infty)$ is a bit imprecise, as $[0,2)$ usually refers to the real numbers between 0 and 2, while DC's involve 'intervals' of positive rationals.

More precise, but longer notation, would be

$$[0,2) \cap \mathbb{Q}^{\geq 0} \mid [2,\infty) \cap \mathbb{Q}^{\geq 0},$$ or better yet
$$\{x \in \mathbb{Q}^{\geq 0} : x < 2\} \mid \{x \in \mathbb{Q}^{\geq 0} : x \geq 2\}.$$

Let's use the short notation, but remember that we're looking at rational numbers (and sets thereof).

Example: Similarly, $\frac{1}{2}$ as a nonnegative real "is" the Dedekind cut $[0, \frac{1}{2}) \mid [\frac{1}{2}, \infty)$

rational intervals.

Example: Define

$$A_{\sqrt{2}} := \{x \in \mathbb{Q}^{\geq 0} : x^2 < 2\}$$
$$B_{\sqrt{2}} := \{x \in \mathbb{Q}^{\geq 0} : x^2 \geq 2\}$$

as the sets of nonnegative rational numbers that have square <2 (for $A_{\sqrt{2}}$) or ≥ 2 (for $B_{\sqrt{2}}$).

Then i) $A_{\sqrt{2}} \cup B_{\sqrt{2}} = \mathbb{Q}^{\geq 0}$ by definition (as either $x^2 < 2$ or $x^2 \geq 2$)

ii) if $a \in A_{\sqrt{2}}$, $b \in B_{\sqrt{2}}$ then $a < b$ (as $a^2 < b^2 \Leftrightarrow a < b$)

iii) $A_{\sqrt{2}}$ has no largest element (check!)

and $3 \in B_{\sqrt{2}} \Rightarrow B_{\sqrt{2}}$ nonempty.

So $A_{\sqrt{2}} \mid B_{\sqrt{2}}$ is a Dedekind cut.

As $B_{\sqrt{2}}$ has no least element, by the Example of the Pythagoreans, $A_{\sqrt{2}} \mid B_{\sqrt{2}}$ is a "new" element of $\mathbb{R}^{\geq 0}$

Order and inequalities in $\mathbb{R}^{\geq 0}$

Let $r \in \mathbb{R}^{\geq 0}$ be the D.C. $A_r | B_r$, and $s \in \mathbb{R}^{\geq 0}$ be $A_s | B_s$.

We say that $r < s$ (r is <u>less than</u> s)

when $A_r \subsetneq A_s$, that is, when A_r is a proper subset of A_s.

<u>Equivalently</u>: $r < s$ exactly when $B_r \supsetneq B_s$. (Why is this equivalent?)

We extend the $<$ relation to a $\leq$ relation as usual.

<u>Example</u>: Consider $\sqrt{2} = A_{\sqrt{2}} | B_{\sqrt{2}}$ as previously defined.

Since $A_{\sqrt{2}}$ contains all nonnegative rationals w/ square <2,

we see that if $r^2 < 2$, then $A_r \subsetneq A_{\sqrt{2}}$ (for any $r \in \mathbb{Q}^{\geq 0}$).

Similarly, if $s^2 > 2$, then $A_{\sqrt{2}} \subsetneq A_s$, so $s > \sqrt{2}$.

This helps justify the notation $\sqrt{2}$ for this D.C.!

Of course, $\mathbb{R}^{\geq 0}$ is not well-ordered by $\leq$.

To see this, it suffices to check that the interval $(0, \infty) \subseteq \mathbb{R}^{\geq 0}$

has no least element. But if $r = A_r | B_r$ is any element

with $r > 0$, then we can find a smaller element:

$$\{x \in \mathbb{Q}^{\geq 0} : 2x \in A_r\} \mid \{x \in \mathbb{Q}^{\geq 0} : 2x \in B_r\}. \quad \checkmark$$

Arithmetic on $\mathbb{R}^{\geq 0}$:

Let $r = A_r | B_r$ and $s = A_s | B_s$ be in $\mathbb{R}^{\geq 0}$.

