Math 108a Professor: Padraic Bartlett

Lecture 1: Fields, Informally

Week 0 *UCSB 2013*

1 The Real Number System

The real numbers, denoted $\mathbb{R}$, have a lot of different definitions. The most common is probably the "infinite decimal sequence" definition, which we state here:

Definition. Suppose that a_0 is some natural number (i.e. an element of $\mathbb{N}$), and $a_1, a_2, a_3, \ldots$ are an infinite sequence of numbers all from the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Then we can form a **real number using decimal notation** by stringing these objects together, in the way you're used to:

$$a_0.a_1a_2a_3a_4a_5a_6a_7\ldots$$

For example, $1/3$ would be expressed as $0.3333333\ldots$, where a_0 is equal to 0 while the objects $a_1, a_2, a_3\ldots$ are all equal to 3. If we allow ourselves to possibly prefix any of these strings with a $-$, we can express **any** real number using this decimal notation: i.e. the elements of $\mathbb{R}$ are precisely the strings that we can write using these rules.

(To stop strings from being ambigious, we consider things like $.02999999\ldots$, where the 9's are repeated forever, to be the same thing as $.03$. There is a much deeper and more interesting way of defining the real numbers that makes this feel less artificial, but that could take an entire class on its own!)

There are two operations on the real numbers that we start studying from the start of elementary school: addition ($+$) and multiplication ($\cdot$.) These operations satisfy a number of properties that you may be familiar with: for example, you know that adding 0 to any number doesn't change that number, and that the order in which we multiply things doesn't matter. We list many of these properties here:

- **Closure($+$)**: $\forall a, b \in \mathbb{R}$, we have $a+b \in \mathbb{R}$.
- **Identity($+$)**: $\exists 0 \in \mathbb{R}$ such that $\forall a \in \mathbb{R}$, $0 + a = a$.
- **Commutativity($+$)**: $\forall a, b \in \mathbb{R}, a + b = b + a$.
- **Associativity($+$)**: $\forall a, b, c \in \mathbb{R}, (a + b) + c = a + (b + c)$.
- **Inverses($+$)**: $\forall a \in \mathbb{R}, \exists$ a unique number$-a \in \mathbb{R}$ such that $a + (-a) = 0$.
- **Closure($\cdot$)**: $\forall a, b \in \mathbb{R}$, we have $a \cdot b \in \mathbb{R}$.
- **Identity($\cdot$)**: $\exists 1 \in \mathbb{R}$ such that $\forall a \in \mathbb{R}$, $1 \cdot a = a$.
- **Commutativity($\cdot$)**: $\forall a, b \in \mathbb{R}, a \cdot b = b \cdot a$.
- **Associativity($\cdot$)**: $\forall a, b, c \in \mathbb{R}, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Inverses($\cdot$)**: $\forall a \neq 0 \in \mathbb{R}, \exists$ a unique number$a^{-1} \in \mathbb{R}$ such that $a \cdot a^{-1} = 1$.

- **Distributivity$(+,\cdot)$** : $\forall a,b,c \in \mathbb{R}, (a+b)\cdot c = (a\cdot c)+(b\cdot c)$

Something you may have noticed in the list above is that they we've left off many useful properties of the real numbers! For example, a property that we didn't list above, but that seems pretty important, is the following:

- **New property**?(+) : $\forall a \in \mathbb{Z}, 0\cdot a = 0.$

Another property that we omitted above, is the following:

- **Other new property**?(+) : $\forall a \in \mathbb{Z}.(-a) = (-1)\cdot a.$

Given these properties, a natural question we can ask is the following: should we have listed it above? Or, if we already have the properties we've listed earlier, are these additional properties **superfluous**: i.e. can we prove that they're true just using the list of properties we have above?

As it turns out, we **don't** need to add these properties to our list! In fact, if we use the eleven listed properties that we gave for the real numbers, we can deduce that these two new properties are true as well. We do this here:

Claim 1.

