DEPARTMENT OF MATHEMATICS

TECHNICAL REPORT

A PRESENTATION ON A CONSTRUCTION OF REAL NUMBERS

Courtney Riggs

December 2018

No. 2018-3

TENNESSEE TECHNOLOGICAL UNIVERSITY
Cookeville, TN 38505

A PRESENTATION ON A CONSTRUCTION OF REAL NUMBERS

COURTNEY RIGGS

Abstract. The goal of this paper is to present a construction of the set of real numbers based on set theory. We will do this by starting with the Peano Postulates to construct the set of natural numbers. Then, we will use an equivalence relation on the set of natural numbers to construct the set of integers. In a similar method, we will construct the set of rational numbers with an equivalence relation on the set of integers. Then, we will define Dedekind cuts, which will allow us to define the set of real numbers. We will also define arithmetic operations (addition and multiplication) as well as the order relations on each of these sets, which will yield properties we expect to see.

1. Introduction

Numbers have been used at least since the ancient world. The need to count objects prompted many ancient cultures to use the set of natural numbers along with addition and multiplication. Some cultures, including ancient China and India, also made use of the negative integers and zero, as well, with the negative numbers appearing before zero. In China, Mesopotamia, Egypt, and India, there were rational approximations for certain irrational numbers, though they did not realize that irrational numbers exist. In ancient Greece, it was discovered that pairs of certain line segment lengths could not be represented as rational numbers, but they did not recognize irrational numbers as "numbers" because of the separation between geometry and arithmetic. Through time and the sharing of information among cultures, the sets of numbers we use today were constructed. Although numbers might be represented by different symbols in varying cultures, we are all using the same sets of numbers and mathematical operations. When studying mathematics, it is essential to understand what the concept of a "number" means. In this paper, we will detail the construction of the real numbers by building up from the set of natural numbers, using [1] as a source for definitions, theorems, etc. and resource for proofs not given here. For more details on the history of mathematics, see [2].

2. The construction of the Natural Numbers

A natural place to start when constructing sets of numbers is with those numbers which are used for counting. If there are no objects, there is nothing to count and no collection; but if there is at least one object, the quantity of objects in a collection can be described in some way. Of course, with any collection of objects, we can always add another object to the collection, which means it is then represented by a new quantity. This action of

adding an object to a collection of objects is what we will define the function $s : A \to A$ to mean, where A is the set to which we are referring in this example.

Although thinking about collections of objects is useful for understanding the concept of numbers, we want to formally define them so that we can use them in other ways than just counting objects.

The following axiom provides us with a foundation for constructing a unique set which is more general than, but equivalent to, the set A referred to above.

Axiom 2.1 (Peano Postulates)**.** *There exists a set N with an element $a \in N$ and a function $s : N \to N$ that satisfy the following three properties.*

a) There is no $n \in N$ such that $s(n) = a$.
b) The function s is injective.
c) For an arbitrary subset $G \subseteq N$ with $a \in G$ the following implication holds true. If $s(g) \in G$ for all $g \in G$ then $G = N$.

A proof of the following theorem can be found on page 87 of [1]. Parts (a) and (b) of Axiom 2.1 are used to prove the existence of f and part (c) is used to prove uniqueness.

Theorem 2.2 (Definition by Recursion)**.** *Let N, a and s be as in Axiom 2.1. Let H be a set, let $e \in H$ and let $k : H \to H$ be a function. Then there is a unique function $f : N \to H$ such that $f(a) = e$, and that $f \circ s = k \circ f$.*

This theorem states that the below diagram is commutative, and $f(a) = e$.

$$\begin{array}{ccc} N & \xrightarrow{s} & N \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ H & \xrightarrow[k]{} & H \end{array}$$

In other words, it guarantees that given a set with a distinguished element, e, and a function k as defined above, there is a unique mapping from N to H such that a maps to e and the function s is preserved by this mapping. We will use Theorem 2.2 to prove the following lemma.

Lemma 2.3. *The set given by the Peano Postulates is (essentially) unique.*

Proof. Let N, a and s be as in Axiom 2.1. Also, suppose N', a' and s' satisfy Axiom 2.1. By Theorem 2.2 there exists a unique function $f : N \to N'$ such that $f(a) = a'$ and

$$f \circ s = s' \circ f. \tag{1}$$

$$\begin{array}{ccc} N & \xrightarrow{s} & N \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ N' & \xrightarrow[s']{} & N' \end{array}$$

Also, there exists a unique function $g : N' \to N$ such that $g(a') = a$ and

$$g \circ s' = s \circ g. \tag{2}$$

$$\begin{array}{ccc} N' & \xrightarrow{s'} & N' \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g} \\ N & \xrightarrow[s]{} & N \end{array}$$

Let $G = \{m \in N : g(f(m)) = m\}$ and let $G' = \{m' \in N' : f(g(m')) = m'\}$. Notice that

$$f(g(a')) = f(a) = a'$$

and

$$g(f(a)) = g(a') = a,$$

so $a \in G$ and $a' \in G'$.

Moreover by (1) and (2), for all $n \in N$, if $n \in G$, then

$$g(f(s(n))) = g(s'(f(n))) = s(g(f(n))) = s(n).$$

So $s(n) \in G$ for all $n \in N$. By Axiom 2.1(c), $G = N$.

Similarly, for all $n' \in N'$, the condition $n' \in G'$ implies

$$f(g(s'(n'))) = f(s(g(n'))) = s'(f(g(n'))) = s'(n').$$

Thus, $s'(n') \in G'$ for all $n' \in N'$. By Axiom 2.1(c), $G' = N'$. Therefore, f and g are inverses of each other, in particular f is bijective.

$$\begin{array}{ccc} N & \xrightarrow{s} & N \\ {\scriptstyle f}\downarrow & & \uparrow{\scriptstyle g=f^{-1}} \\ N' & \xrightarrow[s']{} & N' \end{array}$$

In fact, f preserves the function s, that is $s = f^{-1} \circ s' \circ f$. This proves N is essentially unique. □

Now that we've shown that the set N given in Axiom 2.1 is essentially unique, we will define all sets satisfying Axiom 2.1 as follows.

Definition 2.4 (Natural Numbers)**.** *The set of natural numbers, denoted* $\mathbb{N}$*, is a set of existence which is given in the Peano Postulates. That is, for* (N, a, s) *satisfying Axiom 2.1, we define*

$$\begin{aligned} \mathbb{N} &= N \\ 1 &= a \\ 2 &= s(a) \\ 3 &= s(s(a)) \\ &\vdots \end{aligned}$$

Therefore, $\mathbb{N} = \{1, 2, 3, ...\}$.

Observe that the set $\mathbb{N}$ together with the distinguished element 1 and the injective function s is well defined up to bijective mapping f obtained in Theorem 2.1.

We will write $n+1$ in place of $s(n)$ for $n \in \mathbb{N}$. Then given another set N', along with an element $a' \in N'$ and a function $s' : N' \to N'$, which satisfies Axiom 2.1 we have a unique bijective function $f : \mathbb{N} \to N'$ that maps every element of $\mathbb{N}$ to an element of N' and preserves 1 and the function s in the sense that $f(1) = a$ and $s(n) = f^{-1}(f(n+1))$ for all $n \in \mathbb{N}$.

A proof for the following lemma can be found on page 4 of [1]. For reader's convenience, we will also prove it here.

Lemma 2.5. *Let $a \in \mathbb{N}$. Suppose that $a \neq 1$. Then there is a unique $b \in \mathbb{N}$ such that $a = b + 1$.*

Proof. To prove uniqueness, suppose that both $a = b + 1$ and $a = c + 1$ for some $b, c \in \mathbb{N}$. By Axiom 2.1(b), $b = c$.

Now we will prove existence. Let

$$G = \{1\} \cup \{c \in \mathbb{N} : \text{ there is some } b \in \mathbb{N} \text{ such that } b + 1 = c\}.$$

Clearly, $G \subseteq \mathbb{N}$ and $1 \in G$. Suppose that $n \in G$. Let $m = n + 1$. Clearly, $m \in G$. By Axiom 2.1(c), $G = \mathbb{N}$. This implies the existence of b. □

The notation $n + 1$ might remind some readers of the Principle of Weak Mathematical Induction. In fact, we can prove that it is equivalent to the Peano Postulates. We will state the Principle of Weak Mathematical Induction here for completeness.

Definition 2.6 (The Principle of Weak Mathematical Induction)**.** *Let $P(n)$ be a proposition defined for each $n \in \mathbb{N}$. If*

(1) $P(1)$ holds true

(2) for every $n \in \mathbb{N}$, $P(n)$ holds true implies $P(n+1)$ holds true,

then $P(n)$ holds true for every $n \in \mathbb{N}$

Theorem 2.7. *The Principle of Weak Mathematical Induction is equivalent to The Peano Postulates.*

Proof. (Forward direction) Let $P(n)$ be a proposition and let $G \subset \mathbb{N}$ be defined by

$$G = \{n \in \mathbb{N} \mid P(n) \text{ holds true}\}.$$

If $P(1)$ holds true, then $1 \in G$. Assume $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$. Then, $n \in G$ implies $n + 1 \in G$, whence $G = \mathbb{N}$.

(Reverse direction) Assume that the Peano Postulates hold true. Let, for $n \in \mathbb{N}$, $P(n)$ be a proposition such that $P(1)$ holds true and $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$. Let

$$G = \{n \in \mathbb{N} : P(n) \text{ holds true}\}.$$

Clearly, $1 \in G$ and $n \in G$ implies $n + 1 \in G$, for all $n \in \mathbb{N}$. By Axiom 2.1(c), $G = \mathbb{N}$, that is $P(n)$ holds true for all $n \in \mathbb{N}$. □

Proceeding, we will use the more familiar Weak Induction rather than The Peano Postulates in proofs.