We <u>define</u> arithmetic operations on $\mathbb{R}^{\geq 0}$, based on

those already defined for $\mathbb{Q}^{\geq 0}$.

Notice that the 2nd part of a D.C. is the set complement

of the 1st part: that is, for D.C. $A | B$,

$$B = \mathbb{Q}^{\geq 0} \setminus A = \{x \in \mathbb{Q}^{\geq 0} : x \notin A\}.$$

In particular, it is enough to specify the 1st part of a D.C.

Definition:

1) Addition: Assume $r, s > 0$.

Then let $r+s := A|B$, where $A = \{x+y : x \in A_r \text{ and } y \in A_s\}$.

That is, $r+s$ is the cut so that

- A has all the nonnegative rationals that can be written as a sum of numbers in A_r, A_s, while
- B has all the nonneg. rationals that cannot be written in this form

(As usual, if r or $s=0$, we'll define $0+s := s$ and $r+0 := r$.)

2) Multiplication: Similarly, let $r \cdot s := A|B$, where $A = \{x \cdot y \mid x \in A_r, y \in A_s\}$

Proposition: Addition and multiplication yield cut pairs that satisfy the definition of a D.C.

Proof: 1) Addition: Check the properties! If r or $s=0$, then trivial. Otherwise,

(i) is automatic by the "1st part" specification.

(ii) Follows, as if $a \in A$ with $a = x+y$ $(x \in A_r, y \in A_s)$ and $0 \le b < a$, then either

- $0 \le b \le x$, so $b \in A_r$, so $b = b+0 \in A$ ✓

or

- $x < b < x+y$, so $b = x+w$, some $0 \le w < y$. Then $w \in A_s$, so $b \in A$. ✓

(iii) follows: B is nonempty as $z \in B_r$, $w \in B_s \Rightarrow z+w \in B$ ~~(by basics of inequalities)~~ (since $\le$ is compatible w/ $+$ in $\mathbb{Q}^{\ge 0}$)

and A has no greatest element since A_r, A_s do not. (If $x+y \in A$, then $x^*+y \in A$ for any $x^* > x$ in A_s.) ✓

2) Multiplication: is entirely similar. (Check it!)

∎

<u>Example:</u> Calculate $\sqrt{2}\cdot\sqrt{2} = A \mid B$. (That is, show $\sqrt{2}\cdot\sqrt{2}=2$)

We have $A = \{ x\cdot y \in \mathbb{Q}^{\geq 0} : x^2 < 2 \text{ and } y^2 < 2 \text{ w/ } x, y \in \mathbb{Q}^{\geq 0} \}$

We want to show that A agrees with

$$A_2 = \{ z \in \mathbb{Q}^{\geq 0} : z < 2 \}.$$

It is clear that $A \subseteq A_2$, as $x^2 < 2$ and $y^2 < 2 \Rightarrow x^2 y^2 < 4$

$\Rightarrow xy < 2.$

For the other way, it is enough to find $\frac{m}{n} \in \mathbb{Q}^{+}$ values so that $\left(\frac{m}{n}\right)^2$ can be taken arbitrarily close to 2.

The decimal approximations 1.4, 1.41, 1.414, ... will suffice. (Details on hw.)

<u>Observe:</u> $+$ and $\cdot$ in $\mathbb{Q}^{\geq 0}$ are compatible with the same operations in $\mathbb{R}^{\geq 0}$.

That is, if $\frac{m}{n}$ and $\frac{p}{q}$ are in $\mathbb{Q}^{\geq 0}$ then as reals (via the usual embedding)

we have for addition

$$\left([0, \tfrac{m}{n}) \mid [\tfrac{m}{n}, \infty) \right) + \left([0, \tfrac{p}{q}) \mid [\tfrac{p}{q}, \infty) \right)$$

$$= \{ x+y : 0 \leq x < \tfrac{m}{n},\ 0 \leq y < \tfrac{p}{q} \} \mid \text{(2nd part)}$$

$$= [0, \tfrac{m}{n} + \tfrac{p}{q}) \mid [\tfrac{m}{n} + \tfrac{p}{q}, \infty)$$

as the least value not expressing as $x+y$ w/ $x < \frac{m}{n}$, $y < \frac{p}{q}$ is $\frac{m}{n} + \frac{p}{q}$.

