DESCRIBING THE REAL NUMBERS

TONY VÁRILLY

1. Introduction

The goal of these notes is to *uniquely describe* the real numbers by taking certain statements as axioms. We are not trying to *construct* the real numbers, we are just trying to make sense of our experience with them.This exercise might seem tedious at times, but it is important to do it at least once in one's life. Don't worry if you can't make sense of all the details the first time you read this handout. Reading mathematics takes time and patience. It would be a good idea to have pencil and paper in hand so that you can verify many of the proofs presented here as you go along. Most of the material covered here is not in a way essential to Math 25, but the handout does have many detailed proofs which you are invited to explore as you learn how to write proofs.

2. First Step: $\mathbb{R}$ is a field

Definition. A *field* F is a set for which two operations from $F \times F$ into F are defined. We will call them addition $(+)$ and multiplication $(\cdot)$:

$$(a, b) \mapsto a + b \qquad (a, b) \mapsto a \cdot b$$

For $a, b, c \in F$, these operations satisfy:

Associativity	$a + (b + c) = (a + b) + c;$	$a(bc) = (ab)c,$
Commutativity	$a + b = b + a;$	$a \cdot b = b \cdot a,$
Identities $\exists\ 0, 1 \in F$	$a + 0 = a;$	$a \cdot 1 = a,$
Inverses $\exists\ -a$ and $a^{-1} (a \neq 0)$	$a + (-a) = 0;$	$a \cdot a^{-1} = 1.$

Our two operations are linked through *distributivity*: $a \cdot (b + c) = a \cdot b + a \cdot c$ for $a, b, c \in F$. Finally, we assume that $1 \neq 0$.

Remark. We will often write the product $a \cdot b$ simply as ab.

Examples. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields. Another good example is $\mathbb{R}(X)$, the field of rational functions in one indeterminate. An element of this field is of the form $S(X)/T(X)$ where S and T are polynomials with coefficients in $\mathbb{R}$ and $T \neq 0$.

We can prove many results which seem trivial through experience from these axioms.

Proposition 1. *The additive identity of a field F is unique.*

Proof. Suppose there are two additive identities $0, 0' \in F$. Then

$$0 = 0 + 0' = 0'.$$

Date: *Math 25a, Fall 2001.*

The left equality follows because 0 is an additive identity of F. Similarly, the right equality follows because $0'$ is an additive identity of F. □

Theorem 2.1. *For any $a \in F$ we have $a0 = 0$.*

Proof. This is a highly non-trivial statement. Read aloud, it says that any element of the field multiplied by the additive identity gives you back the additive identity. We defined 0 additively, so why should it have this wonderful multiplicative property? We have

$$\begin{aligned}
0 + 0 &= 0 && \text{additive identity} \\
a(0 + 0) &= a0 && \\
a0 + a0 &= a0 && \text{distributivity} \\
(a0 + a0) + (-a0) &= a0 + (-a0) && \text{existence of additive inverses} \\
a0 + (a0 + (-a0)) &= a0 + (-a0) && \text{associativity of } + \\
a0 + 0 &= 0 && \text{additive inverses} \\
a0 &= 0 && \text{additive identity}
\end{aligned}$$

□

Remark. Most, if not all proofs in Math 25a do not have to be as ultra-rigorous as this last one. I just wanted to give an example of an absolutely water-tight axiomatic proof.

Theorem 2.2. *For $a \in F$ we have $(-1)a = -a$. Furthermore, if $b \in F$ then $(-a)(-b) = ab$.*

We leave the proof as an exercise. (*Hint:* begin with $1 + (-1) = 0$ and use Theorem 2.1.)

The field axioms do not describe $\mathbb{R}$ uniquely. As we saw in the examples, they also describe $\mathbb{Q}$, and we know from experience that $\mathbb{Q}$ and $\mathbb{R}$ are different. Our picture of $\mathbb{R}$ is as of yet incomplete.

3. Second Step: $\mathbb{R}$ has an order

We follow Hewitt and Stromberg [1] in our treatment of ordered fields.

Definition. A field is *ordered* if there is a subset P of F such that

1. $P \cap (-P) = \varnothing$,
2. $P \cup \{0\} \cup (-P) = F$,
3. For $a, b \in P$ we have $a + b \in P$ and $ab \in P$

Think of $\mathbb{R}$ as our field F and the set of positive numbers as P. In particular, $\mathbb{R}$ is an ordered field.

