The reals as cuts

George Sparling
Laboratory of Axiomatics
August 31, 2014

The defining properties of the natural numbers

We begin with the natural numbers \( \mathbb{N} \): these can be added and multiplied and are ordered (obeying all the usual rules of basic number theory); also they have a multiplicative identity 1.

Specifically we have, when \( a, b \) and \( c \) are in \( \mathbb{N} \):

- \( a + b \in \mathbb{N} \) and \( ab \in \mathbb{N} \),
- \( a + b = b + a \) and \( (a + b) + c = a + (b + c) \),
- \( ab = ba \) and \( (ab)c = a(bc) \),
- \( a(b + c) = ab + ac \) and \( (b + c)a = ba + bc \),
- \( 1(a) = a(1) = 1 \).
- If \( S \) is a subset of \( \mathbb{N} \) such that \( 1 \in S \) and if \( k \in S \), then \( k + 1 \in S \), then \( S = \mathbb{N} \).

We remind ourselves of the following key properties:

- For \( a, b \) and \( c \) elements of \( \mathbb{N} \), we have additive cancellation:
  \[
  \text{If } a + b = a + c, \text{ then } b = c.
  \]

- For \( a, b \) and \( c \) elements of \( \mathbb{N} \), we have multiplicative cancellation:
  \[
  \text{If } ab = ac, \text{ then } b = c.
  \]
Next we define the ordering of $\mathbb{N}$:

- If $p$ and $q$ are in $\mathbb{N}$, then $p > q$ if and only if there exists $r \in \mathbb{N}$ (necessarily unique by additive cancellation), such that $p = q + r$.

The ordering properties are:

- Trichotomy: for $a$ and $b$ elements of $\mathbb{N}$, exactly one of $a < b$, $b < a$, $a = b$ holds.

- Transitivity: for $a$, $b$ and $c$ elements of $\mathbb{N}$, if $a < b$ and $b < c$, then $a < c$.

- For $a$, $b$ and $c$ elements of $\mathbb{N}$, if $a < b$ then $ca < cb$.

- For any $x \in \mathbb{N}$, we have $x < 1$ is false.

We can also add 0 to the natural numbers.

For any $0 \notin \mathbb{N}$, put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, equipped with the additional rules, valid for any $x \in \mathbb{N}$: $0 < x$, whereas $x < 0$ is false, $0 + x = x + 0 = x$ and $0x = x0 = 0$; also $00 = 0$ and $0 + 0 = 0$.

Note that for $\mathbb{N}_0$ additive cancellation still holds, namely that for $a$, $b$ and $c$ in $\mathbb{N}_0$, if $a + b = a + c$, then $b = c$, but multiplicative cancellation is modified to: if $ab = ac$, for $a$, $b$ and $c$ in $\mathbb{N}_0$, then $a = 0$ or $b = c$. 


Operations on \( \mathbb{N}^2 \)

Now consider \( \mathbb{N}^2 = \{(x, y) : x \in \mathbb{N} \text{ and } y \in \mathbb{N}\} \).

If \( a \) and \( b \) are in \( \mathbb{N}^2 \), so \( a = (p, q) \) and \( b = (r, s) \), for \( p, q, r \) and \( s \) in \( \mathbb{N} \), we define:

- \( a + b = (ps + qr, qs) \),
- \( ab = (pr, qs) \),
- \( a > b \) if and only if \( ps > qr \).

These operations are commutative and associative and there is a multiplicative identity, namely \((1, 1)\).

By repeated addition of \((1, 1)\) to itself, we can generate a copy of \( \mathbb{N} \), with the correct induced operations for \( \mathbb{N} \), as the set of all \((n, 1) \in \mathbb{N}^2\) such that \( n \in \mathbb{N} \).

Note however that multiplication is in general not distributive over addition: for example we have:

\[
(3, 2)((5, 2) + (7, 2)) = (3, 2)(24, 4) = (72, 8),
\]

\[
(3, 2)(5, 2) + (3, 2)(7, 2) = (16, 4) + (20, 4) = (144, 16).
\]

The ordering properties are:

- Anti-symmetry: for \( a \in \mathbb{N} \), \( a < a \) is false.
- Transitivity: for \( a, b \) and \( c \) elements of \( \mathbb{N} \), if \( a < b \) and \( b < c \), then \( a < c \).
- For \( a, b \) and \( c \) elements of \( \mathbb{N} \), if \( a < b \) then \( ca < cb \).