Similarly for multiplication.

So far we've talked only about $\mathbb{R}^{\geq 0}$.

We extend from $\mathbb{R}^{\geq 0}$ to $\mathbb{R}$ via the Method of Ordered Pairs in an entirely similar way to the extension $\mathbb{N}$ to $\mathbb{Z}$ or $\mathbb{Q}^{\geq 0}$ to $\mathbb{Q}$.

(so take pairs $(a, b) \in (\mathbb{R}^{\geq 0})^2$, identify pairs to think of as "$a-b$")

I'll summarize with a diagram the constructions we've made:

$$\begin{tikzcd} \mathbb{N} \arrow[r, squiggly] \arrow[d, squiggly] & \mathbb{Q}^{\geq 0} \arrow[r, squiggly] \arrow[d, squiggly] & \mathbb{R}^{\geq 0} \arrow[d, squiggly] \\ \mathbb{Z} \arrow[r, squiggly, dashed] & \mathbb{Q} \arrow[r, squiggly, dashed] & \mathbb{R} \end{tikzcd}$$

The dotted arrows are constructions we did not consider, but could have. We took the path that we did, as it simplifies some arguments to only deal w/ positives.

We extend $\leq, +, \cdot$ from $\mathbb{R}^{\geq 0}$ to $\mathbb{R}$ in a manner entirely similar to the extension from $\mathbb{N}$ to $\mathbb{Z}$ or $\mathbb{Q}^{\geq 0}$ to $\mathbb{Q}$. (using the Method of Ordered Pairs).

All the nice arithmetic properties of $\mathbb{Q}$ also hold for $\mathbb{R}$ (This shouldn't be a surprise - after all, we built $+, \cdot$ for $\mathbb{R}$ from that in $\mathbb{Q}$)

<u>Properties of $\langle \mathbb{R}, +, \cdot \rangle$</u>

A) $\langle \mathbb{R}, + \rangle$ is a group.

B) $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$ is a group.

<u>and</u> i) $+, \cdot$ are commutative

ii) $\langle \mathbb{R}, +, \cdot \rangle$ is distributive.

These are properties that we'd like to talk about together (the properties of a "nice" number system), so again, we give the set of properties a name.

<u>Definition:</u> A <u>field</u> is a set $\mathbb{F}$ with operations $+, \cdot$, so that

A) $\langle \mathbb{F}, + \rangle$ is a group, w/ identity element 0.

B) $\langle \mathbb{F} \setminus \{0\}, \cdot \rangle$ is a group (w/ " " 1.)

i) $+, \cdot$ are each commutative, and

ii) $+, \cdot$ satisfy the distributive law.

Remark: We can always name the additive identity of $\mathbb{F}$ as 0, even if $\mathbb{F}$ is unrelated to the reals. Similarly for the multiplicative identity 1.

We can now summarize our lists of properties much more shortly!

Properties of $\mathbb{Q}, \mathbb{R}$: $\langle \mathbb{Q}, +, \cdot \rangle$ and $\langle \mathbb{R}, +, \cdot \rangle$ are both fields.

Example: The following operations on the set $\mathbb{F}_2 = \{0, 1\}$ yield a field.

$a+b$	0	1
0	0	1
1	1	0

$a \cdot b$	0	1
0	0	0
1	0	1

(Exercise / self-check: Verify that the field axioms hold!)

Notice: the orders on $\mathbb{Q}$ and $\mathbb{R}$ are compatible w/ the algebraic/arithmetic structure, in the sense that whenever $r, s, t \in \mathbb{R}$,

- If $r \leq s$, then $r + t \leq s + t$
- If $r \leq s$ and $t \geq 0$, then $r \cdot t \leq s \cdot t$.

(Remark: A field with an order $\leq$ satisfying these additional properties is called an ordered field. Thus, $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields.)

Completeness:

We constructed $\mathbb{R}$ to "fill in holes" in $\mathbb{Q}$ (using D.C.'s). Our next goal will be to give one notion of a "hole".

