Integers and real numbers

The treatment of the real numbers in Section 0.5 of our text, E. D. Gaughan’s *Introduction to Analysis*, is incomplete. The difficulty is that, beginning with the paragraph just above Theorem 0.21, the text wants to consider the integers as real numbers, and tacitly assumes from then on that the set \( Z \) of integers is a subset of the set \( \mathbb{R} \) of real numbers. On the other hand, Gaughan wants to use only the properties of the real numbers given as axioms on page 21, and these don’t mention the integers at all. That is, reading only the axioms, how do we know that there is a real number that we should call “2”, or “100”, or “−1766”? This note sketches one way out of the difficulty. At the end we make a remark about another problem in this section of the text.

From now on, \( \mathbb{R} \) will denote the set of real numbers as described by Axioms 1–12 on pages 21 and 22. We will assume here that we already know all about the integers, and will then show how to “find” them within \( \mathbb{R} \). But there is an awkward notational difficulty. To illustrate this, notice that there are integers 0 and 1 that we are assuming we already know about, but there are also two special real numbers, mentioned in the axioms, called 0 and 1. In the end these will turn out to be the same, but until we understand why, we want to keep them separate. So we will use bold face letters to denote the integers that we already understand: \( \mathbb{Z} \) will be the set of integers and \( \ldots, −1, 0, 1, 2, \ldots \) will be elements of \( \mathbb{Z} \). We will write \( \mathbb{J} \) for the natural numbers, that is, the positive elements of \( \mathbb{Z} \).

The key step is to define a certain function \( f: \mathbb{Z} \to \mathbb{R} \). For positive integers \( n \), \( f(n) \) is defined recursively (see Section 0.3 for a review of the ideas of recursion and induction). The first step in the recursion is to define

\[ f(1) = 1; \quad (1) \]

note that in this equations the 1 on the left hand side (in \( f(1) \)) is an integer belonging to \( \mathbb{Z} \) and the 1 on the right hand side is the real number mentioned in Axiom 6. The general step in the recursion is

\[ f(n + 1) = f(n) + 1. \quad (2) \]

The equations (1) and (2) define \( f \) on \( \mathbb{J} \), and we complete the definition by

\[ f(0) = 0, \quad (3) \]

\[ f(n) = -f(-n) \quad \text{for } n \in \mathbb{Z}, n < 0. \quad (4) \]

Note that the second equation in (4) makes sense because if \( n \in \mathbb{Z} \) and \( n < 0 \) then \( -n > 0 \) and so \( f(-n) \) has been defined above, and \( -f(-n) \) makes sense by Axiom 5.

The next theorem gives the most important properties of the function \( f \). We will state it, then use it to discuss how \( f \) solves the problem discussed above. The proof of the theorem will be given later.

**Theorem:** (a) For every \( m, n \in \mathbb{Z} \), (i) \( f(-m) = -f(m) \), (ii) \( f(m + n) = f(m) + f(n) \), and (iii) \( f(mn) = f(m)f(n) \).

(b) If \( m, n \in \mathbb{Z} \) satisfy \( m < n \) then \( f(m) < f(n) \).

(c) \( f \) is a 1-1 function.

(d) \( f(0) = 0 \) and \( f(1) = 1 \).
Now let $\mathbb{Z}$ (not boldface!) denote the image of $f$. $\mathbb{Z}$ is a subset of $\mathbb{R}$ and $f$ is a 1-1 function from $\mathbb{Z}$ onto $\mathbb{Z}$, that is, an equivalence (in the sense of Section 0.4) between the set $\mathbb{Z}$ of integers and the subset $\mathbb{Z}$ of $\mathbb{R}$. We will think of $\mathbb{Z}$ as a copy of the integers sitting inside $\mathbb{R}$, and once we have finished our discussion here we will forget about $\mathbb{Z}$ and consider $\mathbb{Z}$ to be the integers.

Because $\mathbb{Z}$ is a subset of $\mathbb{R}$ the arithmetic operations of negation, addition, and multiplication are already defined for elements of $\mathbb{Z}$ by the corresponding rules in $\mathbb{R}$, and part (a) of the theorem assures us that these operations in $\mathbb{Z}$ correspond precisely to the same operations in $\mathbb{Z}$. Similarly, the order relation in $\mathbb{Z}$, that is, whether given integers $m$ and $n$ in $\mathbb{Z}$ satisfy $m = n$, $m < n$, or $m > n$, is already defined by the order relation in $\mathbb{R}$, and part (b) assures us that this order corresponds to the original order in $\mathbb{Z}$. Thus $\mathbb{Z}$ and $\mathbb{Z}$ are completely equivalent, and we lose nothing by forgetting about $\mathbb{Z}$ and regarding the integers as the subset $\mathbb{Z}$ of $\mathbb{R}$. For every integer $n$ in $\mathbb{Z}$, such as 2, or 100, or $-1766$, we denote the corresponding "new" integer in $\mathbb{Z}$ without boldface, as $n$, or, for the specific examples, 2, 100, or $-1766$. Notice, however, that 1 and 0 already exist in $\mathbb{R}$, so that we need part (d) to be sure that this naming convention is consistent.

