Math 117: Axioms for the Real Numbers

John Douglas Moore

October 11, 2010

As we described last week, we could use the axioms of set theory as the foundation for real anaysis. To carry this out, we would start by defining the set of natural numbers

$$\mathbb{N} = \{1, 2, 3, \ldots\} \quad \text{and} \quad \omega = \{0\} \cup \mathbb{N} = \{0, 1, 2, 3, \ldots\},$$

together with the usual operations of addition and multiplication. We could then define an equivalence relation $\sim$ on the Cartesian product $\omega \times \omega$ by

$$(m, n) \sim (q, r) \quad \Leftrightarrow \quad m + r = q + n.$$

The set of integers $\mathbb{Z}$ is then the set of equivalence classes. If $[m, n]$ is the equivalence class of the pair $(m, n) \in \mathbb{N} \times \mathbb{N}$, then

$$\mathbb{Z} = \{\ldots, -2 = [0, 2], -1 = [0, 1], 0 = [0, 0], 1 = [1, 0], 2 = [2, 0], \ldots\}.$$

We then define the usual addition and multiplication on $\mathbb{Z}$ and show that it satisfies the familiar properties. Finally, we define an equivalence relation $\sim$ on the Cartesian product $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ by

$$(m, n) \sim (q, r) \quad \Leftrightarrow \quad mr = qn.$$

We would think of the equivalence class $[m, n]$ are representing the fraction m/n as a rational number. We would then estabiish as theorems all the rules you learned for arithmetic with rational numbers in grade school. The process would be long and time-consuming, and you might wonder whether it isn't a bit pedantic to carry this out with so much rigor. But the point to understand is that all of the familiar rules of arithmetic for rational numbers can in fact be established in this way.

The last stage is developing the real numbers $\mathbb{R}$, which can be thought of as limits of sequences of rational numbers. For example π is the limit of the sequence

$$(3, 3.1, 3.14, 3.141, 3.1415, 3.14159, 3.141592, \ldots, 3.14159265358979, \ldots).$$

It is precisely the notion of defining the limit of such a sequence which is the major difficulty in developing real analysis. It would take a long time just

to define the real numbers in this manner. So for a first treatment of real analysis, most authors take a shortcut, and formulate a collection of axioms which characterize the real numbers. One assumes these axioms as the starting point of real analysis, rather than just the axioms of set theory. (Since one does want to use the properties of sets in discussing real numbers, a full formal development of analysis in this shortened form would require both the axioms of set theory and the axioms of real numbers. On the other hand, many authors, such as [1] just use set theory as a basic language whose basic properties are intuitively clear; this is more or less the way mathematicians thought about set theory prior to its axiomatization.)

The axioms for real numbers fall into three groups, the axioms for fields, the order axioms and the completeness axiom.

1 Field axioms

Definition. A *field* is a set F together with two operations (functions)

$$f : F \times F \to F, \qquad f(x, y) = x + y$$

and

$$g : F \times F \to F, \qquad g(x, y) = xy,$$

called addition and multiplication, respectively, which satisfy the following axioms:

- F1. addition is commutative: $x + y = y + x$, for all $x, y \in F$.
- F2. addition is associative: $(x + y) + z = x + (y + z)$, for all $x, y, z \in F$.
- F3. existence of additive identity: there is a unique element $0 \in F$ such that $x + 0 = x$, for all $x \in F$.
- F4. existence of additive inverses: if $x \in F$, there is a unique element $-x \in F$ such that $x + (-x) = 0$.
- F5. multiplication is commutative: $xy = yx$, for all $x, y \in F$.
- F6. multiplication is associative: $(xy)z = x(yz)$, for all $x, y, z \in F$.
- F7. existence of multliplicative identity: there is a unique element $1 \in F$ such that $1 \neq 0$ and $x1 = x$, for all $x \in F$.
- F8. existence of multliplicative inverses: if $x \in F$ and $x \neq 0$, there is a unique element $(1/x) \in F$ such that $x \cdot (1/x) = 1$.
- F9. distributivity: $x(y + z) = xy + xz$, for all $x, y, z \in F$.