Definition 2.8. *Let A be a set. A subset $R \subset A \times A$ is said to be a binary relation on A.*

Now, we are ready to define the binary relation of addition on the natural numbers. A proof of the following theorem can be found on page 5 of [1].

Theorem 2.9. *There is a unique binary relation $+ : \mathbb{N} \times \mathbb{N}$, for which $+(n, m)$ is denoted $n + m$, that satisfies the following two properties for all $n, m \in \mathbb{N}$.*

(a) $n + 1 = s(n)$
(b) $n + s(m) = s(n + m)$

The theorem below shows that the binary relation $+$ on the set of natural numbers has the properties we expect, such as associativity, commutativity, and a cancellation law.

Theorem 2.10. *For all $a, b, c \in \mathbb{N}$ the following conditions hold true.*

(1) $(a + b) + c = a + (b + c)$ *(Associative Law for Addition).*
(2) $1 + a = s(a) = a + 1$.
(3) $a + b = b + a$ *(Commutative Law for Addition).*
(4) If $a + c = b + c$, *then* $a = b$ *(Cancellation Law for Addition).*
(5) $a + b \neq 1$.
(6) $a + b \neq a$.

Proof. (1) Fix $a, b \in \mathbb{N}$. Let $G = \{c \in \mathbb{N} : (a + b) + c = a + (b + c)\}$. Consider $c = 1$. Then,

$$(a + b) + 1 \overset{2.9(a)}{=} s(a + b) \overset{2.9(b)}{=} a + s(b) \overset{2.9(a)}{=} a + (b + 1)).$$

So, $1 \in G$. Suppose that $c \in G$. We will show that $s(c) \in G$

$$\begin{aligned}(a + b) + s(c) &\overset{2.9(b)}{=} s((a + b) + c) \overset{c \in G}{=} s(a + (b + c)) \\ &\overset{2.9(b)}{=} a + s(b + c) \overset{2.9(b)}{=} a + (b + s(c))\end{aligned}$$

Therefore $s(c) \in G$,whence $G = \mathbb{N}$.

(2) Let $G = \{a \in \mathbb{N} : 1 + a = a + 1\}$. Clearly, $G \subset \mathbb{N}$. Since $1 + 1 = 1 + 1$, $1 \in G$. Assume $n \in G$. We will show that $s(n) \in G$.

$$\begin{aligned}1 + s(n) &\overset{2.9(b)}{=} s(1 + n) \overset{n \in G}{=} s(n + 1) \\ &\overset{2.9(b)}{=} n + s(1) \overset{2.9(a)}{=} n + (1 + 1) \\ &\overset{(1)}{=} (n + 1) + 1 \overset{2.9(a)}{=} s(n) + 1\end{aligned}$$

Since $s(n) \in G$, then $G = \mathbb{N}$.

(3) Let $G = \{a \in \mathbb{N} : a + b = b + a\}$. Clearly, $G \subset \mathbb{N}$. From $1 \in G$. Assume $n \in G$. We will prove that $s(n) \in G$.

$$s(n) + b \overset{2.9(a)}{=} (n+1) + b \overset{(1)}{=} n + (1+b)$$
$$\overset{(2)}{=} n + s(b) \overset{2.9(b)}{=} s(n+b)$$
$$\overset{n \in G}{=} s(b+n) \overset{2.9(b)}{=} b + s(n)$$

Thus, $s(n) \in G$, so $G = \mathbb{N}$.

For proofs of (4), (5), and (6) refer to page 7 of [1]. □

Intuitively, we know that we can multiply natural numbers as well. The proof of the following theorem shows that multiplication on the natural numbers exists and is unique.

Theorem 2.11. *There is a unique binary relation $\cdot : \mathbb{N} \times \mathbb{N}$ that satisfies the following two properties for all $n, m \in \mathbb{N}$*

(a) $n \cdot 1 = n$.
(b) $n \cdot (m+1) = (n \cdot m) + n$

Proof. A proof that $\cdot$ exists is given on page 6 of [1]. To prove uniqueness:

Suppose there is another binary operation $\odot : \mathbb{N} \times \mathbb{N}$ such that

(1) $n \odot 1 = n$.
(2) $n \odot (m+1) = (n \odot m) + n$.

Let $n \in \mathbb{N}$ and let $P(m)$ be the proposition that $n \cdot m = n \odot m$. Since $n \cdot 1 = n = n \odot 1$, $P(1)$ is true. Suppose $P(m)$ is true. Then $n \cdot m = n \odot m$. From (b) and (1),

$$n \cdot (m+1) = (n \cdot m) + n = (n \odot m) + n = n \odot (m+1).$$

Hence $P(m+1)$ holds true. Therefore by weak induction, $P(m)$ is true for all $m \in \mathbb{N}$ and $\cdot$ is unique. □

We will now show that multiplication on the natural numbers behaves as we expect it to.

Theorem 2.12. *Let $a, b, c \in \mathbb{N}$.*

(1) $a \cdot 1 = a = 1 \cdot a$ *(Identity Law for Multiplication).*
(2) $(a+b)c = ac + bc$ *(Distributive Law).*
(3) $ab = ba$ *(Commutative Law for Multiplication).*
(4) $c(a+b) = ca + cb$ *(Distributive Law).*
(5) $(ab)c = a(bc)$ *(Associative Law for Multiplication).*
(6) If $ac = bc$ *then* $a = b$ *(Cancellation Law for Multiplication).*
(7) $ab = 1$ *if and only if* $a = 1 = b$.

Proof. (1) By definition, $a \cdot 1 = a$. We will show that the proposition $P(a) : 1 \cdot a = a$ holds true for all $a \in \mathbb{N}$.

Let $a = 1$. By Theorem 2.11(a), $1 \cdot 1 = 1$, hence $P(1)$ holds true.

Assume $P(n)$ holds true, that is $1 \cdot n = n$, for some $n \in \mathbb{N}$. Consider $P(n+1)$.

$$1 \cdot (n+1) \overset{2.11(b)}{=} (1 \cdot n) + 1 = n + 1$$

Therefore $P(a)$ holds true for all $a \in \mathbb{N}$.

(2) Fix $a, b \in \mathbb{N}$. Let $P(c)$ be the proposition that $(a+b)c = ac + bc$. We will show that $P(c)$ holds true for all $c \in \mathbb{N}$.

Let $c = 1$. Then, $(a+b) \cdot 1 \overset{2.12(1)}{=} a + b \overset{2.12(1)}{=} a \cdot 1 + b \cdot 1$, so $P(1)$ holds true.

Assume $P(n)$ holds true for some $n \in \mathbb{N}$. Consider $P(n+1)$.

$$\begin{aligned}(a+b)(n+1) &\overset{2.11(b)}{=} ((a+b)n) + (a+b) \overset{P(n)}{=} an + bn + a + b \\ &\overset{2.10(3)}{=} (an + a) + (bn + b) \overset{2.11(b)}{=} a(n+1) + b(n+1)\end{aligned}$$

Thus $P(c)$ holds true for all $c \in \mathbb{N}$.

(3) Fix $a \in \mathbb{N}$. Let $P(b)$ be the proposition that $ab = ba$. We will show that $P(b)$ holds true for all $b \in \mathbb{N}$.

Let $b = 1$. By (1), $P(1)$ holds true.

Assume $P(n)$ holds true for some $n \in \mathbb{N}$. Consider $P(n+1)$.

$$a(n+1) \overset{2.11(b)}{=} an + a \overset{2.11(a)}{=} an + a \cdot 1 \overset{P(1),P(n)}{=} na + 1 \cdot a \overset{2.12(2)}{=} (n+1)a$$

Thus, $P(b)$ holds true for all $b \in \mathbb{N}$.

(4)

$$c(a+b) \overset{2.12(3)}{=} (a+b)c \overset{2.12(2)}{=} ac + bc \overset{2.12(3)}{=} ca + cb$$

(5) Fix $a, b \in \mathbb{N}$. Let $P(c)$ be the proposition that $(ab)c = a(bc)$. We will show $P(c)$ holds true for all $c \in \mathbb{N}$.

Let $c = 1$. Since $(ab) \cdot 1 \overset{2.11(a)}{=} ab \overset{2.11(a)}{=} a(b \cdot 1)$, $P(1)$ holds true.

Assume $P(n)$ holds true for some $n \in \mathbb{N}$, that is $(ab)n = a(bn)$. Consider $P(n+1)$.

$$(ab)(n+1) \overset{2.11(b)}{=} (ab)n + ab \overset{P(n)}{=} a(bn) + ab \overset{2.12(4)}{=} a(bn + b) \overset{2.11(b)}{=} a(b(n+1))$$

Thus, $P(c)$ holds true for all $c \in \mathbb{N}$.

(6) This proof can be found on page 7 of [1].

(7) (Forward direction) Proceed by contradiction. Assume $ab = 1$. First suppose at least one of a or b does not equal 1. Without loss of generality, let $a = 1$ and $b \neq 1$. Then,

$$ab = 1 \cdot b = b \neq 1$$

Now let $a \neq 1$ and $b \neq 1$. Then by Lemma 2.5 there is some unique $c \in \mathbb{N}$ such that $c + 1 = b$. So,

$$ab = a(c+1) \overset{2.12(4)}{=} ac + a \overset{2.10(5)}{\neq} 1$$

(Reverse direction) Assume $a = 1 = b$. Then $ab = 1 \cdot 1 = 1$.

□

At this point, we can add or multiply two natural numbers, but we cannot compare them to one another. Since we know intuitively that there is an order to the set of natural numbers, we would like to have a way to define that order.

The following definitions characterize types of binary relations on a set. We are particularly interested in the definition of a partial order.