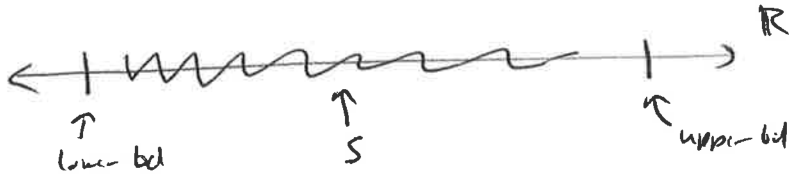
The crucial property of $\mathbb{R}$ is that it has no "holes" in this sense.

(The general idea of $\mathbb{R}$ having no "holes" is called "completeness", and is something that we will return to later, using different language.)

<u>Definition (Bounded Sets):</u>

Let $S \subseteq \mathbb{R}$ be a set of real numbers, and let $\alpha \in \mathbb{R}$.
We say that α is an <u>upper bound</u> for S
if for every $x \in S$, we have $x \leq \alpha$.
Similarly, if $\forall x \in S$, have $x \geq \alpha$,
then we say α is a <u>lower bound</u> for S.

<u>Picture:</u>



<u>Eg:</u> $\{0, 2, 17\}$ has 18 as an upper bound.
(also 17, 20, but <u>not</u> 16.)

<u>Eg:</u> $(-\infty, 2)$ is an interval with $2, 3, \pi, \ldots$ as u.b.'s.
In this example, 2 is the least possible upper bound, and there is <u>no</u> lower bound.

A set with an upper bd (of α) is <u>bounded from above</u> (by α).
Similarly for <u>bounded from below</u>.

If a set is bounded from above (by $\alpha > 0$)
and also " " below (by $-\alpha$)
then we call the set <u>bounded</u>.

<u>Eg:</u> The interval $[0, 2]$ is bounded.

<u>Eg:</u> Which of the above sets $\{0, 2, 17\}$ and $(-\infty, 2)$ are bounded?

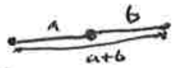
Digression: The Triangle Inequality

The following is often useful for showing sets to be bounded.

Lemma (Δ inequality)

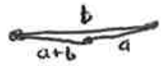
If $a, b \in \mathbb{R}$, then $|a+b| \leq |a| + |b|$.

(as usual, $|a|$ is the absolute value of a.)



Proof Sketch: Either a, b have same sign (so $|a+b| = |a| + |b|$)

or different sign (and $|a+b| \lneq$ " "). $\square$



Example: Assuming that you remember trigonometry,

let S be the set $\{3\sin x + 2\cos 2x : x \in \mathbb{R}\}$.

Show that S is bounded.

Solution: From earlier trig classes, we remember that

$|\sin * | \leq 1$ and $|\cos *| \leq 1$.

Thus, $|3\sin x + 2\cos 2x| \overset{\Delta\text{ineq}}{\leq} |3\sin x| + |2\cos 2x|$

$= 3|\sin x| + 2|\cos 2x|$

$\leq 3 \cdot 1 + 2 \cdot 1 = 5$

so S is bounded by 5.

We return to our main stream of thought, heading towards "Completeness".

Definition: (maximum, supremum)

- If a set S of real numbers has a largest element s_{max} (so $s_{max} \in S$, and for any $s \in S$, have $s \leq s_{max}$) then s_{max} is the maximum of S. Write it as $\max S$.

  Eg: Formula from Course Outline for grades!!

- If a nonempty set S of real numbers has any upper bound, then the least upper bound or supremum for S is a real number t (not necessarily in S), such that

i) t is an upper bound for S, and

ii) if t_* is another upper bound for S,

then $t \le t_*$.

Write $\sup S$ for the supremum of S. (when S has upper bd)

<u>Eg:</u> Consider the following intervals:

- $S = [0,2]$ has $\max S = \sup S = 2$.
- $S = [0,2)$ has no max, but $\sup S = 2$.
- $S = [0,\infty)$ has neither max nor sup. (Nor upper bd!)

It is immediate from definitions that if S has a maximum, then $\max S = \sup S$. (But sets such as $[0,2)$ may have supremum without having a maximum.)

Our 1st notion of completeness is stated in terms of sups. We start with a simplified version.

