Math Club (September 29) — Real Numbers — Paul Cazeaux

... Or how I started to love Analysis.

A bit of history: At the beginning, there were only the *natural integers*, used for counting stuff. *Ratios* then appeared early in Antiquity, with the first *incommensurable* numbers being discovered in the VIth century BC. in Ancient Greece. Eudoxus of Cnidus formalized a theory of commensurable and incommensurable ratios, which we would call nowadays the positive real numbers. Negative numbers had to wait many centuries, because they are so scary...

Although they were used for many centuries, a proper theory or construction of *Real Numbers* had to wait until the end of the 19th century, when Peano, Dedekind, Cantor, Weiestrass and other mathematicians finally formalized the classical relation

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

How well do you know your $\mathbb{R}$?

1. Who is the ancient Greek mathematician that believed all numbers to be rational, and when one of his students discovered the existence of irrational numbers, that student was drowned at sea as a sacrifice to the gods?

2. Pick the irrational and rational numbers out of the list:

$$\left\{ 0,\ \frac{3}{\sqrt{2}},\ \cos(\pi),\ e^{\pi},\ \frac{1+\sqrt{5}}{1-\sqrt{5}},\ \sqrt{-3},\ 0.19191919\ldots, \right\}$$

3. Saying a number is *transcendental* means...
   (a) a synonym for *irrational*,
   (b) it is the root of some nonzero polynomial with integer coefficients,
   (c) it is not the root of any nonzero polynomial with integer coefficients,
   (d) it transcends dental functions.

4. Is $\mathbb{R}$ the only ordered and complete commutative field?

Rational Numbers: the field $\mathbb{Q}$

The rationals numbers p/q are built out of the ring $\mathbb{Z}$ of relative integers, which is itself built out of the associative monoid $\mathbb{N}$ of natural integers.
In each case, we plug 'holes' in our ability to solve equations:

- Equations like $n + 1 = 0$ have no solution in $\mathbb{N}$.

$\rightarrow$ we introduce *opposites* $-n$ of nonzero natural integers.

- Equations like $2x - 1 = 0$ have no solution in $\mathbb{Z}$.

$\rightarrow$ we introduce *inverses* $1/n$ of nonzero relative integers.

Formal definition:

- Equivalence relation on pairs of integers $(a, b) \in \mathbb{Z}\times\mathbb{Z}^*$:

$$(a, b) \sim (c, d) \quad \text{iff } ad = cb.$$

  Denote equivalence classes $a/b \in \mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*)/\sim$.

- Compatible addition and multiplication operations:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

- Operations are commutative, associative, distributive.
- Every element has an opposite: $-a/b = (-a)/b$.
- Every nonzero rational has an inverse: $(a/b)^{-1} = b/a$.
- Total order on $\mathbb{Q}$: a/b is positive iff $ab > 0$ and

$$x \geq y \quad \text{iff} \quad x - y \geq 0, \qquad x, y \in \mathbb{Q}.$$

- Inclusion $\mathbb{Z} \subset \mathbb{Q}$: $n \mapsto n/1$.

Some properties of $\mathbb{Q}$:

- $\mathbb{Q}$ is a *totally ordered field.*
- $\mathbb{Q}$ is countable.
- Every totally ordered field contains a ring isomorphic to $\mathbb{Z}$: $Z = \{n \times 1, \quad n \in \mathbb{Z}\}$ and a sub-field isomorphic to $\mathbb{Q}$,

$$Q = \{pq^{-1}, \qquad p \in Z, q \in Z \setminus \{0\}\}.$$

- $\mathbb{Q}$ has the Archimedean property: for any $x, y \in \mathbb{Q}$,

$$x, y > 0 \implies \exists n \in \mathbb{N}, \quad nx > y.$$

- We have an *absolute value*:

$$|x| = \max(x, -x).$$

Activities

1. Show that any totally ordered field has the Archimidean property if, and only if, Q is dense in K:

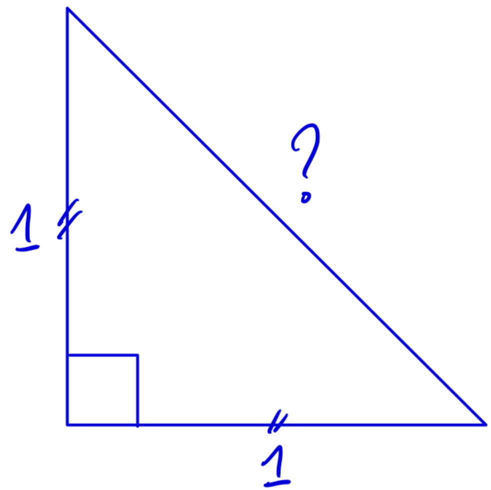
   For any $x < y$ in K, $\quad$ there is $r \in Q$ such that $x < r < y$.

