Math 4111
September 16, 2020 Lecture

Steven G. Krantz

September 16, 2020



Figure: This is your instructor.

APPENDIX: Construction of the Real Numbers

There are several techniques for constructing the real number system $\mathbb{R}$ from the rational numbers system $\mathbb{Q}$. We use the method of Dedekind (Julius W. R. Dedekind, 1831–1916) cuts because it uses a minimum of new ideas and is fairly brief.

The number system that we shall be constructing is an instance of a *field* (the complex numbers, in the next lecture, also form a field). The definition is as follows:

Definition

A set S is called a *field* if it is equipped with a first binary operation (usually called addition and denoted "+") and a second binary operation (called multiplication and denoted "$\cdot$") such that the following axioms are satisfied (Here A stands for "addition," M stands for "multiplication," and D stands for "distributive law."):

A1. S is closed under addition: if $x, y \in S$ then $x + y \in S$.

A2. Addition is commutative: if $x, y \in S$ then $x + y = y + x$.

A3. Addition is associative: if $x, y, z \in S$ then $x + (y + z) = (x + y) + z$.

A4. There exists an element, called 0, in S which is an additive identity: if $x \in S$ then $0 + x = x$.

A5. Each element of S has an additive inverse: if $x \in S$ then there is an element $-x \in S$ such that $x + (-x) = 0$.

M1. S is closed under multiplication: if $x, y \in S$ then $x \cdot y \in S$.

M2. Multiplication is commutative: if $x, y \in S$ then $x \cdot y = y \cdot x$.

M3. Multiplication is associative: if $x, y, z \in S$ then $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

M4. There exists an element, called 1, which is a multiplicative identity: if $x \in S$ then $x \cdot 1 = x$.

M5. Each nonzero element of S has a multiplicative inverse: if $0 \neq x \in S$ then there is an element $x^{-1} \in S$ such that $x \cdot (x^{-1}) = 1$. The element x^{-1} is sometimes denoted $1/x$.

D1. Multiplication distributes over addition: if $x, y, z \in S$ then

$$x \cdot (y + z) = x \cdot y + x \cdot z\,.$$

Definition

Let $\mathbb{Q}$ be the rational numbers. A *cut* is a subset $\mathcal{C}$ of $\mathbb{Q}$ with the following properties:

- $\mathcal{C} \neq \emptyset$
- If $s \in \mathcal{C}$ and $t < s$ then $t \in \mathcal{C}$
- If $s \in \mathcal{C}$ then there is a $u \in \mathcal{C}$ such that $u > s$
- There is a rational number x such that $c < x$ for all $c \in \mathcal{C}$

You should think of a cut $\mathcal{C}$ as the set of all rational numbers to the left of some point in the real line. Since we have not constructed the real line yet, we cannot define a cut in that simple way; we have to make the construction more indirect. But if you consider the four properties of a cut, they describe a set that looks like a "rational halfline."

Notice that, if $\mathcal{C}$ is a cut and $s \notin \mathcal{C}$, then any rational $t > s$ is also not in $\mathcal{C}$. Also, if $r \in \mathcal{C}$ and $s \notin \mathcal{C}$ then it must be that $r < s$.

Definition

If $\mathcal{C}$ and $\mathcal{D}$ are cuts then we say that $\mathcal{C} < \mathcal{D}$ provided that $\mathcal{C}$ is a subset of $\mathcal{D}$ but $\mathcal{C} \neq \mathcal{D}$.

Check for yourself that "$<$" is an ordering on the set of all cuts.

Now we introduce operations of addition and multiplication which will turn the set of all cuts into a field.

Definition

If $\mathcal{C}$ and $\mathcal{D}$ are cuts then we define

$$\mathcal{C} + \mathcal{D} = \{c + d : c \in \mathcal{C}, d \in \mathcal{D}\}.$$

We define the cut $\widehat{0}$ to be the set of all negative rationals.

The cut $\widehat{0}$ will play the role of the additive identity. We are now required to check that field axioms **A1**–**A5** hold.

For **A1**, we need to see that $\mathcal{C} + \mathcal{D}$ is a cut. Obviously $\mathcal{C} + \mathcal{D}$ is not empty. If s is an element of $\mathcal{C} + \mathcal{D}$ and t is a rational number less than s, write $s = c + d$, where $c \in \mathcal{C}$ and $d \in \mathcal{D}$. Then $t - c < s - c = d \in \mathcal{D}$ so $t - c \in \mathcal{D}$; and $c \in \mathcal{C}$. Hence $t = c + (t - c) \in \mathcal{C} + \mathcal{D}$. A similar argument shows that there is an $r > s$ such that $r \in \mathcal{C} + \mathcal{D}$. Finally, if x is a rational upper bound for $\mathcal{C}$ and y is a rational upper bound for $\mathcal{D}$, then $x + y$ is a rational upper bound for $\mathcal{C} + \mathcal{D}$. We conclude that $\mathcal{C} + \mathcal{D}$ is a cut.

Since addition of rational numbers is commutative, it follows immediately that addition of cuts is commutative. Associativity follows in a similar fashion.