Theorem 3.1. *Let F be an ordered field. If $a \in F$ and $a \neq 0$, then $a^2 \in P$. In particular, $1 \in P$.*

Proof. Since $a \neq 0$, Properties 1. and 2. above tell us $a \in P$ or $a \in (-P)$. If $a \in P$, then by Property 3. $a^2 \in P$. If $a \in (-P)$, then $-a \in P$, and by Property 3. $(-a)^2 \in P$. But by Theorem 2.2, $(-a)(-a) = a^2$, so again $a^2 \in P$. Since $1 \cdot 1 = 1$, we have $1 \in P$. □

Remark. It is true that $\mathbb{Q}$ can be embedded into every ordered field F that is infinite. This just means there's a copy of $\mathbb{Q}$ lurking at the core of every infinite ordered field. We are not finished with our description of $\mathbb{R}$ then, since $\mathbb{Q}$ is also an ordered field. However, $\mathbb{C}$ is *not* an ordered field, so we have indeed made some progress towards our goal of describing $\mathbb{R}$ uniquely.

Definition. Let F be an ordered field. We write $a < b$, or equivalently $b > a$ if and only if $b - a \in P$.

Theorem 3.2 (Trichotomy)**.** *Let F be an ordered field and $a, b \in F$. Then exactly one of the following relations hold:*

$$a < b, \qquad a = b, \qquad a > b.$$

Proof. The proof follows directly from the definition of ordered field. □

You can prove now, for example, that given elements a, b and c of an ordered field, such that $a > b$, then $a + c > b + c$ and if $c > 0$ then $ac > bc$ as well.

Definition. Let F be an ordered field and $a \in F$. We define $|a|$ as

$$|a| = \begin{cases} a & \text{if } a \geq 0, \\ -a & \text{if } a < 0. \end{cases}$$

Theorem 3.3. *Let a, b be elements of an ordered field F. Then*

1. $|a| = |-a|$,
2. $|ab| = |a||b|$,
3. $|a + b| \leq |a| + |b|$,
4. $||a| - |b|| \leq |a - b|$.

Proof. The first two statements follow straight from the definition of the absolute value. We prove the third asserion. It is easily checked that $a \leq |a|$ and $b \leq |b|$. Hence

$$a + b \leq |a| + |b|.$$

We also have $-a \leq | - a| = |a|$, and similarly for b. Thus

$$-(a + b) \leq |a| + |b|.$$

To see why the fourth statement is true, substitute in turn $a - b$ for a and $b - a$ for b in the third statement. □

As we said before, our description of $\mathbb{R}$ is still unsatisfactory. So far, an ordered field describes both $\mathbb{R}$ and $\mathbb{Q}$. We know, for example that $\sqrt{2} \in \mathbb{R}$ but $\sqrt{2} \notin \mathbb{Q}$. So somehow we must fill in the 'holes' that $\mathbb{Q}$ has in order to obtain $\mathbb{R}$. Would filling in these 'holes' be enough to characterize $\mathbb{R}$ uniquely? Consider the following example.

Example. Let $\mathbb{Q}(X)$ be the field of rational functions with coefficients in $\mathbb{Q}$. An element of this field is of the form $A(X)/B(X)$ where $A(X) = \sum_0^n a_i X^i$ and $B(X) = \sum_0^m b_j X^j \neq 0$. Now introduce an order in $\mathbb{Q}(X)$ by putting $A(X)/B(X)$ in P if and only if $a_n b_m$ is a positive rational number. Certainly this field is 'bigger' than $\mathbb{Q}$ since a copy of $\mathbb{Q}$ can be found in the constant polynomials of $\mathbb{Q}(X)$. But is this field intrinsically different from $\mathbb{R}$? If so, in what way?

4. Third Step: $\mathbb{R}$ is Archimedian

Definition. An ordered field F is called *Archimedian* if for all $a \in F$ and $b \in P$ there exists a positive interger n such that $nb > a$.