Note the similarity between axioms F1-F4 and axioms F5-F8. In the language of algebra, axioms F1-F4 state that F with the addition operation f is an *abelian group*. (The group axioms are studied further in the first part of abstract algebra, which is devoted to group theory.) Axioms F5-F8 state that $F - \{0\}$ with the multiplication operation g is also an abelian group. Axiom F9 ties the two field operations together.

Most important examples. The key examples of fields are the set of rational numbers $\mathbb{Q}$, the set of real numbers $\mathbb{R}$ and the set of complex numbers $\mathbb{C}$, in all cases taking f and g to be the usual addition and multiplication operations. On the other hand, the set of integers $\mathbb{Z}$ is NOT a field, because integers do not always have multiplicative inverses.

Other useful examples. Another example is the field $\mathbb{Z}/p\mathbb{Z}$, where p is a prime ≥ 2, which consists of the elements $\{0, 1, 2, \ldots, p-1\}$. In this case, we define addition or multiplication by first forming the sum or product in the usual sense and then taking the remainder after division by p, so as to arrive back in the set $\{0, 1, 2, \ldots, p-1\}$. This is often referred to as mod p addition and multiplication. Thus for example,

$$\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$$

and within $\mathbb{Z}/5\mathbb{Z}$,

$$3 + 4 = 7 \bmod 5 = 2, \qquad 3 \cdot 4 = 12 \bmod 5 = 2.$$

On the other hand, if n is not a prime, then $\mathbb{Z}/n\mathbb{Z}$ with mod n addition and multiplication is NOT a field. Indeed, in $\mathbb{Z}/4\mathbb{Z}$,

$$2 + 2 = 4 \bmod 4 = 0,$$

so 2 does not have a multiplicative inverse in $\mathbb{Z}/4\mathbb{Z}$, contradicting Axiom F8.

Yet other examples of fields arise when studying roots of polynomials with rational coefficients. Thus, for example, we might consider the field generated by rationals together with the roots $x = \pm\sqrt{2}$ of the polynomial

$$p(x) = x^2 - 2.$$

This field, to be denoted by $\mathbb{Q}(\sqrt{2})$, consists of real numbers of the form $a+b\sqrt{2}$, where a and b are rational. One checks that if $x, y \in \mathbb{Q}(\sqrt{2})$, say

$$x = a + b\sqrt{2} \quad \text{and} \quad y = c + d\sqrt{2},$$

where a, b, c and d are rational, then

$$x + y = (a + c) + (b + d)\sqrt{2}, \qquad x \cdot y = (ac + 2bd) + (ad + bc)\sqrt{2}$$

are also elements of $\mathbb{Q}(\sqrt{2})$. Similarly, we check that

$$-x = (-a) + (-b)\sqrt{2},$$

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

are elements of $\mathbb{Q}(\sqrt{2})$. From these facts it is easy to check that $\mathbb{Q}(\sqrt{2})$ is indeed a field such that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Needless to say, many many fields can be constructed in this way by adjoining roots of certain polynomials.

Starting with the field axioms, one can prove that the usual rules for addition and multiplication hold. As long as we are within ANY field, we can then use those rules with perfect confidence. For example, we could begin by giving a complete proof of the cancellation law:

Proposition. If F is a field and $x, y, z \in F$, then

$$x + z = y + z \quad \Rightarrow \quad x = y.$$

Proof: Suppose that $x + z = y + z$. Let $(-z)$ be an additive inverse to z, which exists by Axiom F4. Then

$$(x + z) + (-z) = (y + z) + (-z).$$

By associativity of addition (Axiom F2),

$$x + (z + (-z)) = y + (z + (-z)).$$

Then by Axiom F4, $x + 0 = y + 0$ and by Axiom F3, $x = y$.

Proposition. If F is a field and $x \in F$, then $x \cdot 0 = 0$.