Definition 2.13. *A binary relation, R, on a set A is said to be an equivalence relation on A if the following conditions hold*

(1) $(a, a) \in R$ *for all* $a \in A$ *(R is reflexive)*
(2) $(a, b) \in R$ *and* $(b, c) \in R$ *implies* $(a, c) \in R$ *for all* $a, b, c \in A$ *(R is transitive)*
(3) $(a, b) \in R$ *if and only if* $(b, a) \in R$ *for all* $a, b \in A$ *(R is symmetric)*

Definition 2.14. *A binary relation, R, on a set A is said to be a partial order if*

(1) $(a, a) \in R$ *for all* $a \in A$ *(R is reflexive)*
(2) $(a, b) \in R$ *and* $(b, c) \in R$ *implies* $(a, c) \in R$ *for all* $a, b, c \in A$ *(R is transitive)*
(3) $(a, b) \in R$ *and* $(b, a) \in R$ *implies* $a = b$ *for all* $a, b \in A$ *(R is antisymmetric)*

We will now define a method for comparison of two natural numbers.

Definition 2.15. *The relation $<$ on $\mathbb{N}$ is defined by $a < b$ $(a, b \in \mathbb{N})$ if and only if there is some $p \in \mathbb{N}$ such that $a + p = b$. The relation $\leq$ on $\mathbb{N}$ is defined by $a \leq b$ $(a, b \in \mathbb{N})$ if and only if $a < b$ or $a = b$.*

We can write $b < a$ as $a > b$ and $b \leq a$ as $a \geq b$.

The following theorem gives useful properties for the relations $<$ and $\leq$. Proofs for (2), (4), (5), (7), (11), and (13) can be found on page 8 of [1].

Theorem 2.16. *For all $a, b, c, d \in \mathbb{N}$ the following statements hold true.*

(1) $a \leq a$.
(2) If $a \leq b$ *and* $b \leq a$, *then* $a = b$.
(3) If $a \leq b$ *and* $b \leq c$, *then* $a \leq c$.
(4) $a \leq b$ *or* $b \leq a$.
(5) $1 \leq a$.
(6) If $a < b$ *and* $b < c$, *then* $a < c$.
(7) Precisely one of $a < b$ *or* $a = b$ *or* $a > b$ *holds (Trichotomy Law).*
(8) $a \not< a$ *and* $a < a + 1$.
(9) $a < b$ *if and only if* $a + c < b + c$.
(10) $a < b$ *if and only if* $ac < bc$.
(11) It cannot be that $b < a < b + 1$.
(12) If $a \leq b$ *and* $b < c$, *then* $a < c$; *if* $a < b$ *and* $b \leq c$, *then* $a < c$.
(13) $a \leq b$ *if and only if* $a < b + 1$.
(14) $a < b$ *if and only if* $a + 1 \leq b$.

By Theorem 2.16 (1), (2), and (3), the relation $\leq$ is a partial order on $\mathbb{N}$. In addition, a partially ordered set along with Theorem 2.16 (4) (a comparability condition) is a total order.

Now that we have the relation $\leq$, we can define two more important principles that can be used to prove that a set is equivalent to the set of natural numbers.

Definition 2.17 (Principle of Strong Mathematical Induction)**.** *Let $P(n)$ be a proposition defined for each $n \in \mathbb{N}$. If*

(1) $P(1)$ holds true

(2) For all $k \in \mathbb{N}$, $P(n)$ holds true for all $n \leq k$ implies $P(k+1)$ holds true,

then $P(n)$ holds true for all $n \in \mathbb{N}$.

A proof for the following theorem can be found on page 9 of [1]. It uses Axiom 2.1 rather than weak induction, but since we know that they are equivalent, either can be used.

Theorem 2.18 (Well-Ordering Principle)**.** *Let $G \subseteq \mathbb{N}$ be a non-empty set. Then there is some $m \in G$ such that $m \leq g$ for all $g \in G$.*

This theorem states that every non-empty subset of $\mathbb{N}$ has a smallest element. In fact, Theorem 2.16 implies that a smallest element is unique. The smallest element in the set of natural numbers is 1, which is essentially stated in Axiom 2.1(a). Since both the Well-Ordering Principle and the Peano Postulates ensure that the smallest element of the set of natural numbers is 1, we suspect that those statements might be equivalent. In fact, the following theorem holds true.

Theorem 2.19. *The following are equivalent*

(1) The Well-Ordering Principle

(2) The Principle of Strong Mathematical Induction

(3) The Principle of Weak Mathematical Induction

Proof. $((WO) \Rightarrow (SI))$ Let $P(n)$ be a proposition defined for each $n \in \mathbb{N}$. Assume conditions (1) and (2) of Definition 2.17 hold true. Let

$$S = \{n \in \mathbb{N} : P(n) \text{ does not hold true}\}.$$

Suppose that $S \neq \emptyset$. By (WO), S has a smallest element, say n_0. By (1) of Definition 2.17, $1 \notin S$. Therefore, $n_0 \neq 1$. By Theorem 2.5, there is a $k \in \mathbb{N}$ such that $n_0 = k + 1$. We have $1, 2, 3, ..., k \notin S$. By definition of S, $P(1), P(2), \ldots, P(k)$ holds true. By (2) of Definition 2.17 we get $P(n_0)$ holds true. That is $n_0 \notin S$. This is a contradiction with the statement that n_0 is the smallest element in S. Whence $S \neq \emptyset$ is impossible. Therefore $S = \emptyset$, which is equivalent to $P(n)$ holds true for all $n \in \mathbb{N}$.

$((SI) \Rightarrow (WI))$ Suppose that $P(1)$ holds true and that $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$. For $k \in \mathbb{N}$, we get

$$P(1) \Rightarrow P(2) \Rightarrow \cdots \Rightarrow P(k).$$

Therefore the assumptions for (SI) are satisfied, which implies $P(n)$ holds true for all $n \in \mathbb{N}$.

$((WI) \Rightarrow (WO))$ Let $S \neq \emptyset$, $S \subset \mathbb{N}$. Let $B \subset \mathbb{N}$ be defined by

$$n \in B \text{ if and only if for all } m \in \mathbb{N}, m \leq n \Rightarrow m \notin S.$$

Define $P(n) =$ "$n \in B$".

We have that $P(1) =$ "$1 \in B$", which is equivalent to for all $m \in \mathbb{N}$, $m \leq 1 \Rightarrow m \notin S$.

If $1 \in S$, then 1 is the smallest element of S. Suppose that $1 \notin S$, then $1 \in B$, that is $P(1)$ holds true.

Let $n \in \mathbb{N}$. Suppose that $P(n)$ holds true. We want to show that $P(n+1)$ holds true.

Since $P(n)$ holds true, $n \in B$, which is equivalent to $1, 2, 3, \ldots, n \notin S$. If $n+1 \in S$, then $n+1$ is the smallest element of S. Suppose that $n+1 \notin S$. Then $P(n+1)$ holds true. By (WI), $P(n)$ holds true for all $n \in \mathbb{N}$, that is $B = \mathbb{N}$. Therefore $S = \emptyset$, a contradiction. Therefore, it must be the case that either $1 \in S$ or for some $n \in \mathbb{N}$, $n+1 \in S$ while $1, 2, 3, \ldots, n \notin S$. In any case, it must be that (WO) holds true.

□

3. The construction of the Integers

In the previous section, we constructed a set of numbers on which addition, multiplication, and order were defined. However, we want to do more than just add, multiply, and compare numbers. In particular, we would like to be able to solve all equations of the type

$$x + n = m \tag{3}$$

where $n, m \in \mathbb{N}$ are given and x is unknown. It is easy to see that (3) has a solution $x \in \mathbb{N}$ if and only if $m > n$. In order to have (3) solvable, for all $n, m \in \mathbb{N}$, we need a "larger" set of numbers which "contains" $\mathbb{N}$ as a subset and on which operations of addition, multiplication, and order are defined extending the corresponding operations on $\mathbb{N}$. Intuitively, we know that if $m < n$, then x will be a "negative number", and if $m = n$, then x will be "zero". In this section, we will construct a "larger" set of numbers from the set of natural numbers on which "negative numbers" and "zero" are defined.

First, we will introduce a new relation on $\mathbb{N} \times \mathbb{N}$ that will help in constructing the set we are interested in. By constructing this set from the natural numbers, we will be able to use the properties of the natural numbers from the previous section for the proofs in this section.

Definition 3.1. *The relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ is defined by $(a, b) \sim (c, d)$ if and only if $a + d = b + c$, for all $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$.*

A proof of the following lemma can be found on page 12 of [1].

Lemma 3.2. *The relation $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

Definition 3.3 (Integers)**.** *The set of integers, denoted $\mathbb{Z}$, is the set of equivalence classes of $\mathbb{N} \times \mathbb{N}$ with respect to the equivalence relation $\sim$. That is,*

$$\mathbb{Z} = \{[(a, b)] : a, b \in \mathbb{N}\}.$$

The elements $\hat{0}, \hat{1} \in \mathbb{Z}$ are defined by

$$\hat{0} := [(1, 1)] = \{(a, b) \in \mathbb{N} \times \mathbb{N} : 1 + b = 1 + a\} \overset{2.10(4)}{=} \{(a, b) \in \mathbb{N} \times \mathbb{N} : a = b\}$$

and

$$\hat{1} := [(1+1, 1)] = \{(a, b) \in \mathbb{N} \times \mathbb{N} : (1+1) + b = 1 + a\} \overset{2.10(1),(4)}{=} \{(a, b) \in \mathbb{N} \times \mathbb{N} : 1 + b = a\}.$$

This set differs from the natural numbers in that the elements of the integers are equivalence classes rather than single elements. In other words, in the set of natural numbers, 1 can only be expressed by the element 1, but in the integers, the element $\hat{1}$ can be expressed as $[(2,1)]$, $[(3,2)]$, or any $[(a,b)]$ such that $1+b=a$ where $a,b \in \mathbb{N}$.

