From Naturals to Integers

John McCuan

January 28, 2020

In the construction of numbers for analysis, once one consents to the logical and set theoretic "foundations," such as they are, and constructs the set

$$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$$

with $0 = \phi$, $1 = \{\phi\} = \{1\}$ and so on, then there are usually three more steps or constructions to get to the real numbers $\mathbb{R}$. Having discussed equivalence relations, groups, rings, fields and order relations, we may review some of the details of the extensions. These may be represented diagramatically by

$$\mathbb{N}_0 \xrightarrow{\nu_0} \mathbb{Z} \xrightarrow{\phi} \mathbb{Q} \xrightarrow{\gamma} \mathbb{R}.$$

As mentioned in regard to our construction of $\mathbb{N}_0$, there are many important results in arithmetic of the natural numbers (not to mention details in the construction itself) which we will use without explicitly proving them. The same applies to the integers $\mathbb{Z}$. One should, hopefully, get the feeling that these results "can be proved" and have some idea of "how the proof would go." And, of course, one should prove some of them—or as many as one can.

I have chosen the symbols[1] ν_0, ϕ, and γ as follows:

- ν_0 (the Greek letter "nu" pronounced "new") for "negatives"
- ϕ (the Greek letter "phi" pronounced "fee") for "fractions"
- γ (the Greek letter "gamma" pronounced "gam-ma") for "complete"

It is possible to, and Gunning does, start with $\mathbb{N} = \{1, 2, 3, \ldots\}$. I think we will not need to refer formally to the injection of $\mathbb{N}$ into $\mathbb{N}_0$ (or of $\mathbb{N}$ into $\mathbb{Z}$) but if we do, we

[1] We could also take γ for "cuts" or δ for "Dedikind cuts" here, but we shall follow Gunning (who followed Cantor) using the notion of **Cauchy sequences** and hence that of **metric completeness**.

can take $\zeta : \mathbb{N} \to \mathbb{N}_0$ and $\nu : \mathbb{N} \to \mathbb{Z}$ so that $\nu = \nu_0 \circ \zeta$ is the restriction of ν_0 to $\mathbb{N} \subset \mathbb{N}_0$.

Generally speaking, especially at each stage of the construction, the sets $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ will consist of elements which may look unfamiliar and should be thought of as quite different and distinct from the antecedent sets—because at each stage they are quite different elements. Once the construction is accomplished, however, it is customary to only consider the initial fundamental set, say $\mathbb{N}_0$, as a subset of the newly constructed set, say $\mathbb{Z}$. Furthermore, somewhat paradoxically, the actual form of the constructed set $\mathbb{Z}$ is "forgotten" and the notation from the injected antecedent set is adopted (at least to whatever extent possible) and extended as appropriate. This comment should become clear after one or two of the constructions/extensions have been explained.

Our objective here is to discuss/summarize some of the most important details for the construction of $\mathbb{Z}$ from $\mathbb{N}_0$, that is the map $\nu_0 : \mathbb{N}_0 \to \mathbb{Z}$ which appends the negative integers to $\mathbb{N}_0$. The construction may be thought of in two steps

$$\mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \to (\mathbb{N}_0 \times \mathbb{N}_0)/\sim = \mathbb{Z}$$

where $\mathbb{N}_0 \times \mathbb{N}_0 = \{(m, n) : m, n \in \mathbb{N}_0\}$ is the Cartesian product and "$\sim$" is a certain equivalence relation. To be specific $(m, n) \sim (r, s)$ if $m - n = r - s$ (but we are not allowed to say this because we are limited to $\mathbb{N}_0$ and $m - n = m + (-n)$ and $r - s = r + (-s)$ are not well-defined in $\mathbb{N}_0$ because $\mathbb{N}_0$, having no additive inverses, is not a group). Thus, we say instead

$$(m, n) \sim (r, s) \qquad \Longleftrightarrow \qquad m + s = n + r.$$

Therefore, elements of $\mathbb{Z}$ (integers) initially have the rather unappealing form

$$[(m, n)] = \{(r, s) \in \mathbb{N}_0 \times \mathbb{N}_0 : m + s = n + r\}$$

with the integers $n \in \mathbb{N}_0$ taking the form

$$[(n, 0)],$$

or if you take Gunning's approach, the even more cumbersome $[(n + 1, 1)]$.

Here are the important results to prove:

Theorem 1 $\mathbb{Z} = (\mathbb{N}_0 \times \mathbb{N}_0)/\sim$ *is an* **additive group** *under the operation*

$$[(m, n)] + [(r, s)] = [(m + n, r + s)]$$

with additive identity

$$[(0,0)] = [(1,1)]$$

and for which the additive inverse of $[(n,0)]$ *is* $[(0,n)]$.

Theorem 2 $\nu_0 : \mathbb{N}_0 \to \mathbb{Z}$ *is an injection by* $\nu_0(n) = [(n,0)]$*, and the "negative" integers*

$$\{[(0,n)] : n \in \mathbb{N}\}$$

are disjoint from the positive integers $\nu_0(\mathbb{N})$ *and* $\{[(0,0)]\} = \{\nu_0(0)\}$*, so that*

$$\{[(0,n)] : n \in \mathbb{N}\} \cup \{[(0,0)]\} \cup \{[(n,0)] : n \in \mathbb{N}\}$$

is a partition of $\mathbb{Z}$.