Operations on subsets of \( \mathbb{N}^2 \)

Let \( r \) and \( s \) be subsets of \( \mathbb{N}^2 \).

- Define \( r + s = \{a + b : a \in r, b \in s\} \).
- Define \( rs = \{ab : a \in r, b \in s\} \).

These operations are associative and commutative.
Defining the set $\mathbb{R}^+$ of extended positive reals

Now we can define the extended positive reals.

- Let $s \subset \mathbb{N}^2$.
  We say that $s$ is upper complete if when $a \in s$, then $b \in s$, for any $b \in \mathbb{N}^2$, such that $b > a$.

- Let $s \subset \mathbb{N}^2$.
  We say that $s$ is downwardly open, if given any $c \in s$, there exists $d \in s$, such that $d < c$.

Then the set of extended positive reals, denoted $\mathbb{R}^+$, is by definition the set of subsets $r$ of $\mathbb{N}^2$, such that $r$ is both upper complete and downwardly open. The addition and multiplication operations of $\mathbb{R}^+$ are those of subsets of $\mathbb{N}^2$, as just defined above.

The ordering for $\mathbb{R}^+$ is given by the relation $r \leq s$, for $r$ and $s$ in $\mathbb{R}^+$ if and only if $s \subset r$.

Examples

- The empty set $\emptyset$ is in $\mathbb{R}^+$, since it obeys the defining conditions of a real vacuously.
  This extended positive real is denoted $\infty$.
  We have $x \leq \infty$ for any $x \in \mathbb{R}^+$.
  If $x \in \mathbb{R}^+$ obeys $x < \infty$, then $x$ is said to be finite.

- The set $\mathbb{N}^2$ is in $\mathbb{R}^+$.
  This extended positive real is denoted $0$.
  We have $x \geq 0$ for any $x \in \mathbb{R}^+$.
  If $x \in \mathbb{R}^+$ obeys $x > 0$, then $x$ is said to be positive.

- If $a \in \mathbb{N}^2$, put $[a] = \{x \in \mathbb{N}^2 : x > a\}$.
  Then $[a]$ is a positive real.
  $[a]$ is called a rational number.
  Note that for $a$ and $b$ in $\mathbb{N}^2$, we have $[a] = [b]$ if and only if $a < b$ and $b < a$ are both false.
  If $a = (p, q)$ we often denote the rational number $[a]$ by $[a] = \frac{p}{q}$.

  Then for example, we have $[(9, 6)] = [(120, 80)] = [(3, 2)] = \frac{9}{6} = \frac{120}{80} = \frac{3}{2}$.
• Let \( z = \{(x, y) \in \mathbb{N}^2 : xx > yy + yy\} \).
  Then \( z \) is a real number that is not rational. The extended positive real \( z \) is denoted \( \sqrt{2} \).

• Let \( t = \{(x, y) \in \mathbb{N}^2 : xx > yy + yy + yy\} \).
  Then \( t \) is a real number that is not rational. The extended positive real \( t \) is denoted \( \sqrt{3} \).

A (formal) polynomial in two variables, with coefficients in \( \mathbb{N}_0 \) is a map \( p : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0 \). We add two such polynomials term-wise:

\[
(p + q)(s, t) = p(s, t) + q(s, t), \text{for any } (s, t) \in \mathbb{N}_0 \times \mathbb{N}_0
\]

We multiply by convolution:

\[
(pq)(s, t) = \sum_{s_1+s_2=s, t_1+t_2=t, (s_1,s_2,t_1,t_2) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0} p(s_1, t_1)q(s_2, t_2), \text{ for any } (s, t) \in \mathbb{N}_0 \times \mathbb{N}_0.
\]

We write \( p \) as:

\[
p(x, y) = \sum_{a=(a_1, a_2) \in \mathbb{N}_0 \times \mathbb{N}_0} p(a)x^{a_1}y^{a_2}.
\]

A polynomial \( p \) is said to be homogenous of degree \( n \in \mathbb{N}_0 \), if \( p(a) \) vanishes for any \( a = (a_1, a_2) \in \mathbb{N}_0 \times \mathbb{N}_0 \) with \( a_1 + a_2 \neq n \). A (non-formal) polynomial is a finite sum of homogeneous polynomials. The sum and product of non-formal polynomials is again non-formal. For example, the polynomial \((x + y)^n\) is homogeneous of degree \( n \). We have:

\[
(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.
\]