Intuitively, the Archimedian property says that given any 'length' a and a unit of measurement b, we can produce enough copies of b to totally cover the length a. The rational numbers are Archimedian, and so are the real numbers. But the field we described in the example from the previous section isn't. To see why this is the case, take $a = X \in Q(X)$ and $b = 1 \in P$. Then $nb > a$ if and only if $nb - a \in P$. But $nb - a = -X + n$, and this element is not in P according to

our order of $\mathbb{Q}(X)$. So we have an example of an ordered field which is not Archimedian. The real numbers, however, do constitute an Archimedian ordered field.

We are very close to our goal of describing $\mathbb{R}$. We still need to fill in the holes left by the irrational numbers in $\mathbb{Q}$. Once we do this, our description will be complete. Furthermore, we can *prove* our description is complete, by showing that any two objects satisfying our axioms are isomorphic (i.e., they have 'the same form').

5. Fourth Step: $\mathbb{R}$ has the nested intervals property

Definition. An ordered field F is said to satisfy the *nested intervals property* if given a sequence of closed intervals $([a_n, b_n]_n)$ such that $a_n \leq a_{n+1}$ and $b_{n+1} \leq b_n$ for all n, the intersection of the sequence is non-empty.

Example. $\mathbb{Q}$ does not satisfy the nested intervals property. Consider the fractions

$$x_n = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}$$

where there are n 2's in the fraction x_n. Each x_n is a rational number. Let $a_n = x_{2n}$ and $b_n = x_{2n+1}$. Then one can show $a_n \leq a_{n+1}$ and $b_{n+1} \leq b_n$ for all $n \in \mathbb{N}$. If $\mathbb{Q}$ satisfies the nested intervals property, then $\cap_n([a_n, b_n]) \neq \varnothing$ in $\mathbb{Q}$. But this intersection is $\sqrt{2}$, which is not in $\mathbb{Q}$.

Remark. The nested intervals property is what makes $\mathbb{R}$ *complete*. There are many other notions that are equivalent to completeness. A popular one, found in most analysis books, and included in this week's problem set, is done using *Cauchy sequences*. The nested intervals approach is equivalent and very clean. Many theories in Math have more than one way of going about them. This is my personal favorite.

We now prove a very important theorem that is possible by the nested intervals property. In what follows, keep $\mathbb{R}$ in mind whenever we discuss a field F.

Definition. Let X be a non-empty subset of an ordered field F. Let $a \in F$. If $x \leq a$ for all $x \in X$, then a is called an *upper bound* of the subset X. If such an a exists, the set X is said to be *bounded above*. A *lower bound* is defined analogously. A set X that is bounded above and below is said to be *bounded*.

Theorem 5.1. *Let F be an Archimedian ordered field that satisfies the nested intervals property. Let X be a non-empty subset of F that is bounded above. Then among all the upper bounds of X, there is a smallest one.*

The theorem asserts the existence of a least upper bound on a set X that is bounded above. We call this least upper bound the *supremum* of X and denote it $\sup X$. One can also prove that a non-empty subset X of F that is bounded below has a greatest lower bound. It is called the *infimum* of X, and it is denoted $\inf X$.

Proof of Theorem 5.1. We'll follow Dieudonné [2] in our proof. Let a be an element of X, and b an upper bound for the set. Since the field we are working on is Archimedian, for every integer n there is another integer m such that $b \leq a + m \cdot 2^{-n}$. If c is an upper bound for X, then so is every other $y \geq c$. Thus there is a smallest p_n such that $b \leq a + p_n 2^{-n}$ is an upper bound for X.

Let $I_n = [a + (p_n - 1)2^{-n}, a + p_n 2^{-n}]$. Then by the definition of p_n, $X \cap I_n$ is not empty. Since $p_n 2^{-n} = (2p_n)2^{-n-1}$, then either $p_{n+1} = 2p_n$ or $p_{n+1} = 2p_n - 1$ because $a + (2p_n - 2)2^{-n-1} = a + (p_n - 1)2^{-n}$ is not an upper bound for X. This means $I_{n+1} \subset I_n$. By the nested intervals property, the intervals I_n have a non-empty intersection J.

We want to show that this non-empty intersection contains only one member of F, and that this member is our least upper bound. Suppose that J contains at least two elements α and β. Assume $\alpha < \beta$. The interval $[\alpha, \beta]$ would be contained in each I_n. But each I_n has length 2^{-n}. Hence $2^{-n} > \beta - \alpha$ for every n, or $1 > 2^n(\beta - \alpha)$. This means F is not Archimedian. For example, since $2^n \geq n$ (which one can prove using mathematical induction), we have $1 \geq n(\beta - alpha)$ for all n, which implies F is not Archimedian. This contradiction tells us the intersection$J$ can have at most one element. Since it is not empty, we conclude J has excatly one element, $J = \{\gamma\}$.

