Natural Numbers, Integers, and Rational Numbers

In our math classes we often take the subjects in the title for granted. By that I mean we don’t “prove” their existence nor the usual properties (e.g., addition is commutative). The purpose of this note is to describe one way - a typical way - of developing them from axioms.

Axioms in this context doesn’t merely mean “self-evident truth” á la the Greek geometers. Surely there is some of that (after all, everybody “knows” how natural numbers behave on a very intuitive level), but there is also a fair degree of the mathematical way of using axioms simply as a matter of defining objects of study.

At any rate, the Peano Axioms (actually first explicitly listed by Dedekind in the late 1800’s) are typically taken as the properties we need of \( \mathbb{N} \), the natural numbers 0, 1, 2, ... It’s a pretty minimalist set of axioms; they are enough to get the job done, so to speak, without unnecessary bulk. Without further ado, here they are.

\begin{align*}
\text{P1:} & \text{ There is a number 0.} \\
\text{P2:} & \text{ For each number } n, \text{ there is a successor } n' \text{ which is not equal to } n. \\
\text{P3:} & \text{ For no number } n \text{ is } n' = 0. \\
\text{P4:} & \text{ If } m \text{ and } n \text{ are numbers such that } m' = n', \text{ then } m = n. \\
\text{P5:} & \text{ If } S \text{ is a set of numbers such that } 0 \in S \text{ and, for every } n \in S, n' \in S, \text{ then } S = \mathbb{N}. 
\end{align*}

The fifth axiom contains the all-important “principal of mathematical induction” which we all know and love.

You’ll note that there is no mention of addition and multiplication. That’s because these can be developed using the Peano axioms. Of course it’s important that, while perhaps tedious to carry out, this development is possible and yields the usual stuff (addition and multiplication are both commutative and associative binary operations, multiplication distributes through addition, 0 is an additive identity element and 1 is a multiplicative identity element). Once you have addition, the ordering of \( \mathbb{N} \) is simple: \( a \leq b \) if \( a + n = b \) for some \( n \). You then have the familiar ordering properties as well. To wit: i) for all \( a \neq b \), either \( a < b \) or \( b < a \); ii) if \( a < b \) and \( b < c \), then \( a < c \); iii) if \( a < b \), then \( a + n < b + n \) for all \( n \) and \( an < bn \) for all \( n \neq 0 \).

Once we have \( \mathbb{N} \) together with addition and multiplication, getting the integers \( \mathbb{Z} \) and rational
numbers \( \mathbb{Q} \) is relatively easy. In fact, addition in \( \mathbb{N} \) is the whole \textit{raison d'être} for \( \mathbb{Z} \), and similarly multiplication in \( \mathbb{Z} \) points to the need for \( \mathbb{Q} \). Specifically, we want \( \mathbb{Z} \) (i.e., negative numbers) in order to have a group, whence a commutative ring, and once we have \( \mathbb{Z} \), \( \mathbb{Q} \) is the quotient field.

Say two ordered pairs \((x, y)\) and \((n, m)\) of natural numbers are \textit{equivalent} if \( x + m = y + n \). It’s important that we don’t (more simply?) say \( x - y = n - m \). Why? Because \( x - y \) doesn’t make sense all the time. After all, if the only thing we have to work with at present is \( \mathbb{N} \), then there is no “\( 5 - 8 \)”, for example.

It isn’t difficult to verify that this is an equivalence relation. Recall that an equivalence relation on a set \( S \) is a relation (technically a subset of the set of ordered pairs \( S \times S \)) that is reflexive, symmetric and transitive: \( a \sim a \) for all \( a \in S \); if \( a \sim b \), then \( b \sim a \); and if \( a \sim b \) and \( b \sim c \), then \( a \sim c \). Since \( x + y = x + y \), \((x, y)\) is equivalent to \((x, y)\). If \( x + m = y + n \), then by commutativity \( n + y = m + x \). In other words, if \((x, y)\) is equivalent to \((n, m)\), then \((n, m)\) is equivalent to \((x, y)\). Finally, suppose \((x, y)\) is equivalent to \((n, m)\), which is in turn equivalent to \((s, t)\). Then \( x + m = y + n \) and \( n + t = m + s \). Thus \( x + m + t = y + n + t = y + m + s \) and \( x + t = y + s \) (this last bit used several properties of addition if you think it over) and \((x, y)\) is equivalent to \((s, t)\).

The integers \( \mathbb{Z} \) are then defined to be the set of \textit{equivalence classes} of ordered pairs of natural numbers. Think of the equivalence class containing \((a, b)\) as representing \(a - b\). We “define” addition and multiplication as follows:

\[
\left[ (a, b) \right] + \left[ (c, d) \right] = \left[ (a + c, b + d) \right],
\]

\[
\left[ (a, b) \right] \times \left[ (c, d) \right] = \left[ (ac + bd, ad + bc) \right],
\]

where \( \left[ (a, b) \right] \) denotes the equivalence class containing \((a, b)\). I put the quotes on “define” here since, technically speaking, one has to verify that this makes sense. You see, these definitions use particular elements of an equivalence class to represent the entire equivalence class, and that could conceivably lead to difficulty. In other words, one has to check that replacing \((a, b)\) above by \((x, y)\) whenever \((x, y)\) is equivalent to \((a, b)\) doesn’t change the sum or product. Luckily that isn’t difficult, and it turns out that \( \mathbb{Z} \) is a commutative ring.

What happened to \( \mathbb{N} \) in all this? After all, the natural numbers are supposed to be a subset of the integers, right? Actually, it isn’t hard to get around this. Given a natural number \( n \), we can view it as an element of \( \mathbb{Z} \) by equating \( n \) with \( \left[ (n, 0) \right] \). In fact, we can list all of \( \mathbb{Z} \) in a similar
Now that you’ve seen how to get $\mathbb{Z}$ from $\mathbb{N}$, getting the rational numbers $\mathbb{Q}$ from $\mathbb{Z}$ is very similar. We created $\mathbb{Z}$ in order to have additive inverses for all our numbers; we create $\mathbb{Q}$ in order to have multiplicative inverses.

Say two ordered pairs $(a, b), (c, d)$ of integers with $bd \neq 0$ are equivalent if $ad = bc$. As with the equivalence defined on ordered pairs of natural numbers above, this is an equivalence relation. The rational numbers $\mathbb{Q}$ are defined to be the set of equivalence classes. Addition and multiplication are defined in the familiar way (think of $[(a, b)]$ as $\dfrac{a}{b}$):

\[
[(a, b)] + [(c, d)] = [(ad + bc, bd)] \quad [(a, b)] \times [(c, d)] = [(ac, bd)].
\]

Again, one must make sure this definition makes sense, i.e., doesn’t depend on the particular element of the equivalence class used.

For an integer $a \in \mathbb{Z}$, we view it as an element of $\mathbb{Q}$ by equating it with $[(a, 1)]$. This makes $\mathbb{Z}$ a subset of $\mathbb{Q}$ (well, kind of). One can verify that $\mathbb{Q}$ is indeed a field with the familiar order properties.