The rational numbers as an ordered field

Sean Fitzpatrick

September 5th, 2014

In class we introduced the number systems

$$\begin{aligned}\mathbb{N} &= \{1, 2, 3, 4, \ldots\}, \text{ the natural numbers}\\ \mathbb{Z} &= \{\ldots, -2, -1, 0, 1, 2, \ldots\}, \text{ the integers, and}\\ \mathbb{Q} &= \{p/q \mid p, q \in \mathbb{Z} \text{ and } q \neq 0\}, \text{ the rational numbers.}\end{aligned}$$

We discussed how each one can be obtained from the previous, and that the motivation for each is to expand the available algebraic operations that can be performed within the set. (Note that by convention $\mathbb{Z}$ is considered the subset of $\mathbb{Q}$ given by elements of the form $p/1$, which we simply write as p.) The end result is that $\mathbb{Q}$ satisfies the properties of an **ordered field**.

First, we note that $\mathbb{N}$ is equipped with operations of addition $(n+m)$ and multiplication $(n \cdot m$ or simply $nm)$ defined as follows:

$$\begin{aligned}n + m &= n + 1 + 1 + \cdots + 1 \ (m \text{ times})\\ n \cdot m &= n + n + \cdots + n \ (m \text{ times}).\end{aligned}$$

(Technically on the first line we should include appropriate bracketing — e.g. $n + 1$, then $(n + 1) + 1$, then $((n + 1) + 1) + 1$, etc. since we haven't discussed associativity yet.)

The operations of addition and multiplication both satisfy the *commutative* and *associative* properties: for any $a, b, c \in \mathbb{N}$ we have

$$\begin{aligned}a + b &= b + a\\ a \cdot b &= b \cdot a\\ a + (b + c) &= (a + b) + c\\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c.\end{aligned}$$

The first two equalities are the commutativity of addition and multiplication, respectively, while the last two express associativity. If we include zero in $\mathbb{N}$ then both addition and multiplication have identities as well: for any $n \in \mathbb{N}$ we have

$$n + 0 = 0 + n = n \quad \text{and} \quad n \cdot 1 = 1 \cdot n = n.$$

The natural numbers also satisfy the *distributive property*: for any $a, b, c \in \mathbb{N}$ we have that

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

It's possible to verify that this follows from the defintions of addition and multiplication above, although you might be used to thinking of this property in terms of comparing areas. (Imagine a rectangular field of width a and length divided into two parts of lengths b and c respectively.

Expanding $\mathbb{N}$ to the set $\mathbb{Z}$ allows us to have *additive inverses*: for each $n \in \mathbb{Z}$ there is an element $-n \in \mathbb{Z}$ such that

$$n + (-n) = -n + n = 0.$$

The term "inverse" here refers to the fact that addition of one does the opposite of addition of the other. That is, for any other $m \in \mathbb{Z}$, to recover m from $m + n$ we add $-n$:

$$(m + n) + (-n) = m + (n + (-n)) = m + 0 = m.$$

Similarly, by expanding $\mathbb{Z}$ to the rational numbers $\mathbb{Q}$, we are able to introduce *multiplicative inverses* for all elements except for the zero element: for any $n \neq 0$ we have the element $1/n$ such that $n(1/n) = 1$. Just as with addition, multiplication by $1/n$ "undoes" the operation of multiplying by n. Since we don't want the operations of addition and multiplication to take us outside of our set, we want $\mathbb{Q}$ to include products such as $m \cdot (1/n)$, which we write simply as m/n. With these conventions, the set $\mathbb{Q}$ satisfies the axioms of a **field**. A set A is a field if it is equipped with two operations $+$ and $\cdot$ such that whenever $a, b \in A$ we have $a + b \in A$ and $a \cdot b \in A$ (we say A is "closed" under these operations; the operations are also assumed to be uniquely defined), and the operations satisfy the following axioms:

- (A1) For all $a, b \in A$, $a + b = b + a$ (commutativity of $+$)
- (A2) For all $a, b, c \in A$, $a + (b + c) = (a + b) + c$ (associativity of $+$)
- (A3) There exists an element $0 \in A$ such that $a + 0 = a$ for all $a \in A$ (existence of an additive identity)
- (A4) For each $a \in A$ there exists an element $-a \in A$ such that $a + (-a) = 0$ (existence of additive inverses)
- (M1) For all $a, b \in A$, $a \cdot b = b \cdot a$ (commutativity of $\cdot$)
- (M2) For all $a, b, c \in A$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity of $\cdot$)
- (M3) There exists an element $1 \in A$ such that $a \cdot 1 = a$ for all $a \in A$ (existence of a multiplicative identity)
- (M4) For each $a \neq 0 \in A$ there exists an element $1/a \in A$ such that $a \cdot (1/a) = 1$ (existence of multiplicative inverses)
- (D) For each $a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

We note that $\mathbb{Q}$ satisfies these axioms (and so, by the way, does $\mathbb{R}$), so $\mathbb{Q}$ is a field. Recall that an **order relation** on a set A is a relation $a \leq b$ such that

1. $a \leq a$ (the relation is reflexive)

2. If $a \leq b$ and $b \leq a$, then $a = b$ (the relation is anti-commutative)

3. If $a \leq b$ and $b \leq c$, then $a \leq c$ (the relation is transitive)

The relation $a < b$ is distinguished from $a \leq b$ by the "law of trichotomy": for all $a, b \in A$, **exactly one** of the relations $a < b$, $b < a$, and $a = b$ must hold. If we take $a \leq b$ to mean $a < b$ or $a = b$, then trichotomy implies the anti-commutative property. The usual number line order defines an ordering of the sets $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$. A field A is called an **ordered field** if it is equipped with an order relation $a < b$ that is compatible with the field operations $+$ and $\cdot$, in the sense that it satisfies the following two additional axioms:

- (O1) If $a < b$, then $a + c < b + c$ for all $c \in A$.
- (O2) If $a < b$ and $c > 0$, then $ac > bc$.

In particular, both $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields. You should note that the properties of an ordered field are simply a formal way of stating that an ordered field behaves in exactly the way you expect things to behave according to ordinary arithmetic. To make sure you've understood the axioms of an ordered field, you might want to attempt the following exercises:

1. Using only the axioms of an ordered field as given above, show that if A is an ordered field, then for any elements $a, b, c \in A$, we have

   (a) If $a + c = b + c$, then $a = b$.

   (b) $a \cdot 0 = 0$.

   (c) $-0 = 0$

   (d) $(-1) \cdot a = -a$

   (e) $ab = 0$ if and only if $a = 0$ or $b = 0$.

   (f) $a < b$ if and only if $-b < -a$.

   (g) If $a < b$ and $c < 0$, then $ac > bc$.

2. Let A be the set of all rational functions. That is, A is the set of all functions of the form $P(x)/Q(x)$, where $P(x)$ and $Q(x)$ are polynomials, and $Q(x) \neq 0$. Given an element
$$p(x)/q(x) = \frac{a_n x^n + \cdots a_1 x + a_0}{b_k x^k + \cdots b_1 x + b_0},$$
we define $p/q > 0$ if $a_n b_k > 0$; that is, if the product of the leading coefficients on the top and bottom is positive. Given rational functions p/q and f/g, we define
$$\frac{p}{q} > \frac{f}{g} \text{ if and only if } \frac{p}{q} - \frac{f}{g} > 0.$$
Check that A is an ordered field with respect to the usual addition and multiplication of functions.