REAL ANALYSIS: LECTURE 5

SEPTEMBER 21ST, 2023

1. Preliminaries

Recall, $\mathbb{R}$ satisfies (A1) - (A11), i.e. it's a field. However, we're not done yet, as there are many fields; for example, $\mathbb{Q}, \mathbb{Z} \pmod 2, \mathbb{Z} \pmod 7, \mathbb{C}$. Here $\mathbb{C}$ are the complex numbers. Meta-analytically, we could define

$$\mathbb{C} := \{a + bi \ : \ a, b \in \mathbb{R}\}.$$

We also introduced (A12) by defining a notion of *positive numbers*. Formally, (A12) states $\exists \mathbb{P} \subseteq \mathbb{R}$ s.t.

(i) $\mathbb{P}$ is closed under addition and multiplication, i.e. $\forall x, y \in \mathbb{P}, x + y \in \mathbb{P}, x \cdot y \in \mathbb{P}$
(ii) Trichotomy: for each $x \in \mathbb{R}$, *exactly one* of the following hold:
  1 $x \in \mathbb{P}$
  2 $-x \in \mathbb{P}$
  3 $x = 0$.

Let's take a step back from this weird subset. What does this mean? It induces an **order** on $\mathbb{R}$.

(1) $x < y \iff$ (iff) $y - x \in \mathbb{P}$
(2) $x > y \iff x - y \in \mathbb{P}$.

Does this fulfill our intuition about order? Let's check a proposition, whose statement was fixed by Alex:

Proposition 1. *For $a > 0$. If $x > y$, then $ax > ay$.*

Proof. Blakeley suggested we begin by assuming $x > y$, i.e. $x - y \in \mathbb{P}$. Also, since $a > 0$, $a - 0 \in \mathbb{P} \implies a \in \mathbb{P}$. With some fixes from various individuals (Gabe at the end) we get that

$$\begin{aligned} a(x-y) &\in \mathbb{P} && \text{by closure (A12)} \\ ax - a \cdot (-y) &\in \mathbb{P} && \text{by distributing} \\ ax - ay &\in \mathbb{P} && \text{by what you've proved} \\ \implies ax &> ay && \text{by definition.} \end{aligned}$$

□

An important proof point was made here. We cannot start with $ax > ay$. This is our **goal**. We would love for it to work out and get $ax > ay$, but technically you can't start with that and manipulate it to get to the original expression.

Ok, so (A12) abides by our natural sense of order. But, which of the fields we mention does this eliminate? Turns out the only things left are $\mathbb{Q}$ and $\mathbb{R}$ (our intuitive sense of $\mathbb{R}$). Let's show an example of something that fails (A12).

Proposition 2. $\mathbb{Z} \pmod 2$ *fails (A12).*

Proof. Recall $\mathbb{Z} \pmod 2$ is $\{0, 1\}$ under $+$ mod 2 and $\cdot$ mod 2. □

Proof. Harry suggested beginning with the fact that $1 + 1 = 0 \implies -1 = 1$. If $1 \in \mathbb{P}$, then $-1 = 1$ is *also* positive, which contradicts trichotomy!

Here's another proof idea by Leo. We proved analytically that $1 > 0$. In other words, $1 \in \mathbb{P}$ since we proved that any system that abides (A1)-(A12). Then you can continue as we did above □

Notes on a lecture by Leo Goldmakher; written by Justin Cheigh.

More generally, $\mathbb{Z} \pmod p$ (for prime p) is a field that fails (A12). You will prove on your problem set that $\mathbb{C}$ also cannot be ordered. Ok, last two standing: $\mathbb{Q}$ and $\mathbb{R}$.

2. What distinguishes $\mathbb{R}$ from $\mathbb{Q}$?

Brainstorm time. Ben noted that $\pi \in \mathbb{R} \setminus \mathbb{Q}$. Here's a weird idea. How would you define π just in terms of our axioms? Some other numbers make sense. For example we could define $\frac{2}{3} := 2 \cdot \frac{1}{3}$. Sarah suggested that π is the element such that $\pi > 3.14$ and $\pi < 3.15$. Forrest suggested that we define π as the limit of a sequence of rationals. In other words, you can keep listing rationals (fractions) that get closer and closer to π, and in the limit it makes sense that this number might be π. As an alternate to a limit (whatever that is), it's clear that we would need to repeat this process infinitely many times, else it will still be a rational.