<u>Proposition:</u> ("$\mathbb{R}^{\geq 0}$ completeness")

If a set $S \subseteq \mathbb{R}^{\geq 0}$ is bounded from above, then S has a supremum in $\mathbb{R}^{\geq 0}$.

<u>Proof:</u> We use Dedekind cuts to translate from real numbers to sets.

For each $r \in S$, there is a D.C. $A_r \mid B_r$.

Since S is bounded from above, there is some $A_* \mid B_*$ s.t. for every r, we have $A_r \subseteq A_*$.

We now build a new D.C. by taking

$$t = A \mid B \quad \text{for } A = \bigcup_{r \in S} A_r, \quad B = \mathbb{Q}^{\geq 0} \setminus A.$$

Check that $A|B$ is really a D.C:

(i) is immediate from construction

(ii) is easy; if $a \in A$, then $a \in A_r$ for some r, so any $b < a$ is in A_r so $b \in A$.

(iii) A has no greatest element since the A_r's don't.
B is nonempty since $A \subseteq A_*$, and $B_* \neq \emptyset$.

Now t is an upper bd for S,
as for all $r \in S$ we have $A_r \subseteq A$.
Also, t is the least upper bound. It is enough to show
that if $s < t$, then s is not an u.b.
But if $s = C \mid D < t = A \mid B$
then $C \subsetneq A$, so there's some $\frac{p}{q}$ in A but not C
Now, by definition of A, there is some r_0 w/ $\frac{p}{q} \in A_{r_0}$.
But then $r_0 \not\leq s$!! So s is not an upper bd. ∎

The extension from $\mathbb{R}^{\geq 0}$ to $\mathbb{R}$ via M.P yields no surprises,
and we state the general result:

Theorem: (Completeness of $\mathbb{R}$, Order version)
If $S \subseteq \mathbb{R}$ is bounded from above,
then S has a supremum in $\mathbb{R}$.

Similar notions hold from below.

Definition: (minimum, infimum)
- If a set $S \subseteq \mathbb{R}$ has a least element s_{min},
then s_{min} is the minimum of S. Write as $\min S$.
- If a nonempty set S has some lower bound,
then a <u>greatest lower bound</u> or <u>infimum</u> for S
is the greatest number that is a lower bound for S.
Write as $\inf S$.

Eg: $S = (0,2]$ has inf of 0, while $T = [0,2]$ has $\inf T = \min T = 0$.

<u>Observation:</u> For real numbers r, s, $r < s \iff -r > -s$.

This observation lets us turn any theorems about upper-bounds, maxes, or sups into theorems about lower bds, mins, or infs.
Let's examine this technique closely, applied to Completeness.

<u>Theorem:</u> (Completeness of $\mathbb{R}$, inf version)
If $S \subseteq \mathbb{R}$ is bounded from below,
then S has an infimum in $\mathbb{R}$.

<u>Proof:</u> Let $-S := \{-x : x \in S\}$
We use the observation repeatedly to translate:
If r is a lower bd for S,
then $-r$ is an upper bd for $-S$
so $-S$ has a supremum, $\sup S = -t \in \mathbb{R}$
(by Completeness Thm)
and then $-(-t) = t$ is an infimum for S. ∎

<u>Fact:</u> $\mathbb{R}$ is the only complete, ordered field "up to isomorphism".
That is, if $\langle \mathbb{F}, +, \cdot \rangle$ is a complete ordered field,
then it can be identified with $\mathbb{R}$ by relabelling numbers.

<u>Principle of Trichotomy:</u>
It is sometimes useful to notice that
for any $a, b \in \mathbb{R}$, exactly one of the following occurs:
i) $a < b$, ii) $a > b$, or iii) $a = b$.

E. The Complex Numbers, $\mathbb{C}$

We've seen the real numbers $\mathbb{R}$ to be complete under sup/inf. However, they are lacking another "completeness" or closure property: there are equations, such as $x^2=-1$, without any solution in $\mathbb{R}$.

As a main complaint we had about $\mathbb{Q}$ was that the equation $x^2=2$ has no solution in $\mathbb{Q}$, this is a bit upsetting!