Proof: By Axiom F3, $x \cdot 0 = x \cdot (0+0)$. By distributivity (Axiom F9), $x \cdot (0+0) = x \cdot 0 + x \cdot 0$. By Axiom F3 again,

$$0 + x \cdot 0 = x \cdot 0 + x \cdot 0,$$

and by Axiom F1,

$$x \cdot 0 + 0 = x \cdot 0 + x \cdot 0.$$

Hence $0 = x \cdot 0$ by the preceding proposition.

Several similar propositions can be found in §11 of the text [2]. You should learn how to prove the easiest of these directly from the axioms.

2 Ordered fields

Definition. An *ordered field* is a field F together with a relation $<$ which satisfies the axioms

- O1. trichotomy: if $x, y \in F$, then exactly one of the following is true:

$$x < y, \quad x = y, \quad y < x.$$

- O2. transitivity: if $x, y, z \in F$, then $x < y$ and $y < z$ implies $x < z$.

- O3. if $x, y, z \in F$, then $x < y$ implies $x + z < y + z$.
- O4. if $x, y, z \in F$ and $0 < z$, then $x < y$ implies $x \cdot z < y \cdot z$

We agree that $x > y$ means $y < x$, $x \leq y$ means if $x < y$ or $x = y$ and $x \geq y$ means if $x > y$ or $x = y$.

We could prove the basic rules for working with inequalities directly from the axioms. For example,

Proposition. If F is an ordered field and x and y are elements of F such that $x < y$, then $-y < -x$.

Proof: By Axiom O3, $x + ((-x) + (-y)) < y + ((-x) + (-y))$. By commutativity of addition (Axiom F1), $x + ((-x) + (-y)) < y + ((-y) + (-x))$ and by associativity of addition (Axiom F2) $(x + (-x)) + (-y) < (y + (-y)) + (-x)$. By the axiom on additive inverses (Axiom F4), $0 + (-y) < 0 + (-x)$. Finally, by the axiom on the additive identity (Axiom F3), $-y < -x$.

We could prove several similar familiar rules for dealing with inequalities in the same way. Further proofs of this nature can be found in §11 of the text [2].

Examples of ordered fields include the rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$, as as the field $\mathbb{Q}(\sqrt{2})$. On the other hand, we claim that the complex numbers $\mathbb{C}$ is not an ordered field. Indeed, it follows from the axioms that

$$x > 0 \quad \& \quad y > 0 \quad \Rightarrow \quad x + y > y > 0$$

by axioms O3 and O2. But then

$$1 < 0 \quad \Rightarrow \quad 0 < -1 \quad \Rightarrow \quad 0 < (-1)^2 \quad \Rightarrow \quad 0 < 1.$$

Thus if $x = 0$, then $x^2 + 1 = 0$. Moreover,

$$x < 0 \quad \Rightarrow \quad 0 < -x \quad \Rightarrow \quad 0 < (-x)^2 = x^2 \quad \Rightarrow \quad x^2 + 1 > 0$$

and

$$x > 0 \quad \Rightarrow \quad x^2 > 0 \quad \Rightarrow \quad x^2 + 1 > 0,$$

so for any x in an ordered field, $x^2 + 1 > 0$ On the other hand, the complex number i satisfies $i^2 + 1 = 0$, so $\mathbb{C}$ cannot be an ordered field, just as we claimed.

We should note that any ordered field F must contain the natural numbers $\mathbb{N}$ as a subset. Indeed, one could use the Recursion Theorem from §3 of the Notes on Set Theory to define a function $u : \mathbb{N} \to F$ by

$$u(1) = (\text{the multiplicative idenitity 1 of } F),$$
$$u(n + 1) = u(n) + 1, \quad \text{for } n \in \mathbb{N}.$$

Then one can use the ordering on F to show that

$$n < m \quad \Rightarrow \quad u(n) < u(m),$$

so that u is injective. Finally, one can identify $\mathbb{N}$ with the image of the function u.

