Bob the Algebraic Builder

Constructing Our Everyday Number Systems from Principles

Ethan Pronovost - Ma 0

September 7, 2017

0 Preface

In the last chapter of the course, you get a glimpse into *axiomatic construction.* It's a way of rigorously defining something that we're all intuitively familiar with, but that might otherwise be hard to concretely define. I think a cool part of math is how we can formalize everyday intuition, and then go on to prove more things beyond our intuition.

We use the *Peano Axioms* to construct the set of natural numbers. But can we do more? You've probably heard of other sets of numbers, like the integers ($\mathbb{Z}$), rationals ($\mathbb{Q}$), reals ($\mathbb{R}$), and complex numbers ($\mathbb{C}$). How can we similarly construct these number systems in a rigorous way?

This paper outlines the algebraic process of going from $\mathbb{N}$, to $\mathbb{Z}$, to $\mathbb{Q}$, and points you in the direction of where to do to construct $\mathbb{R}$. Along the way, I do have to use some advanced terminology (the worst probably being *commutative semi-ring with identity*), but don't worry too much about that. Instead, try to focus on the bigger picture of what exactly underpins the number systems we use every day.

1 The Peano Axioms

tl;dr The Peano Axioms define the natural numbers, a sequence of things that form a commutative semi-ring with identity.

1.1 A Sequence of Things

When you get to the last chapter of the course, you'll meet the *Peano Axioms*. These can seem intimidating at first, but let's consider their deeper meaning.

The first 9 axioms lay out the basic framework of a *sequence* of things. Indeed, a generic sequence of elements from any set X is simply a mapping $\mathbb{N} \to X$ that sends every natural number i to the i^{th} element of the sequence.[1]

1.2 Some Special Binary Operators

Given this framework, we then describe two useful binary operations between elements of this sequence, based on their location in the sequence (which is basically the value of the natural number). These two operations, *addition* and *multiplication*, each have several special properties:

- Identity Element: 0 and 1 for addition and multiplication, respectively.
- Commutativity: $a + b = b + a$, and likewise for multiplication

[1] Here we use 0-indexed sequences, so the first element is at location 0, then 1, 2, etc...

- Associativity: $a + (b + c) = (a + b) + c$, and likewise for multiplication

These three properties are very important, because they give us a lot more power than generic binary operators. To see what I mean by this, consider addition as a function which takes two inputs, and returns a single output. In computer pseudo-code,

$$\text{def } add(x, y) = x + y$$

As a simple example, consider simplifying $3 + 2x + 5 + 4x$ to $6x + 8$. Because we know that $add(x, y) = add(y, x)$ (commutativity), and that $add(x, add(y, z)) = add(add(x, y), z)$ (associativity), we can do the following reduction:

$$\begin{aligned}
&add(add(add(3, 2x), 5), 4x)\\
&= add(add(add(2x, 3), 5), 4x)\\
&= add(add(2x, add(3, 5)), 4x)\\
&= add(add(2x, 8), 4x)\\
&= add(add(8, 2x), 4x)\\
&= add(8, add(2x, 4x))\\
&= add(8, 6x)\\
&= add(6x, 8)
\end{aligned}$$

The whole point of this is to demonstrate the underlying assumptions we use to perform algebraic simplification. Now consider replacing our function add with def $f(x) = x^2 - y$, which satisfies none of the three properties above. Clearly, reducing such compound expressions like $f(f(f(3, 2x), 5), 4x)$ to a single call of f suddenly gets a lot more complicated: you have to evaluate the function at each step, instead of simply playing with the inputs. While this is okay when we know what f does, if it's instead a black box, we're stuck, unable to simplify anything.

1.3 Playing Nicely Together

If you've looked at the chapter notes, there's one more key property that I haven't mentioned yet: *distributivity*. This last one isn't a property of a single operation, but of a pair of operations that play nicely together:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Given the axiomatic definition of multiplicaiton,

$$a \cdot S(b) = a + a \cdot b$$

, this may seem obvious. But don't take it for granted! For example, in the above example I lied when I said that commutativity and associativity let us simplify $3 + 2x + 5 + 4x$ down to $6x + 8$. Consider the step of going from $add(2x, 4x)$ to $6x$. What we're really doing is

$$(2 \cdot x) + (4 \cdot x) = (2 + 4) \cdot x = 6 \cdot x.$$

Again, this may seem unnecessarily detailed, but is to simply point out how important these underlying properties are.

1.4 Classifying this Structure

In Abstract Algebra, we have a name for this type of structure: a *set* with two binary operations that are both commutative, associative, and have identity, and are distributive between them. We call it a *commutative semi-ring with identity*. A *semi-ring* requires distributivity and associativity, and then we throw on the other two adjectives to complete the picture.

1.5 What's Missing?

There's one key thing that's missing from this picture: *inverses!* You proved this in the last assignment, showing that for any $a, b \in \mathbb{N}$, $a + b = 0$ iff $a = 0 = b$. We don't need inverses to work inside the natural numbers, but the moment we start introducing them we gain a whole lot more structure.

2 The Integers

tl;dr Including additive inverses gives us the integers, and a 10x power up.

2.1 Additive Inverses

Let's do the easier operation first: addition. To expand $\mathbb{N}$ have additive inverses, we define a new set $\mathbb{Z}$, called the *integers*. Just like how elements in $\mathbb{N}$ could be either 0 or $\mathrm{S}(n)$ for some $n \in \mathbb{N}$, we can divide the elements of $\mathbb{Z}$ into three cases, based off of the natural numbers:

- 0
- $\mathrm{Pos}(n)$ for some $n > 0 \in \mathbb{N}$
- $\mathrm{Neg}(n)$ for some $n > 0 \in \mathbb{N}$

What's more, we can define addition and multiplication for this set in terms of those for the natural numbers. I'll leave it to you to come up with what those definitions would be.