We claim γ is an upper bound for X. Suppose it is not; then there is an $x \in X$ such that $x > \gamma$. If we choose an integer n big enough, we get $2^{-n} < x - \gamma$. Since $\gamma \in I_n$ for this n, we'd have $x > a + p_n 2^{-n}$, contrary to the definition of p_n. Thus γ is an upper bound for X

Finally, γ is the least upper bound of X. Suppose there is a smaller upper bound y. Then $\gamma > y$ means there is some integer n such that $2^{-n} < \gamma - y$. Since $\gamma \in I_n$ for this particualr n, we have $a + (p_n - 1)2^{-n} > y$, so $a + (p_n - 1)2^{-n}$ would be an upper bound for X. Again, this contradict the definition of p_n. Thus γ is the least upper bound of X. □

One can show that a converse to this theorem is true, that is, if in an Archimedian ordered field every non-empty subset bounded above has a least upper bound, then this field must satisfy the nested intervals property. Professor Karu will do this in Math 25a.

From our experience, we feel that $\mathbb{R}$ indeed has the nested intervals property. This is what fills in the holes that $\mathbb{Q}$ has. But how do we *prove* $\mathbb{R}$ has this property? We don't. What we do is *define* $\mathbb{R}$ to be an Archimedian ordered field that has the nested intervals property. We can show $\mathbb{R}$ is well-defined by proving that any two Archimedian ordered fields which satisfy the nested intervals property are 'isomorphic' to each other.

Definition. Two fields F and F' are said to be *isomorphic* if there is a one-to-one and onto map[1] $\phi : F \to F'$ that respects the operations of addition and multiplication, and such that $\phi(1_F) = 1_{F'}$. That is,

$$\phi(a +_F b) = \phi(a) +_{F'} \phi(b) \quad \text{and} \quad \phi(a \cdot_F b) = \phi(a) \cdot_{F'} \phi(b) \quad \forall a, b \in F,$$

where, for example, $+_F$ denotes the operation of addition in the field F.

Theorem 5.2. *Any two Archimedian ordered fields F and F' that satisfy the nested intervals property are isomorphic. Furthermore, if P and P' are their sets of positive elements, respectively, and if ϕ is an isomorphism between F and F', then $\phi(a) \in P'$ if and only if $a \in P$.*

Proof. We'll construct the isomorphism ϕ step by step, following Hewitt and Stromberg [1]. Let 1 and $1'$ be the multiplicative identities of F and F' respectively, and let 0 and $0'$ be their additive

[1] A *one-to-one map* $f : A \to B$ is a map such that for $a \in A$ and $b \in B$, $f(a) = f(b)$ implies $a = b$. The map f is *onto* if for every $b \in B$ there is an $a \in A$ such that $f(a) = b$.

identities. Define $\phi : F \to F'$ by setting

$$\begin{aligned}
\phi(1) &= 1';\\
\phi(0) &= 0';\\
\phi(m \cdot_F 1) &= m \cdot_{F'} 1', \text{ for } m \text{ an integer}\\
\phi(\frac{1}{n} \cdot_F 1) &= \frac{1}{n} \cdot_{F'} 1', \text{ for} n \text{ any non} - \text{zero integer}\\
\phi(\frac{m}{n} \cdot_F 1) &= \frac{m}{n} \cdot_{F'} 1'.
\end{aligned}$$

If $a \in F$ and a is not of the form $(m/n) \cdot 1$ (think of the irrational numbers in $\mathbb{R}$), then define

$$\phi(a) = \sup \left\{ \frac{m}{n} \cdot_{F'} | \frac{m}{n} \cdot_F 1 < a \right\}.$$

You can check that ϕ is one-to-one and onto, and that $\phi(a) \in P'$ if and only if $a \in P$. □

References

[1] E. Hewitt, K. Stromberg, *Real and Abstract Analysis* Springer, Berlin, 1969.
[2] J. Dieudonné *Foundations of Modern Analysis* Academic Press, New York, 1969.

Mathematics Department, Harvard University
E-mail address: varilly@fas.harvard.edu