Ali asked a question: is there always a number between any two rationals? Miles suggested just taking the average (midpoint). That's guaranteed to be another rationals. One can iterate this process forever, which means between any two rationals there are **infinitely many rationals!**

Turns out this question of how to define π is almost a trick question! In other words, there is **no** way to define π using (A1)-(A12). This is a very impressive statement: how can we say there's no brilliant way to prove this? Well, $\mathbb{Q}$ abides by (A1) - (A12), yet π is not an element in $\mathbb{Q}$. Formally, suppose, for the sake of contradiction, that there's a way to prove π lives in a set that abides (A1)-(A12). A counterexample is $\mathbb{Q}$, since $\pi \notin \mathbb{Q}$.

3. Thinking about (A13)

(A13) will capture this general idea of a real number, allowing us to define *arbitrary* real numbers. What are examples of elements in $\mathbb{R}$ that aren't in $\mathbb{Q}$?

Proposition 3. $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.

Meta-Analytic. Suppose $\sqrt{2} \in \mathbb{Q}$. Thus, $\sqrt{2} = \frac{a}{b}$ for $a, b \in \mathbb{Z}_{>0}$ (positive integers). But this would mean that

$$2 = \frac{a^2}{b^2} \implies a^2 = 2b^2, \tag{3.1}$$

which tells us that a^2 is even (since $a^2 = 2k$ for some integer k. Here k is specifically b^2). This tells us that a is even (a is either even or odd. If a is odd then a^2 is also odd thus if a^2 is even then a is even by contrapositive).

So, a is even, which means we can write $a = 2m$ for some positive integer m. Let's plug this back into Equation 3.1:

$$\begin{aligned} a^2 &= 2b^2 \\ (2m)^2 &= 2b^2 \\ 4m^2 &= 2b^2 \\ 2m^2 &= b^2, \end{aligned}$$

which, using the same argument, tells us that b is even ($b = 2n$ for integer n). So, both the numerator and denominator are divisible by 2, so let's simplify and divide both sides by 2:

$$\sqrt{2} = \frac{a}{b} = \frac{2m}{2n} = \frac{m}{n},$$

where m, n are integers. But this means that we just wrote $\sqrt{2}$ as a fraction of 2 integers. **We just proved this means that m and n are both even**. So, divide by two again. And again. And again. We can repeat this process as many times as we want.

This tells us that a and b are divisible by arbitrarily high powers of 2. The only integers that are in fact divisible by arbitrarily high powers of 2 are just 0. So, $a = b = 0$, which means $\sqrt{2} = \frac{0}{0}$, a contradiction. $\square$

Proof. This is a meta-analytic proof that Leo came up with in high school. If $\sqrt{2} = \frac{a}{b}$, which means $2 = \frac{a^2}{b^2}$. This implies $b^2 | a^2$ (a^2 is divisible by b^2), which tells us $b | a \implies \sqrt{2} = \frac{a}{b}$ is an integer. However, $\sqrt{2}$ cannot be an integer, since it's certainly between 1.4 and 1.5. $\square$

Ok, intuition about axiom 13.

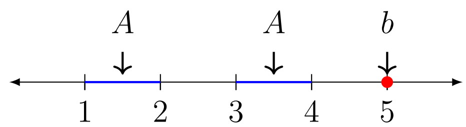
$$\text{We can think of } \sqrt{2} \text{ as the limit of all rationals that are } < \sqrt{2}.$$

(Axiom 13): If $A \subseteq \mathbb{R}$ and A has an upper bound, then A has a least upper bound, called the *supremum* of A and denoted $\sup(A)$.

This leads to a few definitions:

Definition (Upper Bound)**.** We say $b \in \mathbb{R}$ is an upper bound on $A \subseteq \mathbb{R}$ iff $b \geq x \; \forall x \in A$.

Here's an example of a set $A \subseteq \mathbb{R}$ and a potential upper bound b.



Here's the definition of least upper bound, given by Jon:

Definition (Least Upper Bound)**.** We say $\alpha \in \mathbb{R}$ is a *least upper bound* of $A \subseteq \mathbb{R}$ iff α is an upper bound on A and $\forall \beta \in \mathbb{R}$ that's an upper bound on A, $\alpha \leq \beta$. In other words, the least upper bound is an upper bound, and it is the least of all upper bounds.

Let's do a few meta-analytic examples. The interval $A = (0, 1)$ (doesn't include 0 or 1). Some upper bounds are $1, 2, 1000, \pi^\pi$. Also, $\sup(A) = 1$. Here's a rough idea of a proof. Suppose $1 - \epsilon$ is the least upper bound, for $\epsilon > 0$. Well, $1 - \epsilon < 1 - \epsilon/2 < 1$, so $1 - \epsilon$ is not an upper bound.

What about $A = [0, 1]$ (includes 0 and 1)? One potential upper bound is 2. But, $\sup(A)$ is still 1, since $1 \geq x \; \forall x \in A$, whether or not $\sup(A) \in A$ or not.