MAU11602
Lecture 28
2026-04-02

Constructing the rationals, correctly

Last lecture I defined the rational numbers to be lists of three natural numbers and defined addition on such lists, which was commutative and associative.
I could define multiplication similarly, and check that it's commutative and associative.
I could even check the distributive law. So we're done, right?
Unfortunately not. Are $(0, 0, 1)$ and $(1, 1, 1)$ equal? We'd like them to be, since both represent the rational number 0, but they're clearly not the same list.
We'd like additive inverses to exist, and (j, i, k) should be the additive inverse of (i, j, k), but then $(i + j, i + j, k)$ needs to be independent of i, j, and k.
There are two ways to solve this problem:
- Restrict to lists which have greatest common divisor 1 and at least one of the first two numbers equal to zero.
- Leave the set of triples as it is and define an equivalence relation where (i_1, j_1, k_1) is equivalent to (i_2, j_2, k_2) if $i_1 \cdot k_2 + k_1 \cdot j_2 = j_1 \cdot k_2 + k_1 \cdot i_1$. Then define natural numbers to be equivalence classes of such triples rather than individual triples.

Constructing the rationals, correctly, continued

- Restrict to lists which have greatest common divisor 1 and at least one of the first two numbers equal to zero.
- Leave the set of triples as it is and define an equivalence relation where (i_1, j_1, k_1) is equivalent to (i_2, j_2, k_2) if $i_1 \cdot k_2 + k_1 \cdot j_2 = j_1 \cdot k_2 + k_1 \cdot i_1$. Then define natural numbers to be equivalence classes of such triples rather than individual triples.

Either option will work, and both are somewhat painful.

If we choose the first option then addition and multiplication can't be defined as before. For example $(1, 0, 2) + (1, 0, 2)$ was defined to be $(4, 0, 4)$, but the greatest common denominator is now 4, which isn't allowed.

We need to add a final normalisation step, where we divide all three numbers by the greatest common denominator and then subtract off the minimum of the first two numbers from both of them.

This spoils our proof of associativity. The easiest way to fix this is to show that we don't have to perform normalisation after each operation. We can defer it to the end.

Constructing the rationals, correctly, concluded

- Restrict to lists which have greatest common divisor 1 and at least one of the first two numbers equal to zero.
- Leave the set of triples as it is and define an equivalence relation where (i_1, j_1, k_1) is equivalent to (i_2, j_2, k_2) if $i_1 \cdot k_2 + k_1 \cdot j_2 = j_1 \cdot k_2 + k_1 \cdot i_1$. Then define natural numbers to be equivalence classes of such triples rather than individual triples.

If we pick the second option then we still need to redefine addition and multiplication, since rational numbers are now sets of triples, not individual triples.

To add two numbers we choose members from the corresponding equivalence classes, add the two triples, and then take the equivalence class of the result.

This is only well defined if the equivalence class of the result is the same no matter which representatives we chose, which needs to be checked.

This turns out to be the same calculation as the one that shows we can defer normalisation.

Which option should you choose? If you're implementing rational arithmetic on a computer the first is better, but not much better. If you're proving theorems the second is better, but not much better.

Equivalence relations

I used equivalence relations to define the rational numbers, but what is an equivalence relation?

An *equivalence relation* on a set A is a relation R on A with the following three properties:

- Reflexivity: $\forall x.x \in A \rightarrow (x, x) \in R$.
- Symmetry: $\forall x.\forall y.(x, y) \in R \rightarrow (y, x) \in R$.
- Transitivity: $\forall x.\forall y.\forall z.(x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R$.

On any set equality is an equivalence relation. It is the strongest equivalence relation, in the sense that equality implies every other type of equivalence.

On any set there's also weakest equivalence relation, satisfied by all pairs of members.

Usually we're interesting in ones in between, like the equivalence relation on triples where (i_1, j_1, k_1) is equivalent to (i_2, j_2, k_2) if $i_1 \cdot k_2 + k_1 \cdot j_2 = j_1 \cdot k_2 + k_1 \cdot i_1$, which came up in the definition of the rational numbers.

For this relation identity and reflexivity are clear, but transitivity requires some work.

Equivalence classes

Given an equivalence relation on A we say that a subset B of A is an *equivalence class* of A with respect to that relation if B is non-empty, every two members of B are equivalent, and every member of A which is equivalent to a member of B is itself a member of B.

Every member of A belongs to some equivalence class, namely the set of all members of A which are equivalent to it.

You can, and should, check that that set is an equivalence class.

Every member of A belongs to at most one equivalence class.

This one I'll prove. Suppose $x \in B$ and $x \in C$, where B and C are equivalence classes in A for an equivalence relation R on A. If $y \in B$ then $(x, y) \in R$ so $y \in C$ and vice versa. So every member of B is a member of C and vice versa and therefore $B = C$.

The equivalence classes of A with respect to R form a set, a subset of $\mathcal{P}A$, by the Power Set axiom and Separation.

There's a surjective function from A to this set of equivalence classes with respect to R which takes each member of A to the equivalence class to which it belongs.