Here the positive integer \( \binom{n}{k} \), called a binomial coefficient, is determined uniquely by the formula, valid for any non-negative integers \( r \) and \( s \):

\[
r!s! \binom{r+s}{r} = (r+s)!.
\]

Here the formulas \( 0! = 1 \), \( 1! = 1 \) and \( (k+1)! = k!(k+1) \), for any \( k \in \mathbb{N} \), defines the factorial function recursively.
• For \( p(x, y) \) and \( q(x, y) \) homogenous polynomials in variables \( x \) and \( y \), with coefficients in \( \mathbb{N} \), of the same degree, put:

\[
[[p, q]] = \{(a, b) \in \mathbb{N}^2 : p(a, b) > q(a, b) \text{ and if } (c, d) > (a, b), \text{ then } p(c, d) > q(c, d)\}.
\]

Then \( [[p, q]] \) is an extended real number: \( [[p, q]] \) is called an extended positive algebraic number. In general a positive real number \( \alpha \) is said to be algebraic if there exists positive integers \( r, s \) and \( t \) and an extended positive algebraic number \( \beta = [[p, q]] \), for some \( p(x, y) \) and \( q(x, y) \) homogenous polynomials in variables \( x \) and \( y \), with coefficients in \( \mathbb{N} \), such that \( r\alpha \beta = s\beta + t \). All the preceding examples of real numbers that we have given are algebraic, as is easily seen.

• For \( n \) a positive integer, put \( s_n = \sum_{k=0}^{n} \left( \frac{n!}{k!} \right) \).

The sequence \( S = \{s_n : n \in \mathbb{N}\} \) begins:

\[
2, 5, 16, 65, 326, 1957, 13700, 109601, 9864101, \ldots.
\]

Then define:

\[
e = \{a \in \mathbb{N}^2 : a > (s_n, n!), \text{ for all } n \in \mathbb{N}\}.
\]

Note that the sequence \( (s_n, n!) \) is increasing, since we have the recursion \( s_{n+1} = 1 + (n + 1)s_n \), which implies the relation \( s_{n+1}n! - s_n(n + 1)! = n! \), valid for each \( n \in \mathbb{N}_0 \), which gives the formula: \( (s_n, n!) = \sum_{k=0}^{n} (1, k!) \), for any \( n \in \mathbb{N} \).

Then \( e \) is an extended positive real number and is transcendental: it is not algebraic.

In particular, we have the rational bound:

\[
[27182818284590, 10000000000000] < e < [27182818284591, 100000000000000].
\]
Supremum and infimum

Let $S \subset \mathbb{R}^+$. 

- $\inf(S) = \bigcup_{s \in S}$.
- $\sup(S) = \inf\{t \in \mathbb{R}^+ : t > s, \text{ for all } s \in S\}$.

The set $S$ is said to be bounded above if and only if $\sup(S)$ is finite, if and only if there exists a finite positive real $r \in \mathbb{R}^+$, such that $s \leq r$, for all $s \in S$.

- If $S$ is a finite set, then $\sup(S) = \bigcap_{s \in S} s$.

Examples

- For $S = \{(1, n) : n \in \mathbb{N}\}$, we have $\inf(S) = 0$ and $\sup(S) = (1, 1)$. This is a version of the Archimedean Principle.
- For $S = \{(n, 1) : n \in \mathbb{N}\}$, we have $\inf(S) = (1, 1)$ and $\sup(S) = \infty$. This is another version of the Archimedean Principle.
- For $S = \{(3, 10), (33, 100), (333, 1000), (3333, 10000), \ldots\}$, we have $\inf(S) = (3, 10)$ and $\sup(S) = (1, 3)$.
- For $S = \{(s_n, n!) : n \in \mathbb{N}_0\}$, where $s_n = \sum_{k=0}^{n} \frac{(n)!}{k! \binom{n}{k}}$, for any $n \in \mathbb{N}$, we have $\inf(S) = (2, 1)$ and $\sup(S) = e$.  


