VIII REAL NUMBERS

It is a well known fact, and a standard exercise, that $\sqrt{2}$ is not rational. This means the equation $x^2 - 2 = 0$ has no solutions in the rational numbers, hence the need to extend the rational numbers to a larger set that would include the solutions to such equations.

The next set we develop is the set the real numbers which we will indicate by $\mathbb{R}$.

Dedekind Cuts and Real Numbers

Definition A **Cut** or **Dedekind cut** of the rational numbers is a subset A of the rational numbers such that

1. $A \neq \emptyset$, and $A \neq \mathbb{Q}$.
2. If $a \in A,$ and $b < a,$ then $b \in A$.
3. if $a \in A\ \exists\ a' \in A$, such that $a < a'$.

From this definition we see that a cut forms a partition of the rational numbers into two non-empty subsets, the cut and its complement, where every element of the cut is less than every element of its complement. The cut is called the lower set and its complement is called the upper set.

Definition The set of **Real Numbers**, $\mathbb{R}$, is the collection of all cuts of the rational numbers.

We define a natural ordering of the real numbers by the following.

Definition For two real numbers, A and A', we say $A < A'$ if $A \subset A'$. We emphasize the inclusion is proper, i.e., $A \neq A'$.

Theorem 8.1 For any rational number r the set $z = \{p|p < r\}$ is a cut, and hence a real number.

Proof We demonstrate that z satisfies the three conditions of the definition of a cut.

1) $r - 1 < r \Rightarrow r - 1 \in z$ Thus $z \neq \emptyset$. Also $r \not< r \Rightarrow r \notin z \Rightarrow z \neq \mathbb{Q}$.

2) If $q \in z$ and $p < q$, then $p < r$, thus $p \in z$.

3) If $q \in z$, then $q < r \Rightarrow q < \dfrac{q+r}{2} < r$, thus $\dfrac{q+r}{2} \in z$. ■

There is a natural injection of the rational numbers into the real numbers, the injection is given by

$$J : q \hookrightarrow A \text{ where } A = \{p|p < q\}.$$

We will use the notation $\hat{q}$ to represent the real number $\{p|p < q\}$, in particular the rational number 0 embeds as $J : 0 \hookrightarrow \{p|p < 0\} = \hat{0}$. Throughout the remainder of this chapter real numbers will be marked by the symbol $\hat{}$. In subsequent chapters the $\hat{}$ will be omitted, and a number will be known to be real by the context.

Exercise Show that if $r \in \mathbb{Q}$ and $\hat{r} < \hat{x}$, then $r \in \hat{x}$.

Solution $\hat{r} = \{p|p < r\} \subset \hat{x}$, thus $\exists\ t \in \hat{x}$ such that $t \notin \hat{r}$, thus $t \geq r$. If $t = r$ we are done, if $t > r$, then $r \in \hat{x}$.

Trichotomy

Lemma 8.2 *The trichotomy property for real numbers* For any real number $\hat{x}$ exactly one of the following is true:
$\hat{x} > \hat{0}, \quad \hat{x} = \hat{0},$ or $\hat{x} < \hat{0}.$

Proof Let $\hat{x}$ be a real number, then exactly one of the following is true:
$\hat{0} \subset \hat{x},\ \hat{x} = \hat{0},$ or $\hat{x} \subset \hat{0}.$ ■

Definition If $\hat{x} > 0$ then we say $\hat{x}$ is a **positive** real number. If $\hat{x} < 0$ then we say $\hat{x}$ is a **negative** real number.

Addition

We define addition of real numbers by the following:

Definition $\hat{x} + \hat{y} = \{r | r < p + q,\ p \in \hat{x},$ and $q \in \hat{y}\}.$

Theorem 8.3 The sum $\hat{x} + \hat{y}$ is a real number.

Proof We show that $\hat{x} + \hat{y}$ satisfies the definition of a cut.

1) Since $\hat{x}$ and $\hat{y}$ are not empty there exists $p \in \hat{x}$ and $q \in \hat{y}$, and $p + q - 1 < p + q \Rightarrow \hat{x} + \hat{y} \neq \emptyset$. Also since $\exists c \notin \hat{x}$ and $\exists d \notin \hat{y}$ we have $c > t\ \forall t \in \hat{x}$ and $d > w\ \forall w \in \hat{y}$. We have $c + d > t + w\ \forall t + w \in \hat{x} + \hat{y}$. Thus $c + d \notin \hat{x} + \hat{y}$, and so $\hat{x} + \hat{y} \neq \mathbb{Q}$.