We define addition on the set of integers component-wise.

Definition 3.4. *The binary operation $+$ on $\mathbb{Z}$ is defined by $(a,b,c,d \in \mathbb{N})$,*

$$[(a,b)] + [(c,d)] = [(a+c, b+d)].$$

A proof that $+$ is well defined on $\mathbb{Z}$ is on page 13 of [1].

Now, we define "negative integers" in the following way.

Definition 3.5. *The unary operation $-$ on $\mathbb{Z}$ is defined by*

$$-[(a,b)] = [(b,a)], \quad [(a,b)] \in \mathbb{Z}.$$

It can be shown that $-$ is well defined.

As an example, the negative of $\hat{1}$ is given by

$$-\hat{1} = -[(2,1)] = [(1,2)] = \{(a,b) \in \mathbb{N}\times\mathbb{N} : 1+b = 2+a\} \overset{2.10(4)}{=} \{(a,b) \in \mathbb{N}\times\mathbb{N} : b = 1+a\}.$$

We will now look at some of the properties of addition on $\mathbb{Z}$. The following theorem states that $(\mathbb{Z}, +)$ is an abelian group.

Theorem 3.6. *Let $x, y, z \in \mathbb{Z}$*

(1) $(x+y)+z = x+(y+z)$ (Associative Law for Addition)
(2) $x+y = y+x$ (Commutative Law for Addition)
(3) $x+\hat{0} = x$ (Identity Law for Addition)
(4) $x+(-x) = \hat{0}$ (Inverses Law for Addition)

Proof. (1) This proof can be found on page 13 of [1].

(2) This proof can be found on page 13 of [1].

(3) Let $x \in \mathbb{Z}$. Suppose $x = [(a,b)]$ for some $a,b \in \mathbb{N}$. Then,

$$\begin{aligned} x+\hat{0} = [(a,b)] + [(1,1)] &= [(a+1, b+1)] \\ &= \{(c,d) \in \mathbb{N}\times\mathbb{N} : (a+1)+d = (b+1)+c\} \\ &\overset{2.10(4)}{=} \{(c,d) \in \mathbb{N}\times\mathbb{N} : a+d = b+c\} \\ &= [(a,b)] = x \end{aligned}$$

Therefore, $x+\hat{0} = x$.

(4) Let $x \in \mathbb{Z}$. Suppose $x = [(a,b)]$ for some $a,b \in \mathbb{N}$. By the definition of $-$, $(-x) = [(b,a)]$. Then,

$$\begin{aligned} x+(-x) = [(a,b)] + [(b,a)] &= [(a+b, b+a)] \\ &= \{(c,d) \in \mathbb{N}\times\mathbb{N} : (a+b)+d = (b+a)+c\} \\ &\overset{2.10(3)(4)}{=} \{(c,d) \in \mathbb{N}\times\mathbb{N} : d = c\} \\ &= [(1,1)] = \hat{0} \end{aligned}$$

Therefore, $x + (-x) = \hat{0}$.

□

Next, we will define multiplication on the integers.

Definition 3.7. *The binary operation $\cdot$ on $\mathbb{Z}$ is defined by*

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

It can be shown that $\cdot$ is well defined. Now, we can show that multiplication on the set of integers has the properties we expect.

Theorem 3.8. *Let $x, y, z \in \mathbb{Z}$*

(1) $(xy)z = x(yz)$ (Associative Law for Multiplication)
(2) $x \cdot \hat{1} = x$ (Identity Law for Multiplication)
(3) $xy = yx$ (Commutative Law for Multiplication)
(4) $x(y + z) = xy + xz$ (Distributive Law)
(5) If $xy = \hat{0}$, then $x = \hat{0}$ or $y = \hat{0}$ (No Zero Divisors Law)

Proof. A proof for (5) can be found on page 13 of [1]. We will only prove (2) here, but the rest can be proved in a similar way.

Let $x \in \mathbb{Z}$. Suppose $x = [(a,b)]$ for some $a, b \in \mathbb{N}$. Then,

$$\begin{aligned} x \cdot \hat{1} &= [(a,b)] \cdot [(2,1)] \\ &= [(2a + b, a + 2b)] \\ &= \{(c,d) \in \mathbb{N} \times \mathbb{N} : 2a + b + d = a + 2b + c\} \\ &\overset{2.10(4)}{=} \{(c,d) \in \mathbb{N} \times \mathbb{N} : a + d = b + c\} \\ &= [(a,b)] = x \end{aligned}$$

Therefore, $x \cdot \hat{1} = x$ □

Theorem 3.8 (1), (2), and (3) give that $(\mathbb{Z}, \cdot)$ is a commutative monoid.

The standard orders on $\mathbb{Z}$ can be defined in the following way.

Definition 3.9. *The relation $<$ on $\mathbb{Z}$ is defined by $[(a,b)] < [(c,d)]$ if and only if $a+d < b+c$ ($[(a,b)], [(c,d)] \in \mathbb{Z}$).*

The relation $\leq$ on $\mathbb{Z}$ is defined by $[(a,b)] \leq [(c,d)]$ if and only if $[(a,b)] < [(c,d)]$ or $[(a,b)] = [(c,d)]$ ($[(a,b)], [(c,d)] \in \mathbb{Z}$).

A proof that $<$ is well defined on $\mathbb{Z}$ is on page 13 of [1]. Since the relation $\leq$ is defined in terms of $<$, it follows that $\leq$ is also well defined.

Some important properties of the relation $<$ are given below. A proof for (3) in the following theorem can be found on page 13 of [1], and a proof for (5) can be found on page 16.

Theorem 3.10. *Let $x, y, z \in \mathbb{Z}$*

(1) Precisely one of $x < y$ or $x = y$ or $x > y$ holds (Trichotomy Law)

(2) If $x < y$ and $y < z$, then $x < z$ (Transitive Law)
(3) If $x < y$ then $x + z < y + z$ (Addition Law for Order)
(4) If $x < y$ and $z > \hat{0}$, then $xz < yz$ (Multiplication Law for Order)
(5) $\hat{0} < \hat{1}$ (Non-Triviality)

The properties in the following theorem can be proved from the properties we already have. Parts (2), (6), and (8) are proved on page 16 of [1].

Theorem 3.11. *Let $x, y, z \in \mathbb{Z}$*

(1) If $x + z = y + z$, then $x = y$. (Cancellation Law for Addition).
(2) $-(-x) = x$.
(3) $-(x + y) = (-x) + (-y)$.
(4) $x \cdot \hat{0} = \hat{0}$.
(5) If $z \neq \hat{0}$ and if $xz = yz$, then $x = y$ (Cancellation Law for Multiplication).
(6) $(-x)y = -xy = x(-y)$.
(7) $xy = \hat{1}$ if and only if $x = \hat{1} = y$ or $x = -\hat{1} = y$.
(8) $x > \hat{0}$ if and only if $-x < \hat{0}$, and $x < \hat{0}$ if and only if $-x > \hat{0}$.
(9) If $x \leq y$ and $y \leq x$, then $x = y$.
(10) If $x > \hat{0}$ and $y > \hat{0}$, then $xy > \hat{0}$. If $x > \hat{0}$ and $y < \hat{0}$, then $xy < \hat{0}$.

Though the natural numbers and the integers are disjoint sets, we can find a copy of the set of natural numbers in the set of integers by defining the following mapping.

Theorem 3.12. *Let $i : \mathbb{N} \to \mathbb{Z}$ be defined by*

$$i(n) = [(n + 1, 1)].$$

(1) The function i is injective.
(2) $i(\mathbb{N}) = \{x \in \mathbb{Z} : x > \hat{0}\}$.
(3) $i(1) = \hat{1}$
(4) Let $a, b \in \mathbb{N}$. Then
  a) $i(a + b) = i(a) + i(b)$;
  b) $i(ab) = i(a)i(b)$;
  c) $a < b$ if and only if $i(a) < i(b)$.

Proof. (1) Let $a, b \in \mathbb{N}$ be distinct elements such that $i(a) = i(b)$. Then, by the way we defined i,

$$i(a) = [(a + 1, 1)] = [(b + 1, 1)] = i(b).$$

So, $(a + 1, 1) \sim (b + 1, 1)$. Then,

$$(a + 1) + 1 = 1 + (b + 1).$$

By cancellation, $a = b$, hence $i : \mathbb{N} \to \mathbb{Z}$ is injective.
(3) It is clear that $i(1) = [(1 + 1, 1)] = \hat{1}$.

(4*b*) Let $a, b \in \mathbb{N}$. By the way we defined i and the properties of $\mathbb{N}$,

$$\begin{aligned} i(ab) = [(ab+1,1)] &= \{(c,d) \in \mathbb{N} \times \mathbb{N} : (ab+1) + d = 1 + c\} \\ &\overset{2.10(4)}{=} \{(c,d) \in \mathbb{N} \times \mathbb{N} : (ab+1) + d + a + b + 1 = 1 + c + a + b + 1\} \\ &\overset{2.10(1)}{=} \{(c,d) \in \mathbb{N} \times \mathbb{N} : ab + a + b + 1 + 1 + d = a + 1 + b + 1 + c\} \\ &\overset{2.12(2)}{=} \{(c,d) \in \mathbb{N} \times \mathbb{N} : (a+1)(b+1) + 1 \cdot 1 + d = (a+1) \cdot 1 + (b+1) \cdot 1 + c\} \\ &= [((a+1)(b+1) + 1 \cdot 1, (a+1) \cdot 1 + (b+1) \cdot 1)] \\ &\overset{3.7}{=} [(a+1,1)] \cdot [(b+1,1)] \\ &= i(a)i(b) \end{aligned}$$

(4*c*) ($\Rightarrow$) Let $a, b \in \mathbb{N}$. Suppose $a < b$. Then by the properties of $\mathbb{N}$,

$$(a+1) + 1 < 1 + (b+1).$$

By Definition 3.9, $[(a+1,1)] < [(b+1,1)]$, which is equivalent to $i(a) < i(b)$.