2. Show that $\mathbb{Q}$ is countable by coming up with a way to *enumerate* elements of $\mathbb{Q}$.
3. Check the classical properties of the absolute value.

The holes in $\mathbb{Q}$

Why are we not happy with $\mathbb{Q}$?

- **Algebra!**
  Some simple equations have no solution: $x^2 = 2$.
- **Analysis!**
  Some sequences that *should* morally converge do not: take the partial sums of the classical series
  $$u_n = \sum_{k=1}^{\infty} \frac{1}{k!}.$$
- **Topology!**
  Some non-empty parts of $\mathbb{Q}$ are bounded from above, yet have no maximum: take
  $$A = \{x \in \mathbb{Q}, \qquad x^2 \leq 3\}.$$



The dawn of Analysis.

- With order comes idea of *upper bound*:
  $$M = sup(A) \text{ iff } (x \geq a, \quad \forall a \in A) \implies x \geq M.$$
- With absolute value comes notion of *convergence*:
  $$l = \lim_{n\to\infty} u_n \text{ iff } \forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, \ |u_n - l| < \varepsilon.$$
- If we don't know l, we check the Cauchy property: u_n is a Cauchy sequence if
  $$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, \ |u_n - u_m| < \varepsilon$$

Activities

1. Show that there is no $x \in \mathbb{Q}$ such that $x^2 = 2$.
2. Show that the sequence $u_n = 1/n$ converges to 0 in a field K which has the Archimidean property.
3. Show that $u_n = \sum_{k=1}^{\infty} \frac{1}{k!}$ forms a Cauchy sequence.

Completeness

Let K be an ordered field. Here are some desired properties:

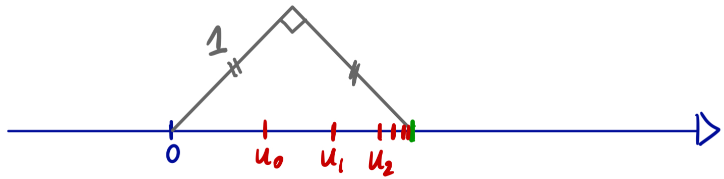
- **Property of the upper bound:**
  Any non-empty part of K, bounded from above, admits an upper bound.
- **Cauchy property:**
  Any Cauchy sequence converges.
- **Property of nested intervals:**
  If $I_n = [a_n, b_n]$ with $I_{n+1} \subset I_n$ and $b_n - a_n \to 0$, then $\bigcap_{n \geq 0} I_n$ contains exactly one element of K.

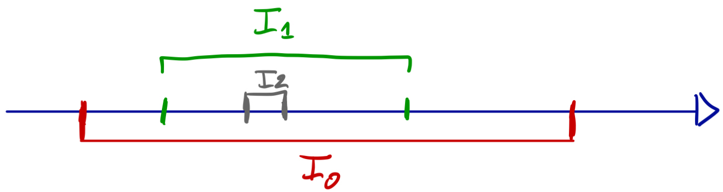
Theorem. The following properties are equivalent:

- K has the property of the upper bound;
- Any increasing sequence bounded from above converges in K;
- K is Archimedean and has the Cauchy property;
- K is Archimedean and has the property of nested intervals.

Under these conditions, we say K is complete.

Narrator: sadly, $\mathbb{Q}$ is not complete.





Activities

1. Let K be a complete ordered field. Show that for any $y \in K$, $y \geq 0$ if and only if there exists $x \in K$ such that $y = x^2$.

Building $\mathbb{R}$, take one: Dedekind Cuts

We've seen that some parts of $\mathbb{Q}$ do not have upper bounds. Let's fix that by making these 'holes' into new objects!

Definition. A Dedekind cut is a partition of $\mathbb{Q}$ into two nonempty parts (α, β) such that

1. $\alpha \cup \beta = \mathbb{Q}$,
2. For all $a \in \alpha$, $b \in \beta$, we have $a < b$:
3. The right part β has no minimum (i.e. a lower bound that also belongs to β).