2.2 Classifying the Structure

Our new numerical set, $\mathbb{Z}$, now features additive inverses. Given all the other properties still hold, we call this a *commutative ring with identity* in Abstract Algebra. As we rarely deal with non-commutative rings, or rings without identity, mathematicians will commonly simply refer to this as a *ring*.

2.3 What This Gives Us

There's a whole field of study (surprisingly named *Ring Theory*) dedicated to the study of such structures. It turns out that, beyond being commutative and having a multiplicative identity, the integers are even more special. They form a *Euclidian Domain*, which requires several additional features:

- If you multiply two non-zero numbers together, you will never get 0
- There exist *prime numbers*.[2]
- We can use the *Euclidian Algorithm* to find the *greatest common divisor* of any two numbers.

With these properties, we can do all sorts of things. One of the most important is solve a linear system of equations: find x and y such that $a \cdot x + b \cdot y = c$ for some fixed a, b, c. Restricted to the integers, there could be either no solutions (e.g. if $a = 2 = b$ and $c = 1$), or infinitely many solutions (e.g. if $a = 2, b = 3, c = 1$).

Being able to solve these sorts of equations is a key stepping stone in the usefulness of our number systems. What's more, we can further extend our notion of rings to another category, called *modules*, which allow us to solve systems of equations (think solving matrices). This line of study is only tangential to the actual construction of our number systems, so I won't go into further detail. The key point is that, by simply including additive inverses, we're able to do a ton more with the integers.

[2] There are many ways to define these, but one is to say that for a prime number p, and any two elements a, b, then $p \mid a \cdot b$ iff $p \mid a$ or $p \mid b$. Another way is to say that the only elements that divide p are 1 and itself. Both of these statements only hold up to sign (i.e. we don't count $-p$ dividing p as unique from p dividing itself).

3 The Rationals

tl;dr Multiplicative inverses are more complicated, but open the floodgates for more advanced study.

3.1 Multiplicative Inverses

Okay, so now for a trickier step: multiplicative inverses. Above, for the additive case, we simply made a "second copy" of $\mathbb{N}$ that we called the "negatives". In other words, we simply took every element of $\mathbb{N}$, and gave it an inverse; no more work was needed.

Things aren't quite this straight forward when including multiplicative inverses. To see this, let's try what we did before. Similar to how you could say we "created" $\text{Neg}(n)$ for every $\text{Pos}(n)$, let's now have our normal integers, $\text{Int}(z)$ for some $z \in \mathbb{Z}$, and inverses $\text{Inv}(z)$, new magical elements with the special property that $\text{Int}(z) \cdot \text{Inv}(z) = \text{Int}(1)$.

We've added inverses! But there's has to be a catch. Going all the way back to the natural numbers, even before commutativity and associativity, addition and multiplication have always been *well defined*: for any two numbers in the set, their sum and product are both also numbers in that set. But what's $\text{Inv}(2) + \text{Inv}(3)$? Suddenly, we've broken everything.[3]

3.2 Fractions

We added some multiplicative inverses, and broke everything. So to fix it, we're gonna add a whole lot more stuff. Concretely, we're gonna construct a *field of fractions*: a set based off of $\mathbb{Z}$, with elements of the form

$$\left\{ \frac{a}{b}, \quad a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

Similar to how we could leverage addition and multiplication in the natural numbers to define similar operations in the integers, we can do so again to define addition and multiplication on this new set, called the *rationals* $\mathbb{Q}$ (since everything is a ratio of two integers). The complication here is that representations of an element are no longer unique: we can have duplicate factors in the numerator and denominator. That's why in chapter 4, you would have to specify "with no common factors"; it can be shown that every such fraction has a unique representation in lowest terms.

With this structure, inverses simply flipping the top and bottom. We've added a lot more elements[4], but now everything has an additive inverse, and every non-zero number has a multiplicative inverse as well.

3.3 Classifying the Structure

Adding multiplicative inverses makes our new number set a *field*. Once again, there's a whole world of mathematics dedicated to the subject, with active ongoing research.

4 And Beyond!

4.1 Doing it in Practice

Everything we've done so far has been very systematic, very *programmatic*. To see the constructions of the naturals, integers, and rationals in code, you can checkout my repo here. Don't worry if you don't understand all the programming aspects of it. You should be able to recognize some of the key concepts, written out in Scala.

Not surprisingly, doing the theoretically-pure construction in practice is rather impractical. Because of the recursive definition of the natural numbers, we quickly hit stack overflows when using any large numbers,

[3] rip

[4] Although the whole set of $\mathbb{Q}$ is still only countably infinite, so have we really made it bigger at all?

or any reasonable amount of precision in fractions. Turns out there's a reason decimal (or binary or hex) representation is useful. Nonetheless, the fact that this number system even *works* is pretty cool.

4.2 There's a Course for That!

Interested in rings and fields, and want to learn more? I skimmed over a year's worth of study to just gain introductory knowledge in Algebra. If you want to learn more (or are a math major and have no other choice), consider taking Ma 5.

Want to skip all this algebra talk and get *real*? It's a non-trivial step to go from $\mathbb{Q}$ to $\mathbb{R}$. You'll look at this next step in Ma 1a, and again - if you're a math major - in Ma 108a.

Think all of this is boring? There's still completely different fields of math! Checkout Ma 2, Ma 3, Ma 6 (a common favorite), or Ma 109 for other subjects in mathematics.

4.3 A Meme