2) Let $a \in \hat{x} + \hat{y}$ and $b < a$. We have $b < a < p + q$ where $p \in \hat{x}$ and $q \in \hat{y}$. Thus $b \in \hat{x} + \hat{y}$.

3) Let $a \in \hat{x} + \hat{y}$, thus $a < p + q$ where $p \in \hat{x}$ and $q \in \hat{y}$. There exists $r > p$ such that $r \in \hat{x}$, thus $p + q < r + q$. Thus $a < p + q \in \hat{x} + \hat{y}$. ■

Corollary $\hat{x} + \hat{y} = \{p + q | p \in \hat{x}, \text{ and } q \in \hat{y}\}$.

Proof From part 2) we have

$$\{p + q | p \in \hat{x}, \text{ and } q \in \hat{y}\} \subseteq \{r | r < p + q, \ p \in \hat{x}, \text{ and } q \in \hat{y}\}.$$

Now if $r < p + q$ where $p \in \hat{x}$ and $q \in \hat{y}$, then $r - p < q$, thus $r - p \in \hat{y}$ and so $r = p + (r - p)$ where $p \in \hat{x}$ and $(r - p) \in \hat{y}$, thus

$$\{r | r < p + q, \ p \in \hat{x}, \text{ and } q \in \hat{y}\} \subseteq \{p + q | p \in \hat{x}, \text{ and } q \in \hat{y}\}.$$

Thus $\hat{x} + \hat{y} = \{p + q | p \in \hat{x}, \text{ and } q \in \hat{y}\}$. ■

We leave to the reader as an exercise to show addition of real numbers is commutative and associative; i.e., $\hat{x} + \hat{y} = \hat{y} + \hat{x}$, and $\hat{x} + (\hat{y} + \hat{z}) = (\hat{x} + \hat{y}) + \hat{z}$ for all real numbers $\hat{x}, \ \hat{y}, \ \hat{z}$.

Exercises For $p, \ q \ \in \mathbb{Q}$, and $A \in \mathbb{N}$ show

i) $\hat{p} + \hat{q} = \widehat{p + q}$.

ii) $\sum_{i \in A} \hat{p}_i = \widehat{\sum_{i \in A} p_i}$.

Theorem 8.4 For any real number $\hat{x}$ and the real number $\hat{0}$, $\hat{x} + \hat{0} = \hat{x}$.

Proof: If $r \in \hat{x} + \hat{0}$, then $r = p + q$ where $p \in \hat{x}$ and $q < 0$, thus $r = p + q < p \ \Rightarrow \ r \in \hat{x}$, thus $\hat{x} + \hat{0} \subseteq \hat{x}$. If $r \in \hat{x}$, then there is a rational number $s \in \hat{x}$, such that $s > r$, thus $r - s < 0$, thus $r - s \in \hat{0}$, and $(r - s) + s = r$, thus $\hat{x} \subseteq \hat{x} + \hat{0}$. Hence $\hat{x} + \hat{0} = \hat{x}$. ■

We say $\hat{0}$ is the **additive identity**.

Definition If for two real numbers $\hat{x}$, and $\hat{y}$ we have $\hat{x} + \hat{y} = \hat{0}$, then we say $\hat{y}$ is the **additive inverse** or **opposite** of $\hat{x}$. We use the notation $-\hat{x}$ to indicate the additive opposite of $\hat{x}$.

Theorem 8.5 Every real number has an additive inverse.

Proof Let $\hat{x}$ be a real number and let $y = \{q \in \mathbb{Q} | q + p < 0 \ \forall \ p \in \hat{x}\}$. We first show that y is a real number, i.e., y is a cut.

1) Since $\hat{x} \neq \mathbb{Q} \ \exists \ d \in \mathbb{Q}$ such that $d \notin \hat{x}$. Thus $d > p \ \forall \ p \in \hat{x}$. Thus $-d < -p \ \forall \ p \in \hat{x}$. Thus $p + (-d) < 0 \ \forall \ p \in \hat{x}$. Thus $-d \in y$. Thus $y \neq \emptyset$. Also we notice for any $p \in \hat{x}$, $p + (-p) = 0$, thus $-p \notin y$, thus $y \neq \mathbb{Q}$.

