Algebraic Structures of Numbers

Andrejs Treibergs

University of Utah

September 8, 2009

2. Peano Axioms

Here are the basic axioms for the Natural Numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$.

N1. There is an element $1 \in \mathbb{N}$;

N2. there is $s : \mathbb{N} \to \mathbb{N}$ called the *successor function;*

N3. 1 is not the successor of any element of $\mathbb{N}$ ($1 \notin s(\mathbb{N})$);

N4. if two elements have the same successor, then they are equal $((\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(s(n) = s(m) \implies n = m)$.

N5. if a subset $A \subset \mathbb{N}$ contains 1 and is closed under succession $((\forall n \in \mathbb{N})(n \in A \implies s(n) \in A))$ then $A = \mathbb{N}$.

3. How addition and multiplication operations are defined.

Addition is an operation $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. For each $m \in \mathbb{N}$, the sequence $\{m + n\}_{n \in \mathbb{N}}$ is defined inductively as follows: First we specify for $n = 1$

$$m + 1 := s(m).$$

Then assuming $m + n$ has been specified, we specify the next

$$m + s(n) := s(m + n),$$

i.e., $m + (n + 1) = (m + n) + 1$.

Multiplication is an operation $\times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. For each $m \in \mathbb{N}$, the sequence $\{m \times n\}_{n \in \mathbb{N}}$ is defined inductively as follows: First we specify for $n = 1$

$$m \times 1 := m.$$

Then assuming $m \times n$ has been specified, we specify the next

$$m \times s(n) := (m \times n) + m,$$

i.e., $m(n + 1) = (mn) + m$.

4. Then the axioms for the integers are proved for the operations.

For example, we prove that the associative law holds for addition.

Theorem

For all $m, n, k \in \mathbb{N}$ there holds $m + (n + k) = (m + n) + k$.

Proof. We fix $m, n \in \mathbb{N}$ and argue by induction on $k \in \mathbb{N}$.
Base case $k = 1$. Follows from the definition of "+" since

$$m + (n + 1) = m + s(n) = s(m + n) = (m + n) + 1.$$

For induction, assume for $k \in \mathbb{N}$ we have $(m + n) + k = m + (n + k)$.
Then for the successor,

$$\begin{aligned}
(m + n) + (k + 1) &= (m + n) + s(k) \\
&= s\big((m + n) + k\big) && \text{by def. "+"} \\
&= s(m + (n + k)) && \text{by induction hypothesis} \\
&= m + s(n + k) && \text{by def. "+"} \\
&= m + \big(n + s(k)\big) && \text{by def "+"} \\
&= m + \big(n + (k + 1)\big). \qquad \square
\end{aligned}$$

In similar fashion, one checks the arithmetic properties of $\mathbb{N}$.

Properties of $(\mathbb{N}, +, \times)$.

A1. [Commutative $+$] $x + y = y + x$ for all $x, y \in \mathbb{N}$;

A2. [Associative $+$] $x + (y + z) = (x + y) + z$ for all $x, y, z \in \mathbb{N}$;

M1. [Commutative $\times$] $xy = yx$ for all $x, y \in \mathbb{N}$;

M2. [Associative $\times$] $x(yz) = (xy)z$ for all $x, y, z \in \mathbb{N}$;

M3. [$\times$ Identity] There is $1 \in \mathbb{N}$ s.t. $1x = x$ for all $x \in \mathbb{N}$;

D. [Distributive] $x(y + z) = (xy) + (xz)$ for all $x, y, z \in \mathbb{N}$.

6. Then order $>$ is defined on $\mathbb{N}$.

We say that two numbers $p, q \in \mathbb{N}$ such that $p \neq q$ satisfy $p < q$ if there is $k \in \mathbb{N}$ such that $q = k + p$.

