Math/CS 103 Professor: Padraic Bartlett

Minilecture 3: Fields

Week 2 *UCSB 2014*

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

Given this property, 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, is this additional property **superfluous**: i.e. can we prove that it's true just using the list of properties we have above?

As it turns out, we **don't** need to add this property to our list! In fact, if we use the eleven listed properties that we gave for the real numbers, we can deduce that this new property is 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

$$0 = 0 \cdot a.$$

□

2 Examples of Fields

We've defined fields, and one example ($\mathbb{R}$) of them. Are there other examples?

Some careful thought will persuade you that $\mathbb{Q}$, the set of rational numbers, is a field. We are not going to study these objects in this class. Instead, I want to look at **finite** fields: i.e. fields with only finitely many elements!

At first, it may be rather surprising that finite fields exist. So: an example!

Definition. The set $\mathcal{C}$, of "clock numbers," is defined along with an addition operation $+$ and multiplication operation $\cdot$ as follows:

- Our set is the numbers $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.
- Our addition operation is the operation "addition mod 12," or "clock arithmetic," defined as follows: we say that $a + b \cong c \mod 12$ if the two integers $a + b$ and c differ by a multiple of 12. Another way of thinking of this is as follows: take a clock, and replace the 12 with a 0. To find out what the quantity $a + b$ is, take your clock, set the hour hand so that it points at a, and then advance the clock b hours; the result is what we call $a + b$.

  For example, $3 + 5 \equiv 8 \mod 12$, and $11 + 3 \equiv 2 \mod 12$. This operation tells us how to add things in our set.
- Similarly, our multiplication operation is the operation "multiplication mod 12," written $a \cdot b \cong c \mod 12$, and holds whenever $a+b$ and c differ by a multiple of 12. Again, given any pair of numbers a, b, to find the result of this "clock multiplication," look at the integer $a \cdot b$, and add or take away copies of 12 until you get a number between 0 and 11.

  For example, $2 \cdot 3 \equiv 6 \mod 12$, $4 \cdot 4 \equiv 4 \mod 12$, and $6 \cdot 4 \equiv 0 \mod 12$.

We often will denote this object as $\langle \mathbb{Z}/12\mathbb{Z}, +, \cdot \rangle$, instead of as $\mathcal{C}$.

This is not a field. To see this, first show that 1 is the multiplicative identity of this field: this is not very hard, and is a good exercise to make sure you understand what's going on. Now, because 1 is the multiplicative identity, we know that if this is a field, any element $x \in \mathbb{Z}/12\mathbb{Z}$ should have a multiplicative inverse x^{-1} that we can multiply x by to get to 1.

However, you can check that no such multiplicative inverse exists for 2. This is not hard to see: take any other element y in $\mathbb{Z}/12\mathbb{Z}$, and multiply 2 by y: you get $2y$, an even integer. Adding or subtracting multiples of 12 to $2y$ will not change this property: because both 12 and $2y$ are even, the result of these operations will always be even.

1, however, is not an even number. Therefore, there is no way for $2y$ to be equal to 1, no matter what y we pick from our set. Therefore, 2 has no multiplicative inverse!

However, some small variations on this object **are** fields:

Definition. The object $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle$,i.e.s defined as follows:

- Your set is the numbers $\{0, 1, 2, \ldots n - 1\}$.

- Your addition operation is the operation "addition mod n," defined as follows: we say that $a + b \cong c \mod n$ if the two integers $a + b$ and c differ by a multiple of n.

  For example, suppose that $n = 3$. Then $1 + 1 \equiv 2 \mod 3$, and $2 + 2 \equiv 1 \mod 3$.

- Similarly, our multiplication operation is the operation "multiplication mod n," written $a \cdot b \cong c \mod n$, and holds whenever $a + b$ and c differ by a multiple of n.

  For example, if $n = 7$, then $2 \cdot 3 \equiv 6 \mod 7$, $4 \cdot 4 \equiv 2 \mod 7$, and $6 \cdot 4 \equiv 3 \mod 7$.

There are many values of n for which this is always a field! On the homework, you are asked to prove that these are fields iff We run one sample calculation here:

Claim 2. *$\langle \mathbb{Z}/5\mathbb{Z}, +, \cdot \rangle$ is a field.*

Proof. So: we're working with the set $\{0, 1, 2, 3, 4\}$, with the operations $+$ and $\cdot$ taken mod 5.

We first note that the operations $+, \cdot$ are closed. This is because given any pair of numbers in $\{0, 1, 2, 3, 4\}$, their sum and product are positive integers. If we take away copies of 5 one-by-one from any positive integer, we must eventually land in the set $\{0, 1, 2, 3, 4\}$, as it is impossible to subtract 5 from a positive integer that is not in this set (i.e. an integer greater than or equal to 5) and get a negative integer. (If you don't see why, draw a number line and try "subtract copies of five one by one" algorithm with some sample numbers!)

We also note that the commutativity, associativty and distribuitivity axioms all hold. To see this, notice that before taking the mod operation, our $+$ and $\cdot$ operations are precisely the same as those for $\mathbb{R}$; therefore, before applying mods, these two operations preserve these properties.

So: all of these properties are equality statements (i.e. $(a + b) + c = a + (b + c)$). These statements all hold before we apply the mod operation, because they hold in $\mathbb{R}$. Therefore, when we apply the mod operation to both sides, we're applying it to the same thing on both sides! Because we're starting from the same number on both sides when we perform our "add or take away copies of 5" algorithm, we can't possibly get these two sides to go to different numbers in $\{0, 1, 2, 3, 4\}$: we're starting from the same place and performing the same algorithm that always has a unique output! (If you don't see why our mod algorithm of "add or take away multiples of 5 until you are in the set $\{0, 1, 2, 3, 4\}$ always has the same output from any set input, prove this to yourself.) Therefore, we preserve these axioms.

To see the identity and inverse properties for $+$ and $\cdot$, consider the following addition and multiplication tables:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Notice how in the 0-row of the addition table, adding 0 to any element doesn't change that element. Therefore 0 is an additive identity! Similarly, notice that there is a 0 in every row and column in the addition table: this means that given any element in $\mathbb{Z}/5\mathbb{Z}$, there is some other element we can add to it to get to 0. Therefore, we have additive inverses.

As well, notice how in the 1-row of the multiplication table, multiplying 1 by any element doesn't change that element. Therefore, 1 is a multiplicative identity. Similarly, notice that there is a 1 in every row and column of the multiplication table not corresponding to a 0: this means that given any element in $\mathbb{Z}/5\mathbb{Z}$, there is some other element we can multiply by it to get to 1. Therefore, we have multiplicative inverses. □

So this is a field! A field with **finitely many elements,** which is weird.