($\Leftarrow$) Let $a, b \in \mathbb{N}$. Suppose $i(a) < i(b)$. Then, $[(a+1,1)] < [(b+1,1)]$ and by Definition 3.9,

$$(a+1) + 1 < 1 + (b+1).$$

By the properties of $\mathbb{N}$, $a < b$.

Proofs for (2) and (4a) are on page 14 of [1]. □

Note that $\hat{2} = [(1+1+1,1)] = [(3,1)]$, $\hat{3} = [(4,1)]$, and so on.

The following theorem shows that $(\mathbb{Z}, \leq)$ is a total order.

Theorem 3.13. *Let $x, y, z \in \mathbb{Z}$.*

(1) $x \leq x$.
(2) If $x \leq y$ and $y \leq x$, then $x = y$.
(3) If $x \leq y$ and $y \leq z$, then $x \leq z$.
(4) Precisely one of $x < y$ or $x = y$ or $x > y$ holds. (Trichotomy Law)

Observe that all equations of the type $x + n = m$ where $n, m \in \mathbb{Z}$ are solvable in $\mathbb{Z}$. Namely, $x = m + (-n) \in \mathbb{Z}$.

The integers can be represented in terms of sets by using Kuratowski's definition of an ordered pair given below.

Definition 3.14. *Let A be a set and $a, b \in A$. The ordered pair (a, b) is defined by* $(a, b) = \{\{a\}, \{a, b\}\}$

Using this definition, the elements of $\mathbb{Z}$ are represented as follows.

$$\begin{aligned}
&\vdots \\
-\hat{1} = [(1,2)] &= [\{\{1\},\{1,2\}\}] = \{\{\{a\},\{a,a+1\}\} : a \in \mathbb{N}\} \\
\hat{0} = [(1,1)] &= [\{\{1\}\}] = \{\{\{a\}\} : a \in \mathbb{N}\} \\
\hat{1} = [(2,1)] &= [\{\{2\},\{2,1\}\}] = \{\{\{1+a\},\{1+a,1\}\} : a \in \mathbb{N}\} \\
\hat{2} = [(3,1)] &= [\{\{3\},\{3,1\}\}] = \{\{\{1+1+a\},\{1+1+a,1\}\} : a \in \mathbb{N}\} \\
&\vdots
\end{aligned}$$

For the remainder of this paper, when referring to the integers, we will write 0 in place of $\hat{0}$, 1 in place of $\hat{1}$, and so on.

4. The construction of the Rational Numbers

So far, we have a set, the integers, which contains a copy of the natural numbers within it and has the operations $+$, $-$ and $\cdot$ as well as the relations $<$ and $\leq$. We see that an equation of the type

$$cx = d \tag{4}$$

where $c, d \in \mathbb{Z}$ is solvable in $\mathbb{Z}$ if and only if $d = kc$ for some $k \in \mathbb{Z}$. Again, we would like to find a "larger" set of numbers with compatible operations $+, \cdot$, and $<$ such that every equation of the type (4), with $c \neq 0$, is solvable in this new set.

To define this "larger" set, we will need a new relation that will allow us to find multiplicative inverses in this set, similar to the way the relation $\sim$ allowed us to find additive inverses in $\mathbb{Z}$.

Definition 4.1. *Let $\mathbb{Z}^* = \mathbb{Z} - \{0\}$. The relation $\asymp$ on $\mathbb{Z} \times \mathbb{Z}^*$ is defined by $(x,y) \asymp (z,w)$ if and only if $xw = yz$, for all $(x,y),(z,w) \in \mathbb{Z} \times \mathbb{Z}^*$.*

This relation being based on multiplication is what will allow us to define multiplicative inverses and division.

A proof for the following lemma is on page 27 of [1].

Lemma 4.2. *The relation $\asymp$ is an equivalence relation.*

Definition 4.3 (Rational Numbers)**.** *The set of rational numbers, denoted $\mathbb{Q}$, is the set of equivalence classes of $\mathbb{Z} \times \mathbb{Z}^*$ with respect to the equivalence relation $\asymp$. That is,*

$$\mathbb{Q} = \{[(x,y)] : x \in \mathbb{Z} \text{ and } y \in \mathbb{Z}^*\}.$$

The elements $\bar{0}, \bar{1} \in \mathbb{Q}$ are defined by

$$\bar{0} := [(0,1)] = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : 0 \cdot y = 1 \cdot x\} \overset{3.8(2),3.11(4)}{=} \{(0,y) \in \mathbb{Z} \times \mathbb{Z}^*\}$$

and

$$\bar{1} := [(1,1)] = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : 1 \cdot y = 1 \cdot x\} \overset{3.8(2)}{=} \{(x,x) \in \mathbb{Z} \times \mathbb{Z}^*\}.$$

Notice that the elements of the set of rational numbers, similar to the integers, are equivalence classes. The difference here is that, for $\mathbb{Q}$, the set of equivalence classes is obtained from the relation $\asymp$ on $\mathbb{Z} \times \mathbb{Z}^*$, whereas for $\mathbb{Z}$, the set of equivalence classes is obtained from the relation $\sim$ on $\mathbb{N} \times \mathbb{N}$.

The following two theorems describe which ordered pairs represent the rational numbers $\bar{0}$ and $\bar{1}$, respectively.

Theorem 4.4. *Let $x \in \mathbb{Z}$ and $y \in \mathbb{Z}^*$. Then $[(x, y)] = \bar{0}$ if and only if $x = 0$.*

Proof. ($\Rightarrow$) Suppose $[(x, y)] = \bar{0}$. Then,

$$(x, y) \in [(0, 1)] = \{(z, w) \in \mathbb{Z} \times \mathbb{Z}^* : 0 \cdot w = 1 \cdot z\}.$$

Thus, $z = 0$ for all $(z, w) \in [(0, 1)]$. Therefore, $x = 0$.

($\Leftarrow$) Suppose $x = 0$. Then,

$$[(x, y)] = [(0, y)] = \{(z, w) \in \mathbb{Z} \times \mathbb{Z} : 0 \cdot w = y \cdot z\}.$$

It is clear that $(0, 1) \in [(x, y)]$,whence $[(x, y)] = [(0, 1)] = \bar{0}$. □

Theorem 4.5. *Let $x \in \mathbb{Z}$ and $y \in \mathbb{Z}^*$. Then $[(x, y)] = \bar{1}$ if and only if $x = y$.*

Proof. ($\Rightarrow$) Suppose $[(x, y)] = \bar{1}$. Then,

$$\begin{aligned}(x, y) = [(1, 1)] &= \{(z, w) \in \mathbb{Z} \times \mathbb{Z}^* : 1 \cdot w = 1 \cdot z\} \\ &= \{(z, w) \in \mathbb{Z} \times \mathbb{Z}^* : w = z\}.\end{aligned}$$

Thus, $x = y$.

($\Leftarrow$) Suppose $x = y$. Then,

$$\begin{aligned}[(x, y)] = [(x, x)] &= \{(z, w) \in \mathbb{Z} \times \mathbb{Z}^* : x \cdot w = x \cdot z\} \\ &\overset{3.11(5)}{=} \{(z, w) \in \mathbb{Z} \times \mathbb{Z}^* : w = z\}.\end{aligned}$$

Clearly, $(1, 1) \in [(x, y)]$, so $[(x, y)] = [(1, 1)] = \bar{1}$. □

Addition on $\mathbb{Q}$ is defined as follows.

Definition 4.6. *The binary operation $+$ on $\mathbb{Q}$ is defined by*

$$[(x, y)] + [(z, w)] = [(xw + yz, yw)]$$

for all $[(x, y)], [(z, w)] \in \mathbb{Q}$.

It can be shown that $+$ on $\mathbb{Q}$ is well-defined.

Definition 4.7. *The unary operation $-$ on $\mathbb{Q}$ is defined by*

$$-[(x, y)] = [(-x, y)], \quad [(x, y)] \in \mathbb{Q}.$$

A proof that $-$ on $\mathbb{Q}$ is well-defined can be found on page 28 of [1].

The below theorem shows that $(\mathbb{Q}, +)$ is an abelian group. A proof for (3) below can be found on page 29 of [1].

Theorem 4.8. *Let $r, s, t \in \mathbb{Q}$.*

(1) $(r+s)+t = r+(s+t)$ *(Associative Law for Addition)*
(2) $r+\bar{0} = r$ *(Identity Law for Addition)*
(3) $r+(-r) = \bar{0}$ *(Inverses Law for Addition)*
(4) $r+s = s+r$ *(Commutative Law for Addition)*

Proof. (2) Let $r = [(x,y)]$ where $(x,y) \in \mathbb{Z} \times \mathbb{Z}^*$. By Definition 4.6,

$$r + \bar{0} = [(x,y)] + [(0,1)] = [(x \cdot 1 + y \cdot 0, y \cdot 1)] = [(x,y)] = r.$$

(4) Let $r = [(x,y)]$ and $s = [(z,w)]$ where $(x,y),(z,w) \in \mathbb{Z} \times \mathbb{Z}^*$. Then,

$$r + s = [(x,y)] + [(z,w)] \overset{4.6}{=} [(xw+yz, yw)] \overset{3.6(2)}{=} [(yz+xw, yw)]$$
$$\overset{3.8(3)}{=} [(zy+wx, wy)] = [(z,w)] \cdot [(x,y)] = s + r.$$

□

Multiplication on $\mathbb{Q}$ is defined component-wise.

