REAL ANALYSIS: LECTURE 4

SEPTEMBER 18TH, 2023

1. Preliminaries

Ok, so where were we? Last class we began listing properties (axioms) of $\mathbb{R}$, and we wish to continue until we *uniquely define* $\mathbb{R}$. To recap, here's the axioms we've written already:

(A1) $\exists + : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
(A2) $+$ is associative
(A3) $+$ is commutative
(A4) $\exists$ additive identity, denoted 0
(A5) $\exists$ additive inverses. We'll denote the additive inverse of x by $-x$. Notice the word "the" is only allowed since we proved additive inverses are unique.

We call any set G with an operation $+$ that satisfies (A1)-(A5) is called an **abelian group**. You will study this much more in abstract algebra. In fact, (A6) - (A10) is basically the exact repeat for an operation $\cdot$ (multiplication).

(A6) $\exists \cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
(A7) $\cdot$ is associative
(A8) $\cdot$ is commutative
(A9) $\exists$ multiplicative identity, denoted 1 (with $1 \neq 0$: otherwise $\mathbb{R}$ could be 0).
(A10) For every $x \neq 0, \exists$ a multiplicative inverse. We'll denote the multiplicative inverse of x by x^{-1} (or $\frac{1}{x}$).

Finally, we have a property connecting $+$ and $\cdot$, know as the distributive property:

(A11) Distributive property: $x \cdot (y + z) = x \cdot y + x \cdot z$.

Any set F with two operations $+$ and $\cdot$ that satisfy (A1) - (A11) is called a **field**.

Here Emily asked an interesting question: does (A11) tell us that (meta-analytically) multiplication is repeated addition, i.e. that $2 \cdot 2 = 2 \cdot (1 + 1) = 2 \cdot 1 + 2 \cdot 1 = 2 + 2$? In fact, it tells us even more! For example, $\pi \cdot e$ still somehow retains this connection with addition, though the intuition isn't as clear.

Ok, let's use these axioms to prove something analytically:

Proposition 1. *If S satisfies (A1) - (A11) (i.e. if S is a field), then*

$$x \cdot 0 = 0 \ \forall x \in S$$

Take 1: (False Proof!)

Proof. Suppose $\exists x \in S$ s.t. $x \cdot 0 \neq 0$. Choose any $y \in S$. Then

$$\begin{aligned} x \cdot 0 &\neq 0 & \\ x \cdot (y + -y) &\neq 0 & \text{by definition of additive inverse} \\ x \cdot y + x \cdot (-y) &\neq 0 & \text{by distributing} \\ x \cdot y + -x \cdot y &\neq 0 & \text{hmm...} \end{aligned}$$

but $xy + -(xy) = 0$ by definition of additive inverse. Ideally this would be the contradiction we wanted, but Annie realized that we can't assume (and never proved) $-(x \cdot y) = x \cdot -y$. In other words, we want to be able to "pull out" the negative sign, i.e. that $-y = -1 \cdot y$. Ok, let's try again. □

Take 2.0 (Yana's Correct Proof!):

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

Proof.

$$\begin{aligned}
x \cdot 0 &= x(0+0) && \text{since } 0 = 0+0 \\
x \cdot 0 &= x \cdot 0 + x \cdot 0 && \text{by distributing} \\
-(x \cdot 0) + x \cdot 0 &= (x \cdot 0 + x \cdot 0) + -(x \cdot 0) && \text{by adding additive inverses} \\
0 &= (x \cdot 0 + x \cdot 0) + -(x \cdot 0) && \text{definition of additive inverses} \\
0 &= (x \cdot 0) + (x \cdot 0 + -(x \cdot 0)) && \text{by associativity} \\
0 &= x \cdot 0 + 0 && \text{by definition of additive inverse} \\
0 &= x \cdot 0 && \text{by definition of additive identity.}
\end{aligned}$$

□

Notice that we use distributivity. Intuitively we *had* to use distributivity, since distributivity is the only axiom connecting addition and multiplication, and our proposition concerns the connection between the two (really, between the additive identity and multiplication). Here's a more rigorous way to see that distributivity is necessary in the proof of our proposition:

Example 1. Consider $S = \{0, 1\}$ where $+$ is addition mod 2 and $\cdot$ is such that

(1) $0 \cdot 0 = 1$
(2) $0 \cdot 1 = 0$
(3) $1 \cdot 0 = 0$
(4) $1 \cdot 1 = 1$

It turns out S as defined satisfies (A1) - (A10) but *fails* (A11) (check this yourself!). However here $0 \cdot 0 = 1 \neq 0$!