One checks that the trichotomy holds: given $m, n \in \mathbb{N}$ exactly ONE of the following is true:

$$m < n; \qquad m = n; \qquad m > n.$$

7. Definition of the Integers.

As a set, the integers are the disjoint union of two copies of natural numbers called the positive numbers $\{n\}_{n\in\mathbb{N}}$, the negative numbers $\{-n\}_{n\in\mathbb{N}}$ and the singleton $\{0\}$.

$$\mathbb{Z} = \{1, 2, 3, \ldots) \amalg \{0\} \amalg \{-1, -2, -3, \ldots\}.$$

Addition $+_{\mathbb{Z}}$, multiplication $\times_{\mathbb{Z}}$ and order $<_{\mathbb{Z}}$ are defined from $(\mathbb{N}, +, \times, <)$ case by case, depending whether p and q are positive. For example $p +_{\mathbb{Z}} q = p + q$, $p + 0 = p$, and for positive p and negative $-q$,

$$p +_{\mathbb{Z}} (-q) = \begin{cases} k, & \text{if } p > q \text{ where } p = q + k; \\ 0, & \text{if } p = q; \\ -k, & \text{if } p < q \text{ where } q = p + k. \end{cases}$$

Similarly, $\times_{\mathbb{Z}}$ and $<_{\mathbb{Z}}$ are defined from $\times$ and $<$.

Then one checks that the integers, now called $(\mathbb{Z}, +, \times)$, satisy the axioms of a commutative ring.

Axioms of a commutative ring $(R, +, \times)$.

A1. [Commutative $+$] $x + y = y + x$ for all $x, y \in R$

A2. [Associative $+$] $x + (y + z) = (x + y) + z$ for all $x, y, z \in R$

A3. [$+$ Identity] There is $0 \in R$ s.t. $x + 0 = x$ for all $x \in R$

A4. [$+$ Inverse.] For all $x \in R$ there is a $-x \in R$ s.t. $x + (-x) = 0$.

M1. [Commutative $\times$] $xy = yx$ for all $x, y \in R$

M2. [Associative $\times$] $x(yz) = (xy)z$ for all $x, y, z \in R$

M3. [$\times$ Identity] There is $1 \in R \backslash \{0\}$ s.t. $1x = x$ for all $x \in R$

D. [Distributive] $x(y + z) = (xy) + (xz)$ for all $x, y, z \in R$

9. More Properties of a Commutative Ring.

The following among many other familiar familiar arithmetic properties can be deduced from the axioms of a commutative ring.

- The additive identity 0 is unique.
- The multiplicative identity 1 is unique.
- For all $x \in R$ the additive inverse $-x$ is unique.
- For all $a, x \in R$, if $a = a + x$ then $x = 0$.
- For all $x, y, z \in R$, if $x + y = x + z$ then $y = z$.
- For all $x \in R$, $x \cdot 0 = 0$.
- For all $x, y \in R$, $(-x) \cdot y = -(x \cdot y)$.

Axioms of a Field $(F, +, \times)$**.**

A1. [Commutative $+$] $x + y = y + x$ for all $x, y \in F$

A2. [Associative $+$] $x + (y + z) = (x + y) + z$ for all $x, y, z \in F$

A3. [$+$ Identity] There is $0 \in F$ s.t. $x + 0 = x$ for all $x \in F$

A4. [$+$ Inverse.] For all $x \in F$ there is a $-x \in F$ s.t. $x + (-x) = 0$.

M1. [Commutative $\times$] $xy = yx$ for all $x, y \in F$

M2. [Associative $\times$] $x(yz) = (xy)z$ for all $x, y, z \in F$

M3. [$\times$ Identity] There is $1 \in F \backslash \{0\}$ s.t. $1x = x$ for all $x \in F$

M4. [$\times$ Inverse.] For all $x \in F \backslash \{0\}$ there is a $x^{-1} \in F$ s.t. $x \cdot (x^{-1}) = 1$.