Definition. An ordered field F is said to be *Archimedean* if for every $x, y \in F$ with $x > 0$, there exists an $n \in \mathbb{N}$ such that

$$nx = \overbrace{x + x + \cdots + x}^{n} > y.$$

There are several equivalent formulations of the the Archimedean property. For example, an ordered field F is Archimedean if and only if for every $x > 0$ in F, there is an $n \in \mathbb{N}$ such that $1/n < x$. A field F is Archimedean if and only if the subset $\mathbb{N} \subseteq F$ of natural numbers is unbounded.

We will see shortly that $\mathbb{R}$ and $\mathbb{Q}$ are Archimedean ordered fields. An important example of an ordered field that is not Archimedean is the field $\mathbb{F}$ of rational functions. By definition, a *rational function* is a quotient $f(x) = p(x)/q(x)$ of two polynomials with real coefficients, where $q(x)$ is nonzero. Thus

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$
$$q(x) = b_m x^n + b_{n-1} x^{m-1} + \cdots + b_1 x + b_0,$$

where the coefficients $a_n, \ldots, a_1, a_0$ and $b_m, \ldots, b_1, b_0$ are real numbers, and $b_m \neq 0$. Notice that the sum of two rational functions is a rational function, as is the product of two rational functions.

We say that the rational function

$$f(x) = \frac{p(x)}{q(x)} = \frac{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0}{b_m x^n + b_{n-1} x^{m-1} + \cdots + b_1 x + b_0},$$

is positive if $a_n/b_m > 0$, and that $f < g$ if $g - f$ is positive. It is easily checked that with this relation $<$, together with the usual addition and multiplication, the set $\mathbb{F}$ of rational functions is indeed an ordered field. Moreover, $x > n$, for all $n \in \mathbb{N}$, so this ordered field is not Archimedean.

Curious application of non-Archimedean fields. One might try to develop calculus on the basis of infinitesimal quantities, numbers dx that satisfy the property that

$$0 < dx < \frac{1}{n}, \quad \text{for all } n \in \mathbb{N}.$$

The idea would be to imbed the reals in a non-Archimedean ordered field which contains suchan infinitesimal element dx. One can then express derivatives in terms of these infinitesimal quantities. Pursuing this approach leads to the subject *nonstandard analysis*, developed by Abraham Robinson [3] and others. However, most most mathematicians do not do this, but rather consider the foundations of calculus to be based upon the ϵ and δ arguments that we will present later.

3 Complete ordered fields

Note that the field $\mathbb{F}$ of rational functions contains a subfield of constant functions, which we can identify with $\mathbb{R}$. Thus we have inclusions

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{F}$$

In some sense, $\mathbb{Q}$ has too few elements to use as a foundation for calculus, while $\mathbb{F}$ has too many. There is an additional axiom which together with earlier axioms completely characterizes the real numbers.

Definition. Suppose that S is a subset of a field F. An *upper bound* for S is an element $m \in F$ such that

$$x \in S \quad \rightarrow \quad x \leq m,$$

while a lower bound for S is an element $m \in F$ such that

$$x \in S \quad \rightarrow \quad x \geq m.$$

A *least upper bound* or *supremum* of S is an upper bound m for S such that whenever m' is an upper bound for S, then $m \leq m'$. A *greatest lower bound* or *infimum* is a lower bound m for S such that whenever m' is a lower bound for S, then $m \geq m'$.

Definition. A *complete ordered field* is an ordered field F such that if a nonempty subset $S \subset F$ has an upper bound, then S has a least upper bound or supremum which lies within F.

This is equivalent to requiring that if a nonempty subset $S \subset F$ has a lower bound, it has a greatest lower bound in F.

Proposition. If F is a complete ordered field, F is Archimedean.

Proof: Suppose there exist nonzero elements $x, y \in F$ such that $x > 0$ and $nx \leq y$ for all $n \in \mathbb{N}$. Then the set $\{nx : n \in \mathbb{N}\}$ has an upper bound and by the completeness axiom, it must have a least upper bound m. We claim that then $m - x$ must also be an upper bound. Indeed if $m - x$ is not an upper bound, then

$$nx > m - x \quad \text{for some } n \in \mathbb{N} \quad \Rightarrow \quad (n+1)x > m,$$

so m is not an upper bound either. But $m - x < m$ and this contradicts the assertion that m is a least upper bound for $\{nx : n \in \mathbb{N}\}$. Thus F cannot be complete.