Definition 4.9. *The binary operation $\cdot$ on $\mathbb{Q}$ is defined by*

$$[(x,y)] \cdot [(z,w)] = [(xz, yw)]$$

for all $[(x,y)], [(z,w)] \in \mathbb{Q}$.

A proof that $\cdot$ on $\mathbb{Q}$ is well-defined can be found on page 28 of [1].

Our next goal is to show that $(\mathbb{Q}^*, \cdot)$ is an abelian group (recall that $(\mathbb{Z}, \cdot)$ is just a commutative monoid). We will start by defining a new unary operation on $\mathbb{Q}$.

Definition 4.10. *Let $\mathbb{Q}^* = \mathbb{Q} - \{\bar{0}\}$. The unary operation $^{-1}$ on $\mathbb{Q}^*$ is defined by $[(x,y)]^{-1} = [(y,x)]$ for all $[(x,y)] \in \mathbb{Q}^*$.*

A proof for (2) in the following theorem is given on page 29 of [1]. Properties (1), (2), (3), and (4) show that $(\mathbb{Q}, \cdot)$ an abelian group.

Theorem 4.11. *Let $r, s, t \in \mathbb{Q}$.*

(1) $(rs)t = r(st)$ *(Associative Law for Multiplication)*
(2) $r \cdot \bar{1} = r$ *(Identity Law for Multiplication)*
(3) If $r \neq \bar{0}$, then $r \cdot r^{-1} = \bar{1}$ (Inverses Law for Multiplication)
(4) $rs = sr$ *(Commutative Law for Multiplication)*
(5) $r(s+t) = rs + rt$ *(Distributive Law)*

Theorem 4.11 along with Theorem 4.8 makes $(\mathbb{Q}, +, \cdot)$ a field. In fact, we will soon see that $(\mathbb{Q}, +, \cdot, <)$ is an ordered field.

Definition 4.12. *The relation $<$ on $\mathbb{Q}$ is defined by ($[(x,y)], [(z,w)] \in \mathbb{Q}$),*

$$[(x,y)] < [(z,w)] \text{ if and only if } \begin{cases} xw < yz & \text{whenever } y,w > 0 \text{ or } y,w < 0 \\ xw > yz & \text{whenever } y > 0, w < 0 \text{ or } y < 0, w > 0. \end{cases}$$

The relation $\leq$ on $\mathbb{Q}$ is defined by $[(x,y)] \leq [(z,w)]$ if and only if either $[(x,y)] < [(z,w)]$ or $[(x,y)] = [(z,w)]$, for all $[(x,y)], [(z,w)] \in \mathbb{Q}$.

It can be shown that $<$ is well-defined, and the fact that $\leq$ is well-defined follows.

Theorem 4.13. *Let $x \in \mathbb{Z}$ and $y \in \mathbb{Z}^*$. $\bar{0} < [(x, y)]$ if and only if $0 < xy$.*

Proof. ($\Rightarrow$) Suppose $\bar{0} = [(0, 1)] < [(x, y)]$. By Definition 4.14, since $1 > 0$, either

$$0 \cdot y < 1 \cdot x \text{ if } y > 0$$

or

$$0 \cdot y > 1 \cdot x \text{ if } y < 0.$$

Thus, if $y > 0$, then $x > 0$, and if $y < 0$, then $x < 0$. In either case, $0 < xy$.

($\Leftarrow$) Suppose $0 < xy$. There are two cases.

Case 1: $x > 0$ and $y > 0$. Then, $0 \cdot y < 1 \cdot x$, which implies $\bar{0} = [(0, 1)] < [(x, y)]$.

Case 2: $x < 0$ and $y < 0$. Then, $0 \cdot y > 1 \cdot x$, which implies $\bar{0} = [(0, 1)] < [(x, y)]$. □

Similarly, by applying Definition 4.7, we can see that $\bar{0} > [(x, y)]$ if and only if $0 > xy$.

The following theorem gives the remaining properties that make $(\mathbb{Q}, +, \cdot, <)$ an ordered field. Parts (1) and (4) of the following theorem are proved on page 29 of [1].

Theorem 4.14. *Let $r, s, t \in \mathbb{Q}$.*

(1) Precisely one of $r < s$ or $r = s$ or $r > s$ holds (Trichotomy Law)
(2) If $r < s$ and $s < t$, then $r < t$ (Transitive Law)
(3) If $r < s$ then $r + t < s + t$ (Addition Law for Order)
(4) If $r < s$ and $t > \bar{0}$, then $rt < st$ (Multiplication Law for Order)
(5) $\bar{0} < \bar{1}$ (Non-Triviality)
(6) Let $s \in \mathbb{Q}$. Then $s \cdot s \geq \bar{0}$.

Proof. (6) If $s = \bar{0}$, then $s \cdot s = \bar{0} \cdot \bar{0} = \bar{0}$.

If $s > \bar{0}$, then by Theorem 4.14(4), $s \cdot s > \bar{0} \cdot s = \bar{0}$.

If $s < \bar{0}$, then $-s > \bar{0}$. By Theorem 4.14(4), $s \cdot (-s) = -(s \cdot s) < \bar{0} \cdot (-s) = \bar{0}$. Thus, $s \cdot s > \bar{0}$. □

Once again, we can find a copy of the set of integers inside the set of rational numbers. Part (4) of the following theorem is proved on page 30 of [1].

Theorem 4.15. *Let $i : \mathbb{Z} \to \mathbb{Q}$ be defined by*

$$i(x) = [(x, 1)].$$

(1) The function i is injective.
(2) $i(0) = \bar{0}$ and $i(1) = \bar{1}$.
(3) Let $x, y \in \mathbb{Z}$. Then
  a) $i(x + y) = i(x) + i(y)$;
  b) $i(-x) = -i(x)$;
  c) $i(xy) = i(x)i(y)$;
  d) $x < y$ if and only if $i(x) < i(y)$.

This mapping preserves additive and multiplicative identities as well as the operations $+$, $-$, $\cdot$, and the relation $<$. It also preserves the relation $\leq$ since $\leq$ was defined in terms of $<$. Below are some properties of the relation $\leq$.

Theorem 4.16. *Let $r, s, t \in \mathbb{Q}$.*

(1) $r \leq r$.
(2) If $r \leq s$ and $s \leq r$, then $r = s$.
(3) If $r \leq s$ and $s \leq t$, then $r \leq t$.
(4) Precisely one of $r < s$ or $r = s$ or $r > s$ holds. (Trichotomy Law)

Theorem 4.16 shows that $(\mathbb{Q}, \leq)$ is a total order.

The binary operations of subtraction and division are defined in terms of addition with additive inverses and multiplication with multiplicative inverses, respectively.

Definition 4.17. *The binary operation $-$ on $\mathbb{Q}$ is defined by $r - s = r + (-s)$ for all $r, s \in \mathbb{Q}$. The binary operation $\div$ on $\mathbb{Q}^*$ is defined by $r \div s = rs^{-1}$ for all $r, s \in \mathbb{Q}^*$; we also let $\bar{0} \div s = \bar{0} \cdot s^{-1} = \bar{0}$ for all $s \in \mathbb{Q}^*$. The number $r \div s$ is also denoted $\frac{r}{s}$.*

The following lemma is a restatement of previous properties using this new notation.

Lemma 4.18. *Let $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{Z}^*$.*

(1) $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.
(2) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.
(3) $-\frac{a}{b} = \frac{-a}{b}$.
(4) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.
(5) If $a \neq 0$, then $(\frac{a}{b})^{-1} = \frac{b}{a}$.
(6) If $b > 0$ and $d > 0$, or if $b < 0$ and $d < 0$, then $\frac{a}{b} < \frac{c}{d}$ if and only if $ad < bc$; if $b > 0$ and $d < 0$, or if $b < 0$ and $d > 0$, then $\frac{a}{b} < \frac{c}{d}$ if and only if $ad > bc$.

Notice that an equation $cx = d$ with $c \in \mathbb{Q}^*$ and $d \in \mathbb{Q}$ is solvable in $\mathbb{Q}$. Namely, $x = \frac{d}{c} \in \mathbb{Q}$.

Just as we did for the integers, we can write the elements of $\mathbb{Q}$ in terms of sets. We only express $\bar{0}$ and $\bar{1}$ in terms of sets below, but other $r \in \mathbb{Q}$ can be expressed in a similar manner.

$$\bar{0} = [(0,1)] = [\{\{0\}, \{0,1\}\}] = \{\{\{\{\{a\}\}\}\}, \{\{\{\{a\}\}\}, \{\{\{1+a\}, \{1+a, 1\}\}\}\} : a \in \mathbb{N}\}$$
$$\bar{1} = [(1,1)] = [\{\{1\}\}] = \{\{\{\{\{1+a\}, \{1+a, 1\}\}\}\} : a \in \mathbb{N}\}$$

5. The construction of the Real Numbers

We will now switch to writing 0 instead of $\bar{0}$, 1 instead of $\bar{1}$, and so on.

Observe that an equation of the type

$$x \cdot x = r \tag{5}$$

where $r \in \mathbb{Q}$ is solvable in $\mathbb{Q}$ if and only if $r = s \cdot s$ for some $s \in \mathbb{Q}$. We can see that $r = 2$ has no solution to (5) in $\mathbb{Q}$. Since $s \cdot s \geq 0$ for all $s \in \mathbb{Q}$, we would like to construct a set of numbers which is "larger" than $\mathbb{Q}$ (with compatible operations $+, \cdot$, and $<$) such that every equation of the type (5) is solvable for $r \in \mathbb{Q}$ with $r \geq 0$.

In order to construct the set we desire, we will first need to introduce a new type of set.