**Proof of the theorem:** (a.i) We take $m \in \mathbb{Z}$ and show that $f(-m) = -f(m)$. If $m < 0$ then $f(m) = -f(-m)$ by (4); if $m = 0$ then $-m = 0$ and so $f(-m) = 0 = -0 = -f(m)$ by (3); if $m > 0$ then $-m < 0$ and so, again by (4), $f(-m) = -f(-(-m)) = -f(m)$. Note that we have used $-0 = 0$. We may derive this property of $\mathbb{R}$ by noting that from Axiom 4, $0 + 0 = 0$, and from Axiom 5, this means that $0 = -0$.

(a.ii) We suppose that $m, n \in \mathbb{Z}$ and show that $f(m + n) = f(m) + f(n)$. Note that this is trivially true if $m = 0$ or $n = 0$. We next suppose that $m > 0$ and prove the result for $n \geq 1$ by induction on $n$. The case $n = 1$ is immediate from (2), and for the induction step we have, using (2), then the induction assumption, and then (2) again,

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

This completes the proof for $m, n \geq 0$.

Suppose now that $m \geq 0$, $n < 0$, and $m + n \geq 0$; then from the cases proved in the previous paragraph, and (a.i), we have

$$f(m) = f(m + n + (-n)) = f(m + n) + f(-n) = f(m + n) - f(n),$$

and rearranging this gives $f(m + n) = f(m) + f(n)$, as desired. Of course, the same argument applies if $m < 0$ and $m + n \geq 0$, and this completes the proof for all cases with $m + n \geq 0$. Finally, if $m + n < 0$ so that $(-m) + (-n) > 0$, we have

$$f(m + n) = -f((-m) + (-n)) = -(f(-m) + f(-n)) = -(-f(m) - f(n)) = f(m) + f(n),$$

where we have used (a.i) repeatedly. This completes the proof.

(a.iii) Now we want to show that $f(mn) = f(m)f(n)$ if $m, n \in \mathbb{Z}$. This is almost the same as (a.ii): one observes that it is trivially true if $m = 0$ or $n = 0$, checks the case $m, n > 0$.
by induction on \( n \) for fixed \( m \) (here (a.ii) is needed), and then completes all other cases by using (a.i) to reduce to \( m, n \geq 0 \). We leave the details as an exercise.

(b) We first suppose that \( n > 0 \) and show that \( f(n) > 0 \) (this is a special case of the result we want). The proof is inductive; for \( n = 1 \) we have \( f(1) = 1 > 0 \), by (1) and Theorem 0.19 (ii), and then if we assume inductively that \( f(n) > 0 \), \( f(n + 1) = f(n) + 1 > f(n) > 0 \) (we have used Axiom 8). We now prove the general case: if \( m < n, n - m > 0 \), and using (a.ii),

\[ f(n) = f(m + (n - m)) = f(m) + f(n - m) > f(m), \]

as desired, since \( f(n - m) > 0 \) by the special case considered first.

(c) To show that \( f \) is 1-1 we must consider \( m, n \in \mathbb{Z} \) with \( m \neq n \) and show that \( f(m) \neq f(n) \). But if \( m \neq n \) then either \( m < n \) or \( n < m \). Without loss of generality we may suppose that \( m < n \); then \( f(m) < f(n) \) by (b) and so \( f(m) \neq f(n) \), by Axiom 10.

(d) This is just a restatement of (3) and (1).

\[ \blacksquare \]

Remark: There is a further difficulty with our text’s treatment of the integers: the proof of Theorem 0.21 is not correct. In this proof, \( x \) is a given real number; the text defines the set \( A = \{ n \in \mathbb{Z} : n \leq x \} \) and then considers separately two cases, according to whether \( A \) is empty or not. The problem is in the discussion of the case in which \( A \) is empty, the second paragraph of the proof. In fact, this case cannot happen; to show this, the text assumes that \( A = \emptyset \) and tries to derive a contradiction. For this purpose the author introduces the set \( B = \{ n \in \mathbb{Z} : n > x \} \); \( B \) is the complement of \( A \) relative to \( \mathbb{Z} \) (i.e., \( B = \mathbb{Z} \setminus A \)) and since \( A \) is empty by assumption, \( B = \mathbb{Z} \). Thus \( B \) is nonempty, since \( \mathbb{Z} \) is, and from its definition, \( B \) is bounded below (\( x \) is a lower bound for \( B \)); thus \( B \) has a greatest lower bound, called \( z_0 \).

Now comes the key, final sentence: “Then \( z_0 - 1 \) is not in \( B \), contrary to \( B = \mathbb{Z} \).” The first statement is true, but based on what has been said so far there is no contradiction, because it has not been established that \( z_0 - 1 \) belongs to \( \mathbb{Z} \). The text tacitly assumes that \( z_0 \), and hence \( z_0 - 1 \), belongs to \( \mathbb{Z} \), but this has to be shown.

In class we avoided this difficulty by proving the lemma given immediately below. An alternative approach would be to model the proof on the argument in the first paragraph of Gaughan’s proof, starting with the fact that \( z_0 + 1 \) is not a lower bound for \( B \). Details are left to the reader. It is amusing that the author does not assume in the first paragraph that \( n_0 \in \mathbb{Z} \) but does make the corresponding assumption, \( z_0 \in \mathbb{Z} \), in the second paragraph.

Lemma: (a) If \( S \subset \mathbb{Z} \) is nonempty and bounded above then the least upper bound of \( S \) belongs to \( S \) (and hence is an integer).

(b) If \( S \subset \mathbb{Z} \) is nonempty and bounded below then the greatest lower bound of \( S \) belongs to \( S \) (and hence is an integer).

Proof: We leave the proof a an exercise. \[ \blacksquare \]