Foundations of Mathematics, Lecture 4

András Kornai

BMETE91AM35 Fall 2023-24

Constraction of numbers

- Last lecture: $\mathbb{N}$ by Peano Axioms
- Addition and multiplication defined inductively. We didn't do subtraction or division! Today we construct zero and negative numbers, to create $\mathbb{Z}$
- Let us begin with pairs of natural numbers (a, b) and define $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$
- What kind of relation is $\sim$? Equivalence!
- Integers will be the equivalence classes of this relation

$\mathbb{Z}$

- First let's prove that $\sim$ is indeed an equivalence relation
- Then let's define operations on these classes
- We need to prove that these are well defined
- We also need to prove that these have the requisite properties: (i) addition is commutative and associative; (ii) multiplication is commutative and associative; (iii) 0, 1 behave as they should
- We need to show that this is a conservative extension of $\mathbb{N}$
- Now we can define subtraction
- We need to prove that it's well-defined and behaves the way we want it to

$\mathbb{Q}$

- Same trick, but now we use $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ Prove that this is an equivalence
- Define the operations on the equivalence classes
- Prove that these definitions can be used
- We also need to prove that these have the requisite properties: (i) addition is commutative and associative; (ii) multiplication is commutative and associative; (iii) 0, 1 behave as they should
- We need to show that this is a conservative extension of $\mathbb{Z}$
- Now we can define division
- We need to prove that it's well-defined and behaves the way we want it to
- https://www.math.wustl.edu/~freiwald/310integers.pdf

Proof by induction

- CPZ Chapter 6
- In class: well-ordering, $\sum_{i=i}^{n} i$ and $\sum_{i=1}^{n} i^2$
- HW 4.1 Find, and prove, the formula for $\sum_{i=1}^{n} i^3$
- HW 4.2-5 = CPZ 6.18, 6.20, 6.22, 6.24

From $\mathbb{Q}$ to $\mathbb{R}$

- We need a new trick: Dedekind cuts
- Partitions (A,B) of $\mathbb{Q}$ that satisfy $\forall a \in A \, \forall b \in B \; a < b$ are called "Dedekind cuts"
- Example: let A be the set of negative rationals, B the set of nonnegative rationals
- In general, if $q \in \mathbb{Q}$, if A_q is defined as those rationals less than q and B_q as those $\geq q$ this will be a Dedekind cut
- These will model $\mathbb{Q}$, but these are not all Dedekind cuts!

$\sqrt{2}$

- Let $A = \{x \in \mathbb{Q} | x < 0 \vee x^2 < 2\},\ B = \{y \in \mathbb{Q} | y > 0 \wedge y^2 > 2\}$
- This is also a Dedekind cut, this will be $\sqrt{2}$!
- We need to prove that we can compute with Dedekind cuts just as well as with rationals
- For $p, q \in \mathbb{Q}$ prove $D_p + D_q = D_{p+q}$ and $D_p \cdot D_q = D_{pq}$
- Altogether Dedekind cuts make up $\mathbb{R}$
- Creating cuts from $\mathbb{R}$ will not add new elements, why?
- We can build $\mathbb{R}^*$ that is bigger than $\mathbb{R}$ but not this way

Archimedes

- $\mathbb{N}$ has natural ordering $1 < 2 < 3 < 4 \dots$
- This can be extended to $\mathbb{Z}$: $\dots - 4 < -3 < -2 < -1 < 0 < 1$
- This can be further extended to $\mathbb{Q}$: for $p, q, r, s > 0$ we have $p/q > r/s \Rightarrow ps > qr$, the rest need to be segregated by sign
- Archimedean Axiom: $\forall p, q > 0 \exists n \; qn > p$
- Important special case: $q = 1$ 'for every number there is a bigger integer'
- If we build the reals by Dedekind cuts, this is not an axiom but a theorem

Supremum

- Prove that among the rationals every set bound from above has a least upper bound (this is called the supremum of the set)
- From this it follows that between every two rationals there is an irrational and conversely, between every two irrationals there is a rational
- It also follows that there is no real number between 0 and the limit of the sequence $1/n$
- This last statement is equivalent to the Archimedean Axiom
- The converse is not true: we can make a larger set of (hyper)reals that also contain *infinitesimals*

Field axioms

- F is a *field*, if it has 0, 1, addition, subtraction, multiplication, and division except for 0, and these satisfy the usual identities
- There are fields with only finitely many elements!
- The smallest infinite field is $\mathbb{Q}$, this can be extended many ways
- $\mathbb{R}$ is not just a field, it is an *ordered* field (has $<$)
- The ordering has the usual properties, in particular *trichotomy*: of $a < b$ $a > b$ $a = b$ always exactly one is true
- Ordering is preserved under shifts: ifa $a < b$ then $a + r < b + r$ will hold for all r (and conversely)
- Recommended reading: Pugh__RealMathematicalAnalysis1-67.pdf

Practice

- In class: CPZ-bo3l p216
- Further HW: 5.1-7 = CPZ8.30,32,34,34,36,38,40