Definition 5.1. *Let $A \subset \mathbb{Q}$ be a set. The set A is a Dedekind cut if the following three properties hold.*

a) $A \neq \emptyset$ and $A \neq \mathbb{Q}$.
b) Let $x \in A$. If $y \in \mathbb{Q}$ and $y \geq x$, then $y \in A$.
c) Let $x \in A$. Then there is some $y \in A$ such that $y < x$.

So a Dedekind cut is a non-empty proper subset of $\mathbb{Q}$ containing all elements greater than some value, but it does not have a smallest element. Since the construction of the real numbers is quite different than the previous set constructions, we will first discuss Dedekind cuts in more detail to aid in understanding the real numbers.

A proof for the following lemma can be found on page 35 of [1].

Lemma 5.2. *Let $r \in \mathbb{Q}$. Then the set*

$$\{x \in \mathbb{Q} : x > r\}$$

is a Dedekind cut.

The following definition will describe the two types of Dedekind cuts.

Definition 5.3. *Let $r \in \mathbb{Q}$. The rational cut at r, denoted D_r, is the Dedekind cut*

$$D_r = \{x \in \mathbb{Q} : x > r\}.$$

An irrational cut is a Dedekind cut that is not a rational cut at any rational number.

This classification of cuts is how we will distinguish between rational and irrational numbers.

The complement of a Dedekind cut will also be useful.

Lemma 5.4. *Let $A \subseteq \mathbb{Q}$ be a Dedekind cut.*

(1) $\mathbb{Q} - A = \{x \in \mathbb{Q} : x < a \text{ for all } a \in A\}$
(2) Let $x \in \mathbb{Q} - A$. If $y \in \mathbb{Q}$ and $y \leq x$, then $y \in \mathbb{Q} - A$.

Proof. (1) This proof can be found on page 36 of [1].
(2) Let $x \in \mathbb{Q} - A$. Then, $x < a$. Suppose $y \in \mathbb{Q}$ and $y \leq x$. By transitivity, $y < a$, hence $y \in \mathbb{Q} - A$.

□

The following lemma will help us to define order on the set of real numbers. A proof can be found on page 37 of [1].

Lemma 5.5. *Let $A, B \subset \mathbb{Q}$ be Dedekind cuts. Then precisely one of $A \subsetneq B$ or $A = B$ or $B \subsetneq A$ holds.*

We can also consider the union of Dedekind cuts. A proof for the following lemma can be found on page 37 of [1].

Lemma 5.6. *Let $\mathcal{A}$ be a non-empty family of Dedekind cuts of $\mathbb{Q}$. If $\bigcup_{A \in \mathcal{A}} A \neq \mathbb{Q}$, then $\bigcup_{A \in \mathcal{A}} A$ is a Dedekind cut.*

Example 1. Suppose that $a_0 > 0$ and let $A_n = D_{a_n} = \{x \in \mathbb{Q} : x > a_n\}$ where

$$a_n = \frac{1}{2}\left(\frac{2}{a_{n-1}} + a_{n-1}\right) \tag{6}$$

The sequence (a_n) is strictly decreasing. Since $0 \notin \bigcup_{n=0}^{\infty} A_n$, we can see that $\bigcup_{n=0}^{\infty} A_n \neq \mathbb{Q}$, which implies $\bigcup_{n=0}^{\infty} A_n$ is a Dedekind cut. Because (6) does not converge in $\mathbb{Q}$, $\bigcup_{n=0}^{\infty} A_n$ is an irrational cut.

Since we are interested in arithmetic operations on the set of real numbers, we would like to see that those operations on Dedekind cuts produce another Dedekind cut. That is the case, as we can see in the following lemma.

Lemma 5.7. *Let $A, B \subset \mathbb{Q}$ be Dedekind cuts.*

(1) The set

$$\{r \in \mathbb{Q} : r = a + b \text{ for some } a \in A \text{ and } b \in B\}$$

is a Dedekind cut.

(2) The set

$$\{r \in \mathbb{Q} : -r < c \text{ for some } c \in \mathbb{Q} - A\}$$

is a Dedekind cut.

(3) Suppose that $0 \in \mathbb{Q} - A$ and $0 \in \mathbb{Q} - B$. The set

$$\{r \in \mathbb{Q} : r = ab \text{ for some } a \in A \text{ and } b \in B\}$$

is a Dedekind cut.

(4) Suppose that there is some $q \in \mathbb{Q} - A$ such that $q > 0$. The set

$$\{r \in \mathbb{Q} : r > 0 \text{ and } \frac{1}{r} < c \text{ for some } c \in \mathbb{Q} - A\}$$

is a Dedekind cut.

Proof. Proofs for parts (1), (2), and (4) can be found on page 38 of [1].

(3) Suppose that $0 \in \mathbb{Q} - A$ and $0 \in \mathbb{Q} - B$ where A and B are Dedekind cuts. Let

$$C = \{r \in \mathbb{Q} : r = ab \text{ for some } a \in A \text{ and } b \in B\}.$$

Clearly, $C \neq \emptyset$. Since $0 \notin C$, then $C \neq \mathbb{Q}$.

Now, let $x \in C$. So, $x = ab$ for some $a \in A$ and $b \in B$. Suppose $y \in \mathbb{Q}$ and $y \geq x$. If $y = x$, then $y = ab \in C$. Suppose $y > x$. Since $y \in \mathbb{Q}$, then $y = a_1 b_1$ for some $a_1, b_1 \in \mathbb{Q}$. Take $a_1 = a$. Then,

$$y = ab_1 > ab = x.$$

Since $a > 0$ ($0 \in \mathbb{Q} - A$), then $a^{-1} > 0$. By Theorem 4.14(4),

$$a^{-1}ab_1 > a^{-1}ab.$$

Thus, $b_1 > b$, which implies $b_1 \in B$. Therefore, $y = ab_1 \in C$.

Suppose $x = a_1 b_1 \in C$ is the smallest element in C. Since $a_1 \in A$ and A is a Dedekind cut, there exists some $a_0 \in A$ such that $a_0 < a_1$. Let $y = a_0 b_1$. Then $y \in C$. Since $b_1 > 0$ $(0 \in \mathbb{Q} - B)$, then $a_0 b_1 < a_1 b_1$.

Therefore, by Definition 5.1, C is a Dedekind cut. □

A proof for the following lemma can be found on page 39 of [1].

Lemma 5.8. *Let $A \subset \mathbb{Q}$ be a Dedekind cut. Let $y \in \mathbb{Q}$.*

(1) Suppose that $y > 0$. Then there are $u \in A$ and $v \in \mathbb{Q} - A$ such that $y = u - v$, and $v < c$ for some $c \in \mathbb{Q} - A$.

(2) Suppose that $y > 1$, and that there is some $q \in \mathbb{Q} - A$ such that $q > 0$. Then there are $r \in A$ and $s \in \mathbb{Q} - A$ such that $s > 0$, and $y > \frac{r}{s}$, and $s < g$ for some $g \in \mathbb{Q} - A$.

We are now ready to define the set of real numbers.

Definition 5.9. *The set of real numbers, denoted $\mathbb{R}$, is defined by*

$$\mathbb{R} = \{A \subset \mathbb{Q} : A \text{ is a Dedekind cut } \}.$$

Using Lemma 5.7(1), we define addition on $\mathbb{R}$ in the following way.

Definition 5.10. *The binary operation $+$ on $\mathbb{R}$ is defined by*

$$A + B = \{r \in \mathbb{Q} : r = a + b \text{ for some } a \in A \text{ and } b \in B\}$$

for all $A, B \in \mathbb{R}$. The unary operation $-$ on $\mathbb{R}$ is defined by

$$-A = \{r \in \mathbb{Q} : -r < c \text{ for some } c \in \mathbb{Q} - A\}$$

for all $A \in \mathbb{R}$.

By Lemma 5.7, $A + B$ and $-A$ are Dedekind cuts.

We define

$$\tilde{0} := D_0 = \{x \in \mathbb{Q} : x > 0\},$$

$$\tilde{1} := D_1 = \{x \in \mathbb{Q} : x > 1\}.$$

Now, we will show that addition on $\mathbb{R}$ has the properties we expect. Proofs for (1), (3), and (4) below can be found on page 44 of [1].

Lemma 5.11. *Let $A, B, C \in \mathbb{R}$.*

(1) $(A + B) + C = A + (B + C)$ (Associative Law for Addition).

(2) $A + B = B + A$ (Commutative Law for Addition).

(3) $A + \tilde{0} = A$ (Identity Law for Addition).

(4) $A + (-A) = \tilde{0}$ (Inverses Law for Addition).

We see that $(\mathbb{R}, +)$ is an abelian group.

Multiplication on $\mathbb{R}$ is defined in the following way.

Definition 5.12. *The binary operation $\cdot$ on $\mathbb{R}$ is defined by*

$$A \cdot B = \begin{cases} \{r \in \mathbb{Q} : r = ab \text{ for some } a \in A \text{ and } b \in B\}, & \text{if } A \geq \tilde{0} \text{ and } B \geq \tilde{0} \\ -[(-A) \cdot B], & \text{if } A < \tilde{0} \text{ and } B \geq \tilde{0} \\ -[A \cdot (-B)], & \text{if } A \geq \tilde{0} \text{ and } B < \tilde{0} \\ (-A) \cdot (-B), & \text{if } A < \tilde{0} \text{ and } B < \tilde{0}. \end{cases}$$

The unary operation $^{-1}$ is defined by

$$A^{-1} = \begin{cases} \{r \in \mathbb{Q} : r > 0 \text{ and } \frac{1}{r} < c \text{ for some } c \in \mathbb{Q} - A\}, & \text{if } A > \tilde{0} \\ -(-A)^{-1}, & \text{if } A < \tilde{0}. \end{cases}$$

Again, from Lemma 5.7, we know that $A \cdot B$ and A^{-1} are Dedekind cuts.