D. [Distributive] $x(y + z) = (xy) + (xz)$ for all $x, y, z \in F$

11. Construction of the Rational Numbers $\mathbb{Q}$.

As a set, the rational numbers are equivalence classes of pairs of integers

$$\mathbb{Q} = \left\{ \frac{n}{m} : n \in \mathbb{Z}, \quad m \in \mathbb{Z}\backslash\{0\} \right\} / \sim$$

where two symbols are equivalent

$$\frac{n}{m} \sim \frac{p}{q} \qquad \Longleftrightarrow \qquad mp = nq.$$

The symbols can be thought of as "ordered pairs" and the quotient as the collection of equivalence classes

$$\left[\frac{n}{m}\right] = \left\{ \frac{p}{q} : \ p \in \mathbb{Z} \text{ and } q \in \mathbb{Z}\backslash\{0\} \text{ such that } nq = mp. \right\}.$$

In other words, a rational number is a set of all symbols that are equivalent to each other. Any of the symbols $\frac{a}{b} \in \left[\frac{n}{m}\right]$ is called a representative of the equivalence class.

12. Addition, Multiplication and Inversion in $\mathbb{Q}$.

The sum of two equivalence classes is defined to be the equivalence class of the sum

$$\left[\frac{n}{m}\right] + \left[\frac{p}{q}\right] := \left[\frac{nq + mp}{mq}\right].$$

The product of two equivalence classes is defined to be the equivalence class of the product

$$\left[\frac{n}{m}\right] \cdot \left[\frac{p}{q}\right] := \left[\frac{np}{mq}\right].$$

The role of the additive and multiplicative identities and additive inverse are the equivalence classes

$$\text{Add. Id.} = \left[\frac{0}{1}\right]; \qquad \text{Mult. Id.} = \left[\frac{1}{1}\right]; \qquad -\left[\frac{n}{m}\right] = \left[\frac{-n}{m}\right].$$

A nonzero equivalence class $\left[\frac{n}{m}\right] \neq \left[\frac{0}{1}\right]$ means $n \cdot 1 \neq 0 \cdot m$ or $n \neq 0$. Thus its multiplicative inverse is defined to be the equivalence class of the inverse

$$\left[\frac{n}{m}\right]^{-1} := \left[\frac{m}{n}\right].$$

13. Addition, Multiplication and Inversion in $\mathbb{Q}$ are Well Defined.

First we have to show that these are well defined. This means, if we choose different representatives from the input equivalence classes, then the formulas give the same equivalence class for the output.
E.g., to show addition is well defined, we choose different representatives

$$\frac{n'}{m'} \in \left[\frac{n}{m}\right], \quad \frac{p'}{q'} \in \left[\frac{p}{q}\right] \quad \text{so} \quad \left[\frac{n'}{m'}\right] = \left[\frac{n}{m}\right] \quad \text{and} \quad \left[\frac{p'}{q'}\right] = \left[\frac{p}{q}\right].$$

By the meaning of equivalence,

$$n'm = m'n \quad \text{and} \quad p'q = q'p. \tag{1}$$

We wish to show

$$\frac{n'q' + m'p'}{m'q'} \sim \frac{nq + mp}{mq}. \tag{2}$$

But by (1),

$$(n'q' + m'p')mq = n'mq'q + m'mp'q = m'nqq' + mm'q'p = (nq + mp)m'q'$$

thus (2) holds. Thus the class of the sum does not depend on the representatives of the summands.

The well definedness of the other operations is similar.

14. $(\mathbb{Q}, +, \times)$ is a Field.

One uses the ring properties of $\mathbb{Z}$ to show the field properties of $\mathbb{Q}$. *E.g.*, to show A2, addition is associative, we choose representatives

$$\frac{n}{m} \in \left[\frac{n}{m}\right], \quad \frac{p}{q} \in \left[\frac{p}{q}\right] \qquad \text{and} \qquad \frac{u}{v} \in \left[\frac{u}{v}\right]$$

To show

$$\left(\left[\frac{n}{m}\right] + \left[\frac{p}{q}\right]\right) + \left[\frac{u}{v}\right] = \left[\frac{n}{m}\right] + \left(\left[\frac{p}{q}\right] + \left[\frac{u}{v}\right]\right)$$