2) Let $q \in y$ and $a < q$. We thus have $a + p < q + p < 0 \ \forall \ p \in \hat{x}$. Thus $a \in y$.

3) Let $q \in y$, thus $q + p < 0 \ \forall p \in \hat{x}$. Now assume $p + q + r \geq 0$ for some $p \in \hat{x}$ and $\forall r \in \mathbb{Q}^+$. Thus $p + r \notin \hat{x} \ \forall r \in \mathbb{Q}^+$. But $\forall p \in \hat{x} \ \exists s > p$ such that $s \in \hat{x}$. Let $r = s - p$, and we thus have $p + r = s \in \hat{x}$, which contradicts our assumption. Thus $\forall p \in \hat{x} \ \exists r \in \mathbb{Q}^+$ such that $q + p + r < 0$, thus $q + r \in y$, and $q < q + r$.

Thus y is a cut and we write $y = \hat{y}$.

We now show that $\hat{x} + \hat{y} = \hat{0}$. If $r \in \hat{x} + \hat{y}$, then $r = p + q < 0$, thus $\hat{x} + \hat{y} \subseteq \hat{0}$.

If $s \in \hat{0}$, and $p \in \hat{x}$ is arbitrary, then $s - p \in \mathbb{Q}$ and $p + s - p = s < 0$, thus $s - p \in \hat{y}$. Thus $s = p + s - p \in \hat{x} + \hat{y}$, and thus $\hat{0} \subseteq \hat{x} + \hat{y}$, and thus $\hat{x} + \hat{y} = \hat{0}$. ■

Lemma 8.6 $-(-\hat{x}) = \hat{x}$.

Proof We have

$$\begin{aligned}
& \hat{x} + (-\hat{x}) = \hat{0} = -(-\hat{x}) + (-\hat{x}) \\
\Rightarrow \quad & \hat{x} + (-\hat{x}) + \hat{x} = -(-\hat{x}) + (-\hat{x}) + \hat{x} \\
\Rightarrow \quad & \hat{x} = -(-\hat{x}) \quad \blacksquare
\end{aligned}$$

Lemma 8.7 $\hat{x} > \hat{0}$ if and only if $-\hat{x} < \hat{0}$.

Proof Assume $\hat{x} > \hat{0}$ then $0 \in \hat{x}$, so $\exists p \in \hat{x}$ such that $p > 0$. Now assume $-\hat{x} \geq \hat{0}$, then $\exists q \in -\hat{x}$ such that $q > -p$. Thus $q + p > 0$, and thus $\hat{x} + -\hat{x} > \hat{0}$, which is a contradiction.

Now assume $-\hat{x} < \hat{0}$, then $\exists q < 0$ such that $q > p \; \forall p \in -\hat{x}$. So $-q < -p \; \forall p \in -\hat{x}$. Thus $p + -q < 0 \;\Rightarrow\; -q \in \hat{x}$. Since we have $0 < -q$, we have $0 \in \hat{x}$, and thus $\hat{x} > \hat{0}$. ■

Corollary $-\hat{0} = \hat{0}$.

Lemma 8.8 $-(\hat{x} + \hat{y}) = -\hat{x} + (-\hat{y})$.

Proof We have $-\hat{x} + (-\hat{y}) = \{r + s | r \in -\hat{x} \text{ and } s \in -\hat{y}\}$. Thus for $r \in -\hat{x}$ and $s \in -\hat{y}$, $r + p < 0 \; \forall p \in \hat{x}$ and $s + q < 0 \; \forall q \in \hat{y}$. Thus $r+s+p+q < 0 \; \forall (p+q) \in \hat{x}+\hat{y}$. Thus $-\hat{x}+(-\hat{y}) = \{r+s | (r+s)+(p+q) < 0,\; r \in -\hat{x},\; s \in -\hat{y} \; \forall (p+q) \in (\hat{x}+\hat{y})\}$.