We call $\alpha = \beta^c$ the left part and β the right part of the cut. Note how only the knowledge of β is needed to form the cut.

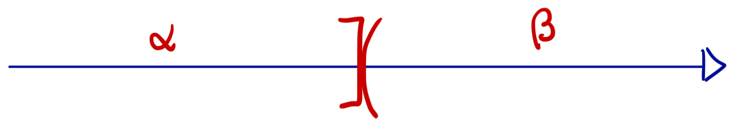
We call $\mathcal{D} \subset P(\mathbb{Q})$ the set of Dedekind cuts.

Example. Any rational $r \in \mathbb{Q}$ defines a unique Dedekind cut $\alpha = \{x \in \mathbb{Q}, x \leq r\}$, $\beta = \{x \in \mathbb{Q}, x > r\}$.
This allows us to identify $\mathbb{Q} \subset \mathcal{D}$.

Structure as an ordered ring

$$
\begin{aligned}
\beta + \beta' &= \{x + x',\ x \in \beta, x' \in \beta'\},\\
-\beta &= \{x \in \mathbb{Q},\ \text{s.t. } \forall b \in \beta, x > -b\} \setminus \{-\max(\beta^c)\},\\
\beta \times \beta' &= \begin{cases} \{xx',\ x \in \beta, x' \in \beta'\} & \text{if } \beta, \beta' \subset \mathbb{Q}^+,\\ -(\beta \times (-\beta')) & \text{if } \beta \subset \mathbb{Q}^+, \beta' \not\subset \mathbb{Q}^+,\\ -((-\beta) \times \beta') & \text{if } \beta \not\subset \mathbb{Q}^+, \beta' \subset \mathbb{Q}^+,\\ ((-\beta) \times (-\beta')) & \text{if } \beta, \beta' \not\subset \mathbb{Q}^+. \end{cases}\\
\beta \leq \beta' &\quad \text{iff } \beta \subset \beta'.
\end{aligned}
$$

Theorem (Dedekind) The set $\mathcal{D}$ of Dedekind cuts can be equipped with a structure of totally ordered, complete commutative field.



Proof: tedious. For the *completeness* property, let us take $A \subset \mathcal{D}$ non-empty, bounded from above. Then

$$\mu = \left(\bigcup_{\beta \in A} \beta^c \right)^c$$

can be shown to be a Dedekind cut:

- μ and μ^c are nonempty, and μ has no minimum;
- if $x \in \mu$, $y \in \mu^c$, then $x > y$;
- μ is the upper bound of A.

Activities

1. Show that the same construction, repeated with $\mathcal{D}$ as a starting point, yields a field which is isomorphic to $\mathcal{D}$.

Building $\mathbb{R}$, take two: Cauchy sequences

A sequence u_n of rationals is a Cauchy sequence if:

$$\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, \; |u_n - u_m| < \varepsilon.$$

1. First, we define the set of Cauchy sequences $\mathcal{C}$. This is a *sub-ring* of the set of rational sequences:
   - For $u, v \in \mathcal{C}$, $u + v = \{u_n + v_n\} \in \mathcal{C}$, $u \times v = \{u_n v_n\} \in \mathcal{C}$,
   - We have neutral elements $\{0, 0, \dots\}$ for the addition and $\{1, 1, \dots\}$ for the multiplication.
2. However, observe that $\mathcal{C}$ is too big:
   - many sequences converge to the same number,
   - there is no inverse for some nonzero sequences, such as $\{1, 0, 1, \dots\}$.

   Define the equivalence relation

$$u \sim v \quad \text{iff} \quad \lim_{n \to \infty} u - v = 0.$$

Definition. The ring $\widetilde{\mathcal{C}}$ is defined as the quotient $\mathcal{C}/\sim$, identifying sequences that have the same limit.

- This set can be ordered: we say that $\pi(u) > 0$ if for any *representative* sequence u, $u_n > 0$ for n big enough.

Theorem. $\widetilde{\mathcal{C}}$ may be equipped with a structure of totally ordered, complete commutative field.

