Math 117: Axioms for the Real Numbers

John Douglas Moore

October 15, 2008

Our goal for this course is to study properties of subsets of the set $\mathbb{R}$ of real numbers. To start with, we want to formulate a collection of axioms which characterize the real numbers. These axioms 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*. 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.

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 these cases, f and g are 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.

A more abstract 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. 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 $\mathbb{Z}/5\mathbb{Z}$,

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

Other examples arise when studying roots of polynomials with rational coefficients. Thus, for example, we might consider the field generated by rationals and 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

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

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 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$.

Starting with the field axioms, one can prove that the usual rules for addition and multiplication hold. 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 [1]. You should know 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 $x = y$.

For example, the rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$ are both ordered fields, as is $\mathbb{Q}(\sqrt{2})$. The complex numbers $\mathbb{C}$ is not an ordered field, because if x is an element of an ordered field, $x^2 + 1 > 0$, but the complex number i satisfies $i^2 + 1 = 0$.

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 [1].

Definition. An ordered field F is *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 set $\mathbb{N}$ of natural numbers is unbounded.

An important example of an ordered field that does not satisfy the Archimedean property 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 an ordered field. Moreover, $x > n$, for all $n \in \mathbb{N}$, so this ordered field is not Archimedean.

One might try to develop calculus on the basis of infinitesimal quantities, numbers dx that satisfy the property that

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

One way to do this would be to imbed the reals in a non-Archimedean ordered field which contains an infinitesimal element dx. Pursuing this approach would lead to the subject *nonstandard analysis*, developed by Abraham Robinson [2] and others. However, most most mathematicians do not do this, but rather give the foundations of calculus based upon the $\epsilon - \delta$ arguments that we will see 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, while $\mathbb{F}$ has too many. We need an additional axiom to rule out both possibilities.

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 $\mathbb{F}$ 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 $A = \{r \in F : r^2 < p\}$. The set A is bounded above, so F contains a least upper bound x for A. 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

$$\delta = \frac{x^2 - p}{2x} > 0.$$

Then

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

so $(x - \delta)^2 > r^2$ whenever $r \in A$, and hence $x - \delta > r$ 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.

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

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