Now we also have $-(\hat{x}+\hat{y}) = \{t | t + (p+q) < 0 \; \forall ((p+q) \in \hat{x}+\hat{y}\}$. Since $(r+s) \in \mathbb{Q} \; \forall r \in -\hat{x}$ and $s \in -\hat{y}$ we have $(r+s) \in -(\hat{x}+\hat{y})$. Thus we have $-\hat{x} + (-\hat{y}) \subseteq -(\hat{x}+\hat{y})$.

Now let $t \in -(\hat{x}+\hat{y})$, then $t + (p+q) < 0 \; \forall p \in \hat{x}$ and $q \in \hat{y}$. Also $t + (p+q) < \dfrac{t+(p+q)}{2} < 0$. So $\dfrac{t+(p+q)}{2} - p + p < 0 \; \forall p \in \hat{x}$ and $q \in \hat{y}$. Thus $\dfrac{t+(p+q)}{2} - p \in -\hat{x}$. Also $\dfrac{t+(p+q)}{2} - q + q < 0 \; \forall p \in \hat{x}$ and $q \in \hat{y}$. Thus $\dfrac{t+(p+q)}{2} - q \in -\hat{y}$. And we have $t = \dfrac{t+(p+q)}{2} - p + \dfrac{t+(p+q)}{2} - q$. Thus $t \in -\hat{x} + (-\hat{y})$. Thus $-(\hat{x}+\hat{y}) \subset -\hat{x} + (-\hat{y})$.

Thus we have $-(\hat{x}+\hat{y}) = -\hat{x} + (-\hat{y})$. ■

Multiplication

We now define multiplication of real numbers. First we define the product of two positive real numbers by:

Definition For $\hat{x},\ \hat{y} > \hat{0}, \hat{x} \cdot \hat{y} = \{r | r < pq, p \in \hat{x}, q \in \hat{y},$ and $p > 0, q > 0\}$.

For ease of notation we will often use juxtaposition to indicate the operation of multiplication. That is $\hat{x}\hat{y} \equiv \hat{x} \cdot \hat{y}$.

Theorem 8.9 If $\hat{x}$ and $\hat{y}$ are positive real numbers, then $\hat{x}\hat{y}$ is a positive real number.

Proof We show $\hat{x}\hat{y}$ is a cut.

1) $\hat{x},\ \hat{y} > \hat{0} \Rightarrow \exists p > 0,\ q > 0,\ p \in \hat{x}$ and $q \in \hat{y}$, thus $0 < pq$, thus $0 \in \hat{x}\hat{y}$, thus $\hat{x}\hat{y} \neq \emptyset$. Now $\exists a \notin \hat{x}$ and $\exists b \notin \hat{y}$, thus $a > p\ \forall p \in \hat{x}$ and $b > q\ \forall q \in \hat{y}$, thus $ab > pq\ \forall p \in \hat{x}$ and $q \in \hat{y}$. Hence $ab \notin \hat{x}\hat{y}$. Hence $\hat{x}\hat{y} \neq \mathbb{Q}$.

2) Let $r \in \hat{x}\hat{y}$, $r < pq$ for some $p \in \hat{x}$ and $q \in \hat{y}$. If $s < r$, then $s < pq$ and thus $s \in \hat{x}\hat{y}$.

3) Let $r \in \hat{x}\hat{y}$. We have $r < pq$ for some positive $p \in \hat{x}$ and $q \in \hat{y}$. Since $\exists s \in \hat{x}$ such that $p < s$ and $\exists t \in \hat{y}$ such that $q < t$ we have $r < pq < st$, thus $pq \in \hat{x}\hat{y}$.

Since $\hat{x}\hat{y}$ satisfies the definition of a cut we conclude $\hat{x}\hat{y}$ is a real number.

To show that $\hat{x}\hat{y}$ is positive we notice that $\hat{x} > \hat{0}\ \Rightarrow \hat{0} \subset \hat{x}\ \Rightarrow 0 \in \hat{x}\ \Rightarrow \exists p > 0,\ p \in \hat{x}$. Similarly $\exists q > 0,\ q \in \hat{y}$. Now let $r \in \hat{x}$ and $r > 0$, $s \in \hat{y}$ and $s > 0$ be arbitrary. We thus have $0 < rs\ \Rightarrow 0 \in \hat{x}\hat{y}\ \Rightarrow \hat{0} \subset \hat{x}\hat{y}\ \Rightarrow \hat{x}\hat{y} > 0$.