We have to show

$$\left(\left[\frac{n}{m}\right] + \left[\frac{p}{q}\right]\right) + \left[\frac{u}{v}\right] = \left[\frac{nq+mp}{mq}\right] + \left[\frac{u}{v}\right] = \left[\frac{(nq+mp)v+mqu}{mqv}\right]$$

equals

$$\left[\frac{n}{m}\right] + \left(\left[\frac{p}{q}\right] + \left[\frac{u}{v}\right]\right) = \left[\frac{n}{m}\right] + \left[\frac{pv+qu}{qv}\right] = \left[\frac{nqv+m(pv+qu)}{mqv}\right].$$

Since the denominators are the same, this follows from numerators being the same

$$(nq + mp)v + mqu = nqv + m(pv + qu).$$

The other field axioms have similar arguments.

The ordering in $\mathbb{Z}$ extends to $\mathbb{Q}$. We declare

$$\left[\frac{n}{m}\right] \leq \left[\frac{p}{q}\right] \qquad \Longleftrightarrow \qquad (nq - mp)mq \leq 0.$$

One checks well definedness.
With this order, $(\mathbb{Q}, +\times, \leq)$ is an ordered field.

Axioms of an Ordered Field $(F, +, \times, \leq)$.
The binary relation"$\leq$" on the field $(F, +, \times)$ is an ordering if for all $x, y, z \in F$

O1. either $x \leq y$ or $y \leq x$;

O2. if $x \leq y$ and $y \leq x$ then $x = y$;

O3. if $x \leq y$ and $y \leq z$ then $x \leq z$;

O4. if $x \leq y$ then $x + z \leq y + z$;

O5. if $x \leq y$ and $0 \leq z$ then $xz \leq yz$.

The ordering in $\mathbb{Z}$ extends to $\mathbb{Q}$. We declare

$$\left[\tfrac{n}{m}\right] \leq \left[\tfrac{p}{q}\right] \qquad \Longleftrightarrow \qquad (nq - mp)mq \leq 0.$$

Let us check that O3, transitivity, holds in $(\mathbb{Q}, +\times, \leq)$. To show

$$\left[\tfrac{n}{m}\right] \leq \left[\tfrac{p}{q}\right] \qquad \text{and} \qquad \left[\tfrac{p}{q}\right] \leq \left[\tfrac{u}{v}\right] \qquad \Longrightarrow \left[\tfrac{n}{m}\right] \leq \left[\tfrac{u}{v}\right]$$

The first two mean $(nq - mp)mq \leq 0$ and $(pv - uq)qv \leq 0$.
Note that $\left[\tfrac{n}{m}\right] = \left[\tfrac{-n}{-m}\right]$ since $n(-m) = (-n)m$. Thus we may assume $m > 0$, $p > 0$ and $v > 0$ by replacing numerator and denominator by their additive inverses if necessary. Also note in $\mathbb{Z}$, for $a > 0$, if $ab \leq 0$ then $b \leq 0$. Equivalently, if $b > 0$ then $ab > 0$.
Multiplying by $v^2, m^2 > 0$ we get $v^2nmq^2 - m^2v^2pq \leq 0$ and $m^2pqv^2 - m^2q^2uv \leq 0$. Adding we get $q^2mv(vn - mu) \leq 0$ so by the note, $(nv - mu)mv \leq 0$. Hence $\left[\tfrac{n}{m}\right] \leq \left[\tfrac{u}{v}\right]$. □

17. More Properties of an Ordered Field.

The following properties can be deduced from the axioms of an ordered field $(F, +, \times, \leq)$

- For all $x, y \in F$, if $x \leq y$ then $-y \leq -x$;
- For all $x \in F$, $x^2 \geq 0$;
- $0 < 1$;
- For all $x, y \in F$, if $x > 0$ and $y > 0$ then $xy > 0$.
- For all $x \in F$, if $x > 0$ then $x^{-1} > 0$.
- For all $x, y \in F$, if $0 < x < y$ then $y^{-1} < x^{-1}$.