Functions on sets of equivalence classes

We often want to define functions from sets of equivalence classes to sets of equivalence classes. For example, if we define rational numbers as equivalence classes of triples of natural numbers then addition will be a function from ordered pairs of equivalence classes of triples to equivalence classes of triples.
We could also think of it as a function from equivalence classes of ordered pairs to equivalence classes, where pairs are equivalent if and only their left and right elements are equivalent.
We already have a function from pairs of triples to triples. Can we use this?
Suppose R is an equivalence relation on A, C is corresponding set of equivalence classes, and p is the function from A to C which takes each member to its equivalence class. Suppose S is an equivalence relation on B, D is corresponding set of equivalence classes, and q is the function from B to D which takes each member to its equivalence class. Suppose f is a function from A to B. Then there is a function g from C to D such that $q \circ f = g \circ p$ if and only if $(f(x), f(y)) \in S$ whenever $(x, y) \in R$.

Algebraic numbers

The way we proved the existence of irrational numbers can be used in many situations.
A real or complex number is called *algebraic* if it is a root of some non-zero polynomial with rational coefficients and is called *transcendental* otherwise.
Proving a particular number, like e and π, is transcendental is hard. Proving that there are transcendental numbers is much easier.
If x is algebraic then it satisfies some polynomial equation $c_n x^n + \cdots c_1 x + c_0 = 0$.
This equation is satisfied by only finitely many numbers, at most n of them, so there is a rational number d such there are no other roots within a distance d of x.
Define a relation between lists of rational numbers and real numbers satisfied by $(c_0, \ldots, c_n, d)$ and x if $c_n x^n + \cdots c_1 x + c_0 = 0$, and if $c_n y^n + \cdots c_1 y + c_0 = 0$ and $|x - y| < d$ imply $y = x$.
This relation is right total and right unique and the set of lists of rational numbers is countable, so the set of algebraic numbers is countable.
The set of real numbers is uncountable, so there must be real numbers which are not algebraic, i.e. transcendental numbers.

Arithmetic sets, intensional and extensional functions

Tarski's theorem gives an example of a subset of the natural numbers which is not arithmetic, but Tarski's theorem is hard.
Proving that there are sets which are not arithmetic is much easier.
A subset of the natural numbers is arithmetic if and only if there is a Boolean expression in Peano arithmetic which describes its members.
Every such expression has an encoding as a natural number.
So there's a right total and right unique relation between natural numbers and arithmetic sets satisfied by such encodings and the sets they encode.
The set of natural numbers is countable so the set of arithmetic sets is countable.
But Cantor's theorem tells us the set of all subsets of the natural numbers is uncountable, so there must be some subset which is not arithmetic.
A similar argument shows us that there must be extensional functions which don't correspond to any intensional function.
In other words, the Junior Cert curriculum lied to you. Functions are not rules, they are sets of ordered pairs.

Axioms of set theory

I introduced axioms gradually, so I'll list what we have so far:
- Extensionality: Equality of sets is defined by membership.
- Separation: Boolean expressions can be used to define subsets.
This axiom has several other names, including Specification and Restricted Comprehension.
- Elementary sets: Sets with zero, one or two specified members exist.
This is usually called Pairing and limited to sets with two specified members.
You can get the case of one member from this, and get the case of zero members from Separation and Infinity!
- Union: The union of a set of sets exists.
- Replacement: Boolean expressions can be used to define functions with given domain (but not codomain).
- Infinity: The natural numbers form a set.
- Power set: For any set its subsets form a set.
Strictly speaking Separation and Replacement are rules of inference rather than axioms. They are often called axiom schemata.

Zermelo-Fraenkel

The axioms on the previous slide, excluding Replacement, are Zermelo set theory.
A more commonly used system is Zermelo-Fraenkel set theory which makes the following changes:
- It adds Replacement.
- It changes Extensionality to forbid atoms (urelements).
- It adds an additional axiom, called Foundation or Regularity.

The first of these is fine as long as you never want to use set theory outside of mathematics.
The second is never really needed outside set theory itself, but sometimes useful and seems intuitive.
The third is frankly bizarre.

Foundation

The Axiom of Foundation, also known as Regularity, is

$$\forall A.((\exists B.B \in A) \rightarrow (\exists B.(B \in A) \wedge \neg(\exists x.(x \in A \wedge x \in B)))).$$

In words, if a set has a member then it has a member which shares no members with it.
If you find this intuitive I would like to know why, because I've never seen anyone give a reason for believing this is true.
I have seen people give arguments claiming that it's harmless and useful.
The argument for harmlessness is that if Zermelo-Fraenkel is consistent without Foundation then it is consistent with Foundation.
But if Zermelo-Fraenkel is consistent without Foundation then it is also consistent with the negation of Foundation.
So relative consistency works equally well as a reason for accepting or rejecting the axiom!

Foundation, continued

Most arguments for the usefulness of Foundation are also suspect.
A surprisingly common argument is that it's needed to prevent the existence of a set of all sets.
The bit of this which is true is that it does imply that that there is no set of all sets.
But we already saw that the other axioms already imply this.
We would only need a new axiom to prevent a set of all sets if the other axioms were consisent with its existence, but then we wouldn't add the axiom, because the only reason we avoid a set of all sets is to maintain consistency.
The idea that you add axioms to gain consistency fundamentally misunderstands the way logic works. Adding or strengthening axioms or rules of inference can never make an inconsistent system consistent. That can only be done by removing or weakening axioms or rules of inference.
Consistency is the reason we weakened Comprehension to Separation, not a reason to add Regularity.
There are things Regularity *is* useful for, but only within set theory, not outside of it.