Now we show that, if $\mathcal{C}$ is a cut, then $\mathcal{C} + \widehat{0} = \mathcal{C}$. For if $c \in \mathcal{C}$ and $z \in \widehat{0}$ then $c + z < c + 0 = c$ hence $\mathcal{C} + \widehat{0} \subseteq \mathcal{C}$. Also, if $c' \in \mathcal{C}$ then choose a $d' \in \mathcal{C}$ such that $c' < d'$. Then $c' - d' < 0$ so $c' - d' \in \widehat{0}$. And $c' = d' + (c' - d')$. Hence $\mathcal{C} \subseteq \mathcal{C} + \widehat{0}$. We conclude that $\mathcal{C} + \widehat{0} = \mathcal{C}$.

Finally, for Axiom **A5**, we let $\mathcal{C}$ be a cut and set $-\mathcal{C}$ to be equal to $\{d \in \mathbb{Q} : c + d < 0 \text{ for all } c \in \mathcal{C}\}$. If x is a rational upper bound for $\mathcal{C}$ and $c \in \mathcal{C}$ then $-x \in -\mathcal{C}$ so $-\mathcal{C}$ is not empty. By its very definition, $\mathcal{C} + (-\mathcal{C}) \subseteq \widehat{0}$. Further, if $z \in \widehat{0}$ and $c \in \mathcal{C}$ we set $c' = z - c$. Then $c' \in -\mathcal{C}$ and $z = c + c'$. Hence $\widehat{0} \subseteq \mathcal{C} + (-\mathcal{C})$. We conclude that $\mathcal{C} + (-\mathcal{C}) = \widehat{0}$.

Having verified the axioms for addition, we turn now to multiplication.

Definition

If $\mathcal{C}$ and $\mathcal{D}$ are cuts then we define the product $\mathcal{C} \cdot \mathcal{D}$ as follows:

- If $\mathcal{C}, \mathcal{D} > \widehat{0}$ then $\mathcal{C} \cdot \mathcal{D} = \{q \in \mathbb{Q} : q < c \cdot d$ for some $c \in \mathcal{C}, d \in \mathcal{D}$ with $c > 0, d > 0\}$
- If $\mathcal{C} > \widehat{0}, \mathcal{D} < \widehat{0}$ then $\mathcal{C} \cdot \mathcal{D} = -(\mathcal{C} \cdot (-\mathcal{D}))$
- If $\mathcal{C} < \widehat{0}, \mathcal{D} > \widehat{0}$ then $\mathcal{C} \cdot \mathcal{D} = -((-\mathcal{C}) \cdot \mathcal{D})$
- If $\mathcal{C}, \mathcal{D} < \widehat{0}$ then $\mathcal{C} \cdot \mathcal{D} = (-\mathcal{C}) \cdot (-\mathcal{D})$
- If either $\mathcal{C} = \widehat{0}$ or $\mathcal{D} = \widehat{0}$ then $\mathcal{C} \cdot \mathcal{D} = \widehat{0}$.

Notice that, for convenience, we have defined multiplication of negative numbers just as we did in high school. The reason is that the definition that we use for the product of two positive numbers cannot work when one of the two factors is negative (exercise).

It is now a routine exercise to verify that the set of all cuts, with this definition of multiplication, satisfies field axioms **M1**–**M5**. The proofs follow those for **A1**–**A5** rather closely.

For the distributive property, one first checks the case when all the cuts are positive, reducing it to the distributive property for the rationals. Then one handles negative cuts on a case by case basis.

We now know that the collection of all cuts forms an ordered field. Denote this field by the symbol $\mathbb{R}$. We next verify the crucial property of $\mathbb{R}$ that sets it apart from $\mathbb{Q}$:

Theorem

The ordered field $\mathbb{R}$ satisfies the least upper bound property.

Proof: Let S be a subset of $\mathbb{R}$ which is bounded above. Define

$$\mathcal{S}^* = \bigcup_{\mathcal{C} \in S} \mathcal{C}\,.$$

Then $\mathcal{S}^*$ is clearly nonempty, and it is therefore a cut since it is a union of cuts. It is also clearly an upper bound for S since it contains each element of S. It remains to check that $\mathcal{S}^*$ is the least upper bound for S.

In fact if $\mathcal{T} < \mathcal{S}^*$ then $\mathcal{T} \subseteq \mathcal{S}^*$ and there is a rational number q in $\mathcal{S}^* \setminus \mathcal{T}$. But, by the definition of $\mathcal{S}^*$, it must be that $q \in \mathcal{C}$ for some $\mathcal{C} \in S$. So $\mathcal{C} > \mathcal{T}$, and $\mathcal{T}$ cannot be an upper bound for S. Therefore $\mathcal{S}^*$ is the least upper bound for S, as desired. $\square$

We have shown that $\mathbb{R}$ is an ordered field which satisfies the least upper bound property. It remains to show that $\mathbb{R}$ contains (a copy of) $\mathbb{Q}$ in a natural way. In fact, if $q \in \mathbb{Q}$ we associate to it the element $\varphi(q) = \mathcal{C}_q \equiv \{x \in \mathbb{Q} : x < q\}$. Then $\mathcal{C}_q$ is obviously a cut. It is also routine to check that

$$\varphi(q + q') = \varphi(q) + \varphi(q') \quad \text{and} \quad \varphi(q \cdot q') = \varphi(q) \cdot \varphi(q').$$

Therefore we see that φ represents $\mathbb{Q}$ as a subfield of $\mathbb{R}$.