Thus the field $\mathbb{F}$ of rational functions is NOT a complete ordered field.

Proposition. If F is a complete ordered field and p is a prime, then there is an element x of F such that $x^2 = p$.

Proof: We let $A = \{r \in F : r^2 \leq p\}$. The set A is bounded above, so F contains a least upper bound x for A. Note that $x > 1$. We claim that $x^2 = p$.

I. Suppose that $x^2 < p$ and $x \geq 1$. Let

$$\delta = \min\left(1, \frac{p - x^2}{2x + 1}\right), \quad \text{so} \quad \delta \leq 1, \quad \delta \leq \frac{p - x^2}{2x + 1}.$$

Then

$$(x + \delta)^2 = x^2 + 2\delta x + \delta^2 \leq x^2 + (2x + 1)\delta \leq x^2 + p - x^2 \leq p,$$

so $x + \delta \in A$ and x is not an upper bound. This contradiction shows that $x^2 \geq p$.

II. Suppose that $x^2 > p$. Let

$$\delta = \min\left(1, \frac{x^2 - p}{2x}\right) > 0.$$

Then

$$(x - \delta)^2 = x^2 - 2\delta x + \delta^2 \geq x^2 - 2\delta x \geq x^2 - (x^2 - p) = p,$$

so $(x - \delta)^2 > r^2$ whenever $r \in A$. If $x - \delta < 0$, then $x < \delta \leq 1$, which leads to a contradiction. Hence $x - \delta > |r| \geq r$ whenever $r \in A$. Thus $x - \delta$ is an upper bound for A, contradicting the fact that x is the least upper bound. This contradiction shows that $x^2 \leq p$.

Putting the two parts together, we see that $x^2 = p$, as we needed to show.

The preceding proposition shows that the field $\mathbb{Q}$ of rational numbers is not a complete ordered field because it does not contain $\sqrt{p}$ when p is a prime, as you saw in Math 8. This fact is also proven as Theorem 12.1 in Lay [2].

4 Conclusion

We emphasize that as a foundation for this course, we ASSUME the existence of a complete ordered field, which we call the *real numbers* and denote by $\mathbb{R}$. We can define an injective function $\iota : \mathbb{Q} \longrightarrow \mathbb{R}$ such that

$$\iota(x + y) = \iota(x) + \iota(y), \quad \iota(x \cdot y) = \iota(x) \cdot \iota(y). \quad x < y \Leftrightarrow \iota(x) < \iota(y),$$

and thereby identify the ordered field $\mathbb{Q}$ of rational numbers with its image $\iota(\mathbb{Q})$ within the complete ordered field $\mathbb{R}$ of real numbers.

A more lengthy treatment would be needed to construct the reals $\mathbb{R}$ from the rationals $\mathbb{Q}$. With sufficient work, everything in real analysis, including construction of the reals $\mathbb{R}$, could be based upon the set theory axioms, and it could be proven that if F is any complete ordered field, there is a bijective function $\psi : F \to \mathbb{R}$ such that

$$\psi(x + y) = \psi(x) + \psi(y), \quad \psi(x \cdot y) = \psi(x) \cdot \psi(y), \quad x < y \Leftrightarrow \psi(x) < \psi(y).$$

Thus the real numbers is the unique complete ordered field up to "order preserving isomorphism."

References

[1] Edward D. Gaughan, *Introduction to analysis*, Brooks-Cole, Pacific Grove, 1998.

[2] Steven R. Lay, *Analysis: with an introduction to proof*, Pearson Prentice Hall, Upper Saddle Riven, NJ, 2005.

[3] Abraham Robinson, *Nonstandard analysis*, North-Holland, Amsterdam, 1966.