So, did we define $\mathbb{R}$? Nope, there's still lots of stuff that satisfy (A1)-(A11) (i.e. $\mathbb{R}$ isn't the only field). Here's some examples of fields.

(1) $\mathbb{R}$ under usual $+, \cdot$
(2) $\mathbb{Q}$ under usual $+, \cdot$
(3) $\mathbb{Z}$ (mod 2) under $+, \cdot$ mod 2
(4) $\mathbb{Z}$ (mod 7) under $+, \cdot$ mod 7

Here $\mathbb{Z}$ (mod 7) means the set $\{0, 1, 2, 3, 4, 5, 6\}$ and $a + b$ (mod 7) means add $a + b$ normally (if $a = 6, b = 4$ then $a + b = 10$) then subtract 7 until you get to something in the set $10 - 7 = 3 \in \mathbb{Z}$ (mod 7). Multiplication modulo 7 is exactly analogous. If $a = 6, b = 4$ then $a \cdot b = 24$ then subtract 7 three times to get to $24 - 7 - 7 - 7 = 3 \in \mathbb{Z}$ (mod 7), which means $a \cdot b$ (mod 7) $= 3$. The analogy here is "clock addition": if today is Monday what day is it in 10 days? One can literally count 10 days, but it's easier to know 10 (mod 7) $= 3$, which tells us that in 10 days it will be the same day it is 3 days from now (i.e. Thursday).

Ok, so we're not done defining $\mathbb{R}$ yet. Let's keep going.

2. Order Axiom

Recall our intuition about the next axiom has to do with relations between two arbitrary numbers. Specifically, given $x, y \in \mathbb{R}$, one of x or y is at least as large as the other. Formally, there is a **trichotomy**: exactly one of

(1) $x > y$
(2) $x = y$
(3) $x < y$

holds. We can't literally use this as (A12) since we have no idea what $>$ means, but let's try to capture it.

Intuition 1. What do $>$ and $<$ mean? Here's some initial thoughts:

(1) $x > y \iff x - y$ is positive
(2) $x < y \iff x - y$ is negative (i.e. $y - x$ is positive)
(3) $x = y \iff x - y = 0$.

This indicates that is suffices to define **positive**. Let's do this.

(A12): $\exists \mathbb{P} \subseteq \mathbb{R}$ s.t.

(i) $\mathbb{P}$ is closed under $+$ and $\cdot$

(ii) Trichotomy: $\forall x \in \mathbb{R}$ exactly one of the following hold

  (a) $x \in \mathbb{P}$

  (b) $-x \in \mathbb{P}$

  (c) $x = 0$

We can extend this to establish some notation. If $x \in \mathbb{P}$ then x is positive. If $-x \in \mathbb{P}$ then x is negative. $x > 0$ means $x \in \mathbb{P}$, and $x < 0$ means $-x \in \mathbb{P}$.

Now, our first theorem. Get ready for some real math:

Theorem 1. $1 > 0$.

Ok, before jumping into a proof let's brainstorm:

Intuition 2. Lexi suggested to use the fact that $1 \neq 0$. Thus by trichotomy, either $1 \in \mathbb{P}$ or $-1 \in \mathbb{P}$. Edith also noticed that, for every positive number x, $1 \cdot x \in \mathbb{P}$.

All this inspired Miles to come up with a proof. First, he restated a lemma Ben had mentioned earlier:

Lemma 1. *For all $x \in \mathbb{R}$ we have $-1 \cdot x = -x$.*

Taking this lemma on faith—it's on this week's problem set!—we have the following proof of our theorem (actually the proof below incorporates a correction of Miles' original proposal, due to Annie):

Proof of Theorem. Suppose $-1 \in \mathbb{P}$. By the above lemma, $-1 \cdot -1 = -(-1) = 1$ (since additive inverses are unique!). Since $\mathbb{P}$ is closed, $-1 \cdot -1 = 1 \in \mathbb{P}$, which contradicts trichotomy (we cannot have both $1 \in \mathbb{P}$ and $-1 \in \mathbb{P}$). Thus $-1 \notin \mathbb{P}$, so once again by trichotomy, $1 \in \mathbb{P}$. $\square$

Next time we'll see that $\mathbb{Z} \pmod 2$ doesn't satisfy (A12), i.e. it doesn't have an order.