- **New property**?*(+)* : $\forall a \in \mathbb{Z}, 0\cdot a = 0.$

Proof. Take any $a \in \mathbb{R}$. Because of the closure$(\cdot)$ property, we know that $0\cdot a$ is also a natural number. Trivially, we know that

$$0\cdot a = 0\cdot a.$$

We also know that 0 is an additive identity: therefore, in specific, we know that $0 = 0+0$, and therefore that

$$0\cdot a = (0+0)\cdot a.$$

Applying the distributive property then tells us that

$$0\cdot a = (0+0)\cdot a = (0\cdot a)+(0\cdot a).$$

Now, we can use the inverse(+) property to tell us that because $0\cdot a$ is a natural number, we also know that there is some other natural number $-(0\cdot a)$ such that $(0\cdot a)+(-(0\cdot a)) = 0$. Then, if we add this to both sides of our equality above (which we can do and still get integers because of closure,) we get

$$(0\cdot a)+(-(0\cdot a)) = ((0\cdot a)+(0\cdot a))+(-(0\cdot a)).$$

Applying the inverse property to the left hand side tells us that it's 0; applying the associative property to the right side tells us that

$$0 = ((0\cdot a)+(0\cdot a))+(-(0\cdot a)) = (0\cdot a)+((0\cdot a)+(-(0\cdot a))) = (0\cdot a)+0 = (0\cdot a),$$

by applying first the inverse property and then the additive identity property to make the $+0$ go away. Therefore, we've proven that for any $a \in \mathbb{R}$, we have

$$0 = 0 \cdot a.$$

□

We continue to our second proof:

Claim 2.

- **Other new property**?$\boldsymbol{(+\ )}: \forall a \in \mathbb{Z}, (-a) = (-1) \cdot a.$

Proof. By the multiplicative identity property, we know that $1 \in \mathbb{Z}$; by the additive inverse property, we then also know that $-1 \in \mathbb{Z}$ and that

$$0 = 1 + (-1).$$

Using closure, distributivity, and the multiplicative identity property, we can take any a and multiply it by the left and right hand sides above:

$$0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a).$$

Using our result above, we know that $0 \cdot a = 0$, and therefore that

$$0 = a + (-1) \cdot a).$$

Using the additive inverse property and closure, we know that $-a$ is an integer and that we can add it to the left and right hand sides above:

$$(-a) + 0 = (-a) + (a + (-1) \cdot a).$$

Using the additive identity property at left and associativity/inverses/the additive identity at right gives us

$$(-a) = ((-a) + a) + (-1) \cdot a = 0 + (-1) \cdot a = (-1) \cdot a,$$

whiish is what we claimed. □

These proofs should hopefully persuade you of a few things. One: it's possible to do an awful lot with the properties listed above. In fact, we find these properties so valuable that we call objects that satisfy these properties **fields**! We will discuss these objects in more depth in our next lecture.

Two it can be really fussy to work with things like field axioms. Throughout most of your UCSB courses, we'll generally assume that things like arithmetic work how we think they do, and not bother too much with citing these properties; usually, we'll keep our focus on the stranger/weirder definitions that each class specializes in, rather than these basic arithmetical definitions. Our next class will likely be the only time we delve this deeply into these axioms.

Three: it does bear noting that the proofs above is cool in a few ways that aren't immediately obvious. Specifically, we showed that $0 \cdot a = 0$, and that $(-a) = (-1) \cdot a$, using **only** these properties, and not anything special to $\mathbb{R}$. Therefore, we know that the same result will be true for **anything** that also satisfies these properties! In particular, we've proven that in any **field**, both of these new properties must hold. This illustrates another thing that it's always worth paying attention to in your proofs: what facts are you specifically using in a proof? Do you need all of them? Can you extend your proof to covering many other situations, because you only care about a few properties and not the details of the object you're studying? (Keeping this in mind is one of the bigger leaps I made when switching from undergraduate-level research to graduate-level mathematical research.)