We define $\mathbb{R}^*$ by $\mathbb{R}^* = \mathbb{R} - \{\tilde{0}\}$. We can see from the following lemma that multiplication on $\mathbb{R}$ has the properties that make $(\mathbb{R}^*, \cdot)$ an abelian group. Parts (2), (4), and (5) of the following lemma are proved on page 44 of [1].

Lemma 5.13. *Let $A, B, C \in \mathbb{R}$.*

(1) $(AB)C = A(BC)$ (Associative Law for Multiplication).
(2) $AB = BA$ (Commutative Law for Multiplication).
(3) $A \cdot \tilde{1} = A$ (Identity Law for Multiplication).
(4) If $A \neq \tilde{0}$, then $AA^{-1} = \tilde{1}$ (Inverses Law for Multiplication).
(5) $A(B + C) = AB + AC$ (Distributative Law).

By Lemma 5.11 and Lemma 5.13, we can see that $(\mathbb{R}, +, \cdot)$ is a field.

Next, we will define order on $\mathbb{R}$.

Definition 5.14. *The relation $<$ on $\mathbb{R}$ is defined by $A < B$ if and only if $A \supsetneq B$, for all $A, B \in \mathbb{R}$. The relation $\leq$ on $\mathbb{R}$ is defined by $A \leq B$ if and only if $A \supseteq B$, for all $A, B \in \mathbb{R}$.*

A proof for (3) in the following lemma can be found on page 43 of [1].

Lemma 5.15. *Let $A \in \mathbb{R}$, and let $r \in \mathbb{Q}$.*

(1) $A > D_r$ if and only if there is some $q \in \mathbb{Q} - A$ such that $q > r$.
(2) $A \geq D_r$ if and only if $r \in \mathbb{Q} - A$ if and only if $a > r$ for all $a \in A$.
(3) If $A < \tilde{0}$ then $-A \geq \tilde{0}$.

Proof. (1) ($\Rightarrow$) Let A be a Dedekind cut and let $D_r = \{x \in \mathbb{Q} : x > r\}$. Suppose $A > D_r$. Then by Definition 5.14, $D_r \supsetneq A$. Then there is some $s \in D_r$ such that $s \notin A$, that is $r < s < a$ for all $a \in A$. By Lemma 5.4(1), $s \in \mathbb{Q} - A$.

($\Leftarrow$) Let A be a Dedekind cut and let $D_r = \{x \in \mathbb{Q} : x > r\}$. Suppose there is some $q \in \mathbb{Q} - A$ such that $q > r$. Since $q \notin A$, it is the case that $q < a$. Because $q > r$, $q \in D_r$. This implies $D_r \supsetneq A$. By Definition 5.14, $A > D_r$.

(2) ($\Rightarrow$) Let A be a Dedekind cut and let $D_r = \{x \in \mathbb{Q} : x > r\}$. Suppose $A \geq D_r$. Then by Definition 5.14, $D_r \supseteq A$. If $A = D_r$, then their complements are equal as well. Since $r \notin D_r$, then $r \in \mathbb{Q} - D_r = \mathbb{Q} - A$. Since $r \notin A$, then $a > r$ for all $a \in A$. Suppose $D_r \supsetneq A$.

Then there is $s \in D_r$ such $s \notin A$, that is $r < s < a$ for all $a \in A$. By Lemma 5.4(1), since $r < a$, then $r \in \mathbb{Q} - A$.

($\Leftarrow$) Let A be a Dedekind cut and let $D_r = \{x \in \mathbb{Q} : x > r\}$. Suppose $r \in \mathbb{Q} - A$. Then by Lemma 5.4(1), $r < a$ for all $a \in A$. This implies $a \in D_r$ for all $a \in A$. Thus $D_r \supseteq A$. $\square$

For the following lemma, a proof for (2) can be found on page 44 of [1], a proof for (4) is on page 45, and a proof for (5) appears on page 46.

Lemma 5.16. *Let $A, B, C \in \mathbb{R}$.*

(1) Precisely one of $A < B$ or $A = B$ or $A > B$ holds (Trichotomy Law).
(2) If $A < B$ and $B < C$, then $A < C$ (Transitive Law).
(3) $\tilde{0} < \tilde{1}$.
(4) If $A < B$ then $A + C < B + C$ (Addition Law for Order).
(5) If $A < B$ and $C > \tilde{0}$, then $AC < BC$ (Multiplication Law for Order).

We have a copy of the set of rational numbers inside the set of real numbers.

Theorem 5.17. *Let $i : \mathbb{Q} \to \mathbb{R}$ be defined by*

$$i(r) = D_r.$$

(1) The function i is injective.
(2) $i(0) = \tilde{0}$ and $i(1) = \tilde{1}$.
(3) Let $r, s \in \mathbb{Q}$. Then
  a) $i(r + s) = i(r) + i(s)$;
  b) $i(-r) = -i(r)$;
  c) $i(rs) = i(r)i(s)$;
  d) if $r \neq 0$ then $i(r^{-1}) = [i(r)]^{-1}$;
  e) $r < s$ if and only if $i(r) < i(s)$.

The following theorem along with 5.16(1) show that $(\mathbb{R}, +, \cdot, \leq)$ is a total order.

Theorem 5.18. *Let $A, B, C \in \mathbb{R}$.*

(1) $A \leq A$.
(2) If $A \leq B$ and $B \leq A$, then $A = B$.
(3) If $A \leq B$ and $B \leq C$, then $A \leq C$.

We can define the elements of $\mathbb{R}$, in terms of sets only, like we did for the integers and rational numbers. We will only show $\tilde{0}$ here, but the other elements of $\mathbb{R}$ can be represented in a similar manner.

$$\tilde{0} = \{x \in \mathbb{Q} : x > \bar{0}\} \overset{4.13}{=} \{[(x, y)] \in \mathbb{Q} : xy > \hat{0}\}$$
$$\overset{3.7}{=} \{[([(a, b)], [(c, d)])] \in \mathbb{Q} : [(ac + bd, ad + bc)] > [(1, 1)]\}$$
$$= \{[([(a, b)], [(c, d)])] \in \mathbb{Q} : ac + bd + 1 > ad + bc + 1 \text{ where } a, b, c, d \in \mathbb{N}\}$$
$$= \{\{[([(a, b)], [(c, d)])] \in \mathbb{Q} : ac + bd > ad + bc \text{ where } a, b, c, d \in \mathbb{N}\}$$
$$= \{\{\{\{\{\{\{a\}, \{a, b\}\}\}\}\}, \{\{\{\{a\}, \{a, b\}\}\}, \{\{\{c\}, \{c, d\}\}\}\}\} : ac + bd > ad + bc \text{ where } a, b, c, d \in \mathbb{N}\}$$

At this point, we have seen that the properties for $+, \cdot$, and $<$ that we had with previous sets still hold for the real numbers. Now, we will discuss the properties that are unique to the real numbers.

Definition 5.19. *Let $A \subseteq \mathbb{R}$ be a set.*

(1) The set A is bounded above if there is some $M \in \mathbb{R}$ such that $X \leq M$ for all $X \in A$. The number M is called an upper bound of A.
(2) The set A is bounded below if there is some $P \in \mathbb{R}$ such that $X \geq P$ for all $X \in A$. The number P is called a lower bound of A.
(3) The set A is bounded if it is bounded above and bounded below.
(4) Let $M \in \mathbb{R}$. The number M is a least upper bound (also called a supremum) of A if M is an upper bound of A, and if $M \leq T$ for all upper bounds T of A.
(5) Let $P \in \mathbb{R}$. The number P is a greatest lower bound (also called a infimum) of A if P is a lower bound of A, and if $P \geq V$ for all lower bounds V of A.

A proof for the following theorem is given on page 47 of [1].

Theorem 5.20. *Let $A \subseteq \mathbb{R}$ be a set. If A is non-empty and bounded below, then A has a greatest lower bound.*

A proof of the following theorem can be found on page 48 of [1].

Theorem 5.21. *Let $A \subseteq \mathbb{R}$ be a set. If A is non-empty and bounded above, then A has a least upper bound.*

Theorem 5.21 is called a completeness axiom of $\mathbb{R}$. Based on it, one can prove that for every $x \in \mathbb{R}$, $x \geq \tilde{0}$, there is a $y \in \mathbb{R}$, $y \geq \tilde{0}$ such that $x \cdot x = y$. That is, every non-negative real number has a square root.

Another method of constructing $\mathbb{R}$ from $\mathbb{Q}$ is to use equivalence classes (with respect to a certain equivalence relation) of Cauchy sequences in the metric space $(\mathbb{Q}, |\cdot|)$, where $|\cdot|$ is the standard distance between rational numbers.

Observe that the equation

$$x \cdot x + 1 = 0 \tag{7}$$

is not solvable in $\mathbb{R}$. It turns out that we can construct another "larger" set of numbers, called the complex numbers (denoted $\mathbb{C}$), which "contains" $\mathbb{R}$ and has appropriate operations $+$ and $\cdot$ defined, so that (7) is solvable. Then, by the Fundamental Theorem of Algebra, every equation of the type

$$a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 = 0$$

where $a_i \in \mathbb{C}$ with $i = 1, 2, \ldots, n \in \mathbb{N}$ is solvable in $\mathbb{C}$.

Acknowledgment

This paper was written under the supervision of Dr. Damian Kubiak. I would like to thank him for all of his help and time spent.

References

[1] E. D. Bloch, *The real numbers and real analysis*, First, Springer, New York, NY, 2011.
[2] M. Kline, *Mathematical thought from ancient to modern times. Vol. 1*, Second, The Clarendon Press, Oxford University Press, New York, 1990. MR1039322