Notice that the difference between $\sqrt{2}$ and "$\sqrt{-1}$" here is that rationals like $1.41, \ldots$ are quite close to 2 when squared. But the square of any rational is positive or 0, so differs by at least 1 with -1.

<u>Definition</u> Let $\mathbb{C}$ be the set of all ordered pairs

$$\{(a,b) \; : \; a,b\in\mathbb{R}\}$$

think of as "$a+bi$"

with operations

$+$, defined entrywise $(a,b)+(c,d):=(a+c,b+d)$, and

$\cdot$, defined by $(a,b)\cdot(c,d):=(ac-bd,ad+bc)$

<u>Remark</u> Unlike previous applications of the MofOP's we make no identifications among ordered pairs!

We can quickly see some behavior that may be familiar:

- the association of $x\in\mathbb{R}$ to $(x,0)\in\mathbb{C}$ gives an embedding of $\mathbb{R}$ into $\mathbb{C}$.

  The embedding respects $+, \cdot$
  (so $a+b$ in $\mathbb{R}$ agrees w/ $a+b$ in $\mathbb{C}$ no matter when we embed.)

- If we write i for the element $(0,1)$,
  and bi " " " $(0,b)$

  then any $(a,b) \in \mathbb{C}$ can be written as $a+bi$.

  Notice that $i^2 = [(0,1)]^2 = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0)$
  $= (-1,0) = -1$.

  We recover our familiar representation of $\mathbb{C}$
  with $(a+bi)\cdot(c+di) = (ac-bd) + (ad+bc)i$.

<u>Properties of $\mathbb{C}$:</u>

For $z = a+bi \in \mathbb{C}$,
write $\overline{z}$ for the <u>complex conjugate</u> $a-bi$.

Notice that $z\cdot\overline{z} = (a+bi)\cdot(a-bi) = a^2+b^2$, a real number.

Using this, we show:

<u>Lemma:</u> If $z \neq 0$ is a complex number,
then z has a multiplicative inverse given by

$$z^{-1} = \frac{\overline{z}}{z\cdot\overline{z}} \qquad \left(= \frac{a-bi}{a^2+b^2}\right)$$

$\nwarrow$ real

<u>Proof:</u>

$$z\cdot z^{-1} = \frac{z\cdot\overline{z}}{z\cdot\overline{z}} = \frac{z\cdot\overline{z}}{a^2+b^2} = \frac{a^2+b^2}{a^2+b^2} = 1.$$ ☒

<u>Eg:</u> For $z = 1-2i$, $z^{-1} = \frac{1+2i}{5} = \frac{1}{5} + \frac{2}{5}i$

or $(\frac{1}{5}, \frac{2}{5})$ in ordered pair notation. ✓

With multiplicative inverses calculated, it is straightforward to verify

<u>Proposition:</u> $\mathbb{C}$ is a field.

<u>Self-check:</u> How would you verify this Proposition?

Completeness in $\mathbb{C}$?

Although $\mathbb{C}$ is a field, it has no sensible order, and is not an ordered field.

Since $\mathbb{C}$ is not ordered, we can't easily use our notion of completeness with sup/inf in $\mathbb{C}$.

Remember that sup/inf depended heavily on order.

(This might be a reason to look for another idea of "completeness", as we later will.)

Closed-ness of $\mathbb{C}$:

We defined $\mathbb{C}$ to have a $\sqrt{-1}$ element.

Much more is true:

- $\mathbb{C}$ is closed under $\sqrt{\ }$:

  You can check by computation that

  $$\sqrt{a+bi} = \sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i \cdot \underbrace{\frac{|b|}{b}}_{\text{"sign } b\text{"}} \cdot \sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}$$

  (or there's a geometric interpretation w/ polar coordinates.)

  It follows that

- $\mathbb{C}$ is closed under taking roots of quadratic equations, since the solution of the quadratic equation only relies on computing square roots.

  If $u, v, w \in \mathbb{C}$, then equation $ux^2 + vx + w = 0$ has solution(s) $x \in \mathbb{C}$, such as $\dfrac{-v + \sqrt{v^2 - 4uw}}{2u}$.