Properties of 0 and $\infty$

Note the properties of the extended positive reals 0 and $\infty$:

- For every $x \in \mathbb{R}^+$, we have $0 \leq x \leq \infty$.
- If $x \in \mathbb{R}^+$ obeys $x \geq (n, 1)$, for all $n \in \mathbb{N}$, then $x = \infty$.
- If $x \in \mathbb{R}^+$ obeys $x \leq (1, n)$, for all $n \in \mathbb{N}$, then $x = 0$.
- We have:
  
  $$0 + 0 = 0, \quad 0 + \infty = \infty, \quad \infty + \infty = \infty.$$  
- We have:
  
  $$0 \cdot 0 = 0, \quad 0 \cdot \infty = \infty, \quad \infty \cdot \infty = \infty.$$  
- For every extended positive real $x$, we have:
  
  $$0 + x = x, \quad x + \infty = \infty.$$  
- For every extended positive real $x$ that is finite, i.e. $x \neq \infty$, we have:
  
  $$0 \cdot x = 0, \quad x \cdot \infty = \infty.$$  
- We have, for extended positive reals $a$ and $b$:
  
  $$a + b = 0, \text{ iff } a = b = 0,$$
  
  $$a + b = \infty, \text{ iff } a = \infty, \text{ or } b = \infty,$$
  
  $$ab = 0, \text{ iff both } a \text{ and } b \text{ are finite and } a = 0 \text{ or } b = 0,$$
  
  $$ab = 0, \text{ iff } a = \infty \text{ or } b = \infty.$$  

8
The full real number system

A (formal) polynomial in one variable, with coefficients in \( \mathbb{R}^+ \) is by definition a map from \( \mathbb{N}_0 \) to \( \mathbb{R}^+ \). We add and multiply such polynomials by the rules, valid for any polynomials \( f \) and \( g \) and for each \( n \in \mathbb{N}_0 \):

\[
(f + g)(n) = f(n) + g(n),
\]
\[
(fg)(n) = \sum_{r+s=n, (r,s) \in \mathbb{N}_0 \times \mathbb{N}_0} f(r)g(s).
\]

For each \( k \in \mathbb{N}_0 \), the polynomial \( f = x^k \) is defined by the formulas, for \( n \in \mathbb{N} \):

\[
x^k(n) = 0, \text{ unless } n = k,
\]
\[
x^k(k) = 1.
\]

Then we have \( x^k x^m = x^{k+m} \), for any \( k \) and \( m \) in \( \mathbb{N}_0 \).

We then often write for the general polynomial \( f \):

\[
f(x) = \sum_{k=0}^{\infty} f(k)x^k.
\]

The degree of \( f \neq 0 \) is the smallest \( n \in 0 \cup \mathbb{N} \cup \infty \), such that \( f(j) = 0 \), for all integral \( j > n \). Then the sum representing \( f \) is a formal sum unless \( f \) has finite degree, in which case \( f \) is just called a polynomial and then \( f \) is just a finite sum of its non-zero terms.
Let \( m \) be a polynomial with coefficients in \( \mathbb{R}^+ \). We define a relation \( \mod m \) (called stable equivalence modulo \( m \)) on formal polynomials with coefficients in \( \mathbb{R}^+ \), by the formula, for formal polynomials \( f \) and \( g \):

- \((f, g) \in \mod m\), if and only if there exist formal polynomials \( p \) and \( q \), such that:
  \[
  f + pm = g + qm.
  \]

When \((f, g) \in \mod m\), we write \( f \equiv_m g \).

It is routine to prove that \( \mod m \) is an equivalence relation and that the operations of multiplication and addition of polynomials respect the equivalence relations, so pass down to the equivalence classes.

- When \( m(x) = x + 1 \), the space of equivalence classes modulo \( m \) of all polynomials (of finite degree), with finite coefficients in \( \mathbb{R}^+ \), is, by definition, the set \( \mathbb{R} \) of reals.

- When \( m(x) = x^2 + 1 \), the space of equivalence classes modulo \( m \) of all polynomials (of finite degree), with finite coefficients in \( \mathbb{R}^+ \), is, by definition, the set \( \mathbb{C} \) of complex numbers.

The non-zero finite elements of \( \mathbb{R}^+ \) embed into \( \mathbb{R} \) as the (equivalence classes of) polynomials of zero degree. The zero element of \( \mathbb{R} \) is the polynomial \( x + 1 \); the additive inverse of 1 is \( x \). We have the relation \( x^2 = 1 \) in \( \mathbb{R} \), by the formula:

\[
x^2 \equiv_{x+1} x^2 + 1(x + 1) = x^2 + x + 1 = 1 + (x^2 + x) \equiv_{x+1} 1 + x(x + 1).
\]

In \( \mathbb{C} \), the additive inverse of 1 is \( x^2 \) and we have \( x^4 \equiv_{x^2+1} 1 \). The reals embed inside \( \mathbb{C} \), by the mapping \( f(x) \rightarrow f(x^2) \), for any \( f(x) \) representing an element of \( \mathbb{R} \).