Proof: tedious. For the *completeness* property, one starts by showing that any element of $\widetilde{\mathcal{C}}$ is the limit of a sequence of "rationals" $\pi(\{r, r, \dots\})$. Given a Cauchy sequence u_n in $\widetilde{\mathcal{C}}$, define "rationals" r_n such that $|r_n - u_n| < 1/n$. Then for m, n big enough,

$$|r_n - r_m| \leq |r_n - \widetilde{u}_n| + |\widetilde{u}_n - \widetilde{u}_m| + |\widetilde{u}_m - r_n| \leq \frac{1}{n} + \frac{1}{m} + \varepsilon,$$

so $\{r_n\}$ is itself a Cauchy sequence, which corresponds to an element r of $\widetilde{\mathcal{C}}$. Finally one finds $\lim_{n\to\infty} u_n - r = 0$.

Activities

1. Show that a Cauchy sequence is bounded, then that the product uv of two Cauchy sequences is a Cauchy sequence.
2. Show that if $u \sim u'$ and $v \sim v'$ then $u + v \sim u' + v'$ and $uv \sim u'v'$.
3. Show that if $u \not\sim 0$, then there exists v such that $uv \sim 1$.
4. Show that the same construction, repeated with $\widetilde{\mathcal{C}}$ as a starting point, yields a field which is isomorphic to $\widetilde{\mathcal{C}}$.

Counting the real numbers

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are all countable. What about $\mathbb{R}$?!

Theorem. (Cantor)
The set $\mathbb{R}$ of real numbers is uncountable.

First proof. I start, you finish! Let us show that $[0,1]$ is uncountable. Assume by contradiction that we can order all its elements in a sequence $\{a_n\}_{\geq 0}$.

1. Divide $I_0 = [0,1]$ in three pieces $[0,1/3]$, $[1/3,2/3]$, $[2/3,1]$. Define I_1 as the left-most piece that does not contain a_0.
2. Write an algorithm continuing this process, forming a sequence of nested intervals I_n such that $a_n \notin I_n$.
3. Compute the length of the intervals I_n.
4. Conclude!

Second proof. Any real number in $(0,1]$ admits a unique proper decimal representation

$$a = 0.d_1 d_2 \dots$$

that does not end in $9999\dots$. As before, assume numbers in $(0,1]$ can be ordered in a sequence $a_0, a_1, \dots$:

$$\begin{aligned} a_0 &= 0.d_{01}d_{02}d_{03}\dots d_{0p}\dots \\ a_1 &= 0.d_{11}d_{12}d_{13}\dots d_{1p}\dots \\ a_2 &= 0.d_{21}d_{22}d_{23}\dots d_{2p}\dots \\ &\vdots \\ a_n &= 0.d_{n1}d_{n2}d_{n3}\dots d_{np}\dots \\ &\vdots \end{aligned}$$

Using a diagonal procedure, create a number $x \in (0,1]$ with proper decimal representation $0.x_1 x_2 \dots x_p \dots$ which is different from all the a_n.

Activities

1. Show there is no surjection from $\mathbb{N}$ onto the set of functions from $\mathbb{N}$ into $\mathbb{N}$.

Rich numbers

- Real numbers are *weird*. Most of them are *rich*!

Let's start with:
Theorem. Let $b \geq 2$ be an integer. A number $x \in \mathbb{R}$ is rational if and only if its developement in base b is periodic after a long enough rank.

Prove this! Let $0 \leq p/q < 1$ a rational number, we get the first digit a_1 by euclidean division:

$$bp = a_1 q + r_1, \qquad 0 \leq r_1 < q.$$

- Why do we have $0 \leq a_1 < b$?
- How to get the next digits?
- Why must this process repeat? (Pigeonhole...)

A real number is *rich* if its decimal expansion contains every possible sequence of numbers. They are all irrational.
We want to prove that **almost all numbers in** $(0, 1]$ **are rich.**

1. Let A_1 be the set of all real numbers in $(0, 1]$ which contains 0 as the first digit of their decimal expansion. Show that A_1 is an interval with length $1/10$.
2. Let A_i be the set of all real numbers in $(0, 1]$ which contains 0 as the i^{th} digit of their decimal expansion. Show that it is a collection of intervals with cumulative length $1/10^i$.
3. Compute the 'length' of the set B_0 of all real numbers that contains 0 anywhere in their decimal expansion.
4. Explain why the same should be true of any set B_n of all the real numbers that contain n's decimal expansion as a sequence of digits anywhere in their decimal expansion.
5. Assuming a countable union of sets of measure (length) zero has measure zero, you can conclude!

Activities

1. Now that you know this, write a few irrational numbers!