MATH 350: LECTURE 7

1. LAST TIME

Recall we added our final axiom for defining the real numers:

(A13): If $S \subseteq \mathbb{R}$ is nonempty and bounded above, then $\sup S \in \mathbb{R}$, where \sup denotes the *least upper bound* of S.

This allows us to distinguish between \mathbb{Q} and \mathbb{R} , e.g.,

$$\sqrt{2} := \sup\{x \in \mathbb{R} : x^2 \le 2\}.$$

Note that this set is nonempty since 1 lives in it, and it is bounded above, e.g. by 2. Noam asked how we know that the supremum of this set actually squares to 2. You will explore this later on!

2. Greatest Lower Bound

(A13) seems like it should have a natural analog: the existence of a "greatest lower bound". Do we need another axiom for this? No! It turns out we can use (A13) to prove the existence of greatest lower bounds on sets that are bounded below.

Claim. If $S \subseteq \mathbb{R}$ is nonempty and bounded below, then \exists a greatest lower bound, or **infimum**, of S, denoted inf S, i.e., inf $S \in \mathbb{R}$.

Proof ideas:

• (Divij) Let S' be the set of all additive inverses of S. Then $\inf S = -\sup S'$.



• (Someone??) Create S' of all things $\leq S$. Hope sup $S' = \inf S$.

Date: September 26, 2024. Template by Leo Goldmakher. Divij's approach is very nice, and will appear on this week's problem set. Here we'll prove this using the second idea, because the proof will illuminate some useful proof mechanics.

Proof. Suppose S is nonempty and bounded below. Let $S' := \{x \in \mathbb{R} : x \leq a \ \forall a \in S\}$, i.e. the set of all lower bounds of S. $S' \neq \emptyset$ by hypothesis, and S' is bounded above by any $b \in S$ (we know such a b exists since $S \neq \emptyset$). Then (A13) $\Longrightarrow \sup S' \in \mathbb{R}$.



To do this, we need to show two things:

- (i) α is a lower bound of S
- (ii) α is at least as big as every lower bound of S

To show (ii), observe that $\alpha = \sup S' \implies \forall x \in S', x \leq \alpha$. If y is a lower bound of S, then $y \in S'$, hence $y \leq \alpha$.

[Note: Here we've only used that α is an upper bound on S'. We have not used the fact that it is the *least* upper bound. So we should expect to use the least-ness of α to show (i).]

Now let's prove (i): $\alpha = \sup S' \implies \alpha \leq \text{ any upper bound of } S' \implies \alpha \leq u \ \forall u \in S$ (since any $u \in S$ is an upper bound on S' by definition of S'). Thus, α is a lower bound of S. \Box

3. Defining $\mathbb{Z}_{pos}, \mathbb{Z}, \mathbb{Q}_{pos}, \mathbb{Q}$

We've defined \mathbb{R} to be any set satisfying (A1) - (A13). (You will show in an upcoming problem set that any set satisfying (A1) - (A13) is \mathbb{R} , up to renaming things). But what about other familiar sets, like the natural numbers or the rationals? Do we need new axioms for these? It turns out we can extract these sets from our definition of \mathbb{R} ! All we really need to do is define the positive integers \mathbb{Z}_{pos} . If we define \mathbb{Z}_{pos} , then we can define

- $\mathbb{Z} := \mathbb{Z}_{pos} \cup \{x : -x \in \mathbb{Z}_{pos}\} \cup \{0\}$
- $\mathbb{Q}_{pos} := \{ab^{-1} : a \in \mathbb{Z}_{pos}, b \in \mathbb{Z}_{pos}\}$

• $\mathbb{Q} := \mathbb{Q}_{pos} \cup \{x : -x \in \mathbb{Q}_{pos}\} \cup \{0\}.$

What is \mathbb{Z}_{pos} ? Evan proposed that it's all the numbers that are some number of ones added together, i.e.

$$\{1, 1+1, 1+1+1, \dots\}$$

To define this formally, we introduce the notion of **successor sets**.

Definition. A successor set is any $S \subseteq \mathbb{R}$ s.t.

(i) $1 \in S$ (ii) $n \in S \implies n+1 \in S$

Meta-analytic examples of successor sets: \mathbb{Z}_{pos} , \mathbb{Q} , {all multiples of 1/2}, \mathbb{R} ,.... These all work, but most of them except for \mathbb{Z}_{pos} have a lot of extra stuff in them. Informally, \mathbb{Z}_{pos} is the smallest/"purest" successor set. This inspires our formal definition of \mathbb{Z}_{pos} .

Definition. $\mathbb{Z}_{pos} := \bigcap_{\substack{\text{successor} \\ \text{sets } S}} S$

This means $Z_{pos} \subseteq S \forall$ successor sets S.

Nicole asked if something like \mathbb{F}_7 is a successor set. It kind of looks like one since it apparently satisfies both criteria given in the definition, but it is not a subset of \mathbb{R} , so it is not one.

4. INDUCTION

For those who have used **induction** to prove things before, the definition of successor set may have looked suspiciously like induction. This is not an accident; we use this definition of the positive integers in terms of successor sets to prove the validity of induction.

Proposition 4.1. Given assertions indexed by elements of \mathbb{Z}_{pos} , say $a(1), a(2), a(3), \ldots$ If

(i) a(1) is true and (ii) whenever a(n) is true, a(n + 1) is true,

then a(m) is true for all $m \in \mathbb{Z}_{pos}$.

Proof. Let $S := \{m \in \mathbb{Z}_{pos} : a(m) \text{ is true }\}$ be a set satisfying the two conditions above. Then S is a successor set. We claim $S = \mathbb{Z}_{pos}$. $S \subseteq \mathbb{Z}_{pos}$ by definition of S. $\mathbb{Z}_{pos} \subseteq S$ since \mathbb{Z}_{pos} is a subset of all successor sets S.

Here's an example of induction in action.

Proposition 4.2. 1 is the least element of \mathbb{Z}_{pos} .

Proof. Let a(n) be the assertion $n \ge 1$. Then a(1) is true since $1 \ge 1$. Suppose a(n) is true, i.e., $n \ge 1$. Then $n+1 \ge 1+1 > 1+0 = 1 \implies a(n+1)$ is true. By induction, a(m) true $\forall m \in \mathbb{Z}_{pos}$.