Theorem 3 $\mathbb{Z}$ *is a* **ring** *with multiplication*

$$[(m,n)][(r,s)] = [(m-n)(r-s),0)] = [(mr+ns, ms+nr)]$$

the middle expression being "wrong" but equivalent to the last one. Furthermore, $\nu_0 : \mathbb{N}_0 \to \mathbb{Z}$ *is a "bimonoid morphism" in the sense that*

$$\begin{aligned} \nu_0(m+n) &= \nu_0(m) + \nu_0(n), \text{ and} \\ \nu_0(mn) &= \nu_0(m)\nu_0(m) \text{ for all } m, n \in \mathbb{N}_0. \end{aligned}$$

Theorem 4 $\mathbb{Z}$ *is an* **ordered ring** *based on the "set of positives"* $\nu_0(\mathbb{N})$*, and* ν_0 *preserves the ordinal ordering of* $\mathbb{N}_0$ *(by set inclusion):*

$$n < m \text{ in } \mathbb{N}_0 \text{ implies } [(n,0)] < [(m,0)] \text{ in } \mathbb{Z}.$$

As mentioned above, once the construction is satisfactorily executed, the unappealing notation of equivalence classes in $\mathbb{Z}$ is "forgotten" and we write n for $\nu_0(n)$, we write $\mathbb{N}$ for $\nu_0(\mathbb{N})$, we write $\mathbb{N}_0$ for $\nu_0(\mathbb{N}_0)$, and

$$-n \text{ for } [(0,n)].$$

We also adopt the usual ring notation, so $-(-n)$ for $n \in \mathbb{N}$ also makes sense.

Among the most important arithmetic results in $\mathbb{N}_0$ and $\mathbb{Z}$ is the **division algorithm**. I state four versions.

Theorem 5 *(division algorithm in $\mathbb{N}$) If $m, n \in \mathbb{N}$ and $0 < n < m$, then there exist unique natural numbers $q \in \mathbb{N}$ and $r \in \mathbb{N}_0$ such that*

$$0 \leq r < n \qquad \text{and} \qquad m = nq + r.$$

Theorem 6 *(division algorithm in $\mathbb{N}_0$) If $m, n \in \mathbb{N}$, then there exist unique natural numbers $q, r \in \mathbb{N}_0$ such that*

$$0 \leq r < n \qquad \text{and} \qquad m = nq + r.$$

Theorem 7 *(division algorithm in $\mathbb{Z}$) If $m \in \mathbb{Z}\backslash\{0\}$ and $n \in \mathbb{N}$, then there exist unique integers $q \in \mathbb{Z}$ and $r \in \mathbb{N}_0$ such that*

$$0 \leq r < n \qquad \text{and} \qquad m = nq + r.$$

Theorem 8 *(general division algorithm in $\mathbb{Z}$) If $m, n \in \mathbb{Z}\backslash\{0\}$, then there exist unique integers $q \in \mathbb{Z}$ and $r \in \mathbb{N}_0$ such that*

$$0 \leq r < |n| \qquad \text{and} \qquad m = nq + r.$$

As you are no doubt aware (from second or third grade), in $\mathbb{N}$ and $\mathbb{Z}$ it is also useful to have the notion of **divisibility**. If $n, m \in \mathbb{N}$ and there exists some $q \in \mathbb{N}$ such that $nq = m$, (i.e., $r = 0$ in the division algorithm), then we say n divides m and write

$$n \,\big|\, m. \tag{1}$$

If $m, n \in \mathbb{Z}\backslash\{0\}$ and there exists some $q \in \mathbb{Z}$ such that $nq = m$, (i.e., $r = 0$ in the division algorithm), then we say n divides m and again write (1). If

1. $q \in \mathbb{N}$,
2. $q|m$ and $q|n$, and
3. Any integer which divides both m and n also divides q,

then we say q is the **greatest common divisor** of m and n.

Theorem 9 *The greatest common divisor of two integers is always uniquely determined.*

An integer $p \in \mathbb{N}\backslash\{1\}$ is called **prime** if its only divisors (in $\mathbb{N}$) are 1 and p. An integer $p \in \mathbb{Z}\backslash\{0, \pm 1\}$ is called prime if its only divisors are ± 1 and $\pm p$. Using these notions and the division algorithm, one can prove the following results which sometimes go under the name the **fundamental theorem of arithmetic**:

Theorem 10 *(unique prime factorization in $\mathbb{N}$) Given $n \in \mathbb{N}\backslash\{1\}$, there exist unique prime numbers $p_1 < p_2 < \cdots < p_k$ and unique powers $a_1, a_2, \ldots, a_k$ such that*

$$n = \prod_{j=1}^{k} p_j^{a_j}.$$

Theorem 11 *(unique prime factorization in $\mathbb{Z}$) Given $n \in \mathbb{Z}\backslash\{0, \pm 1\}$, there exist unique prime numbers $0 < p_1 < p_2 < \cdots < p_k$ and unique powers $a_1, a_2, \ldots, a_k$ such that one of the following holds:*

$$n = \prod_{j=1}^{k} p_j^{a_j} \qquad \text{or} \qquad n = -\prod_{j=1}^{k} p_j^{a_j}, \tag{2}$$

and exactly one of the conditions in (2) holds.

There is a general abstract algebraic development which extends these notions to certain rings. The appropriate terms for you to look up if you want to learn about this are **ideals**, **prime ideals**, and **unique factorization domains** (UFDs).