■

We complete the definition of multiplication by:

$$\hat{x}\hat{y} = \begin{cases} \hat{0} & \text{if} \hat{x} = \hat{0} \text{ or } \hat{y} = \hat{0} \\ -(-\hat{x})\hat{y} & \text{if } \hat{x} < \hat{0} \text{ and } \hat{y} > \hat{0} \\ -(\hat{x}(-\hat{y})) & \text{if } \hat{x} > \hat{0} \text{ and } \hat{y} < \hat{0} \\ ((-\hat{x})(-\hat{y})) & \text{if } \hat{x} < \hat{0} \text{ and} \hat{y} < \hat{0} \end{cases}$$

Corollary If $\hat{x}$and $\hat{y}$ are real numbers, then $\hat{x}\hat{y}$ is a real number.

Associativity and commutativity of multiplication follows immediately from the definition of multiplication and the associativity and commutativity of rational numbers.

Exercise For $p,\ q\ \in \mathbb{Q}, A \in \mathbb{N}$ show

i) $\hat{p} \cdot \hat{q} = \widehat{p \cdot q}$.

ii) $\prod_{i \in A} \hat{p}_i = \widehat{\prod_{i \in A} p_i}$.

Theorem 8.10 The real number $\hat{1} = \{p | p < 1\}$ is the multiplicative identity.

Proof First consider a positive real number $\hat{x}$.

$$\hat{x} \cdot \hat{1} = \{r | r < pq,\ p \in \hat{x},\ q \in \hat{1},\ p > 0,\ q > 0\}.$$

If $t \in \hat{x} \cdot \hat{1}$, then $\exists p \in \hat{x},\ p > 0$ and $q \in \hat{1},\ q > 0$ such that $t < pq < p \in \hat{x}$, thus $t \in \hat{x}$. Now if $t \in \hat{x}$, then there exists $q \in \hat{x},\ q > 0$, such that $t < q$. We now note that $t < \frac{t+q}{2} < q$ and $\frac{t+q}{2q} < 1$. We thus have $t < q \cdot \frac{t+q}{2q}$, thus $t \in \hat{x} \cdot \hat{1}$. Hence $\hat{x} \cdot \hat{1} = \hat{x}$.

For $\hat{x} = \hat{0}$ we always have $\hat{0} \cdot \hat{1} = \hat{0}$.

For $\hat{x} < \hat{0}$ we have $\hat{x} \cdot \hat{1} = -((-\hat{x}) \cdot \hat{1}) = -(-\hat{x}) = \hat{x}$. ■

Theorem 8.11 $\hat{x} \neq \hat{0}$, if and only if $\exists \hat{y}$ such that $\hat{x}\hat{y} = \hat{1}$.

Proof In the converse direction we simple note that $\hat{0}\hat{y} = \hat{0}\ \forall \hat{y} \in \mathbb{R}$. Thus, if $\hat{x}\hat{y} = \hat{1}$, then neither $\hat{x}$ nor $\hat{y}$ can be $\hat{0}$.

In the forward direction, let $\hat{x} > 0$, and let
$\hat{y} = \{s | \exists\ p, q > 0, q \in \hat{x}, pq < 1 \text{ and } s < p\}$.

We first show that $\hat{y}$ is a cut.

1. $\hat{x} > \hat{0} \ \Rightarrow 0 \in \hat{x} \ \Rightarrow \ \exists q \in \hat{x}$ where $q > 0$. Since $0 \cdot q = 0 < 1\ \forall q$ we have $0 \in \hat{y}$. Thus $\hat{y} \neq \emptyset$. To show that $\hat{y} \neq \mathbb{Q}$, pick $q \in \hat{x},\ q > 0$, then $q^{-1} \cdot q = 1$, thus $q^{-1} \notin \hat{y}$.

2. If $s \in \hat{y}$ and $t < s$, then $t < p$, thus $t \in \hat{y}$.

3. If $s \in \hat{y}$, then $s < p$, thus $s < \frac{s+p}{2} < p$, thus $\frac{s+p}{2} \in \hat{y}$.

   We conclude that $\hat{y}$ is a cut and thus is a real number.

For any $s \in \hat{y}$, $q \in \hat{x}$ and $p > 0$ where $pq < 1$ we have $s < p$, thus $sq < pq < 1$. Hence $\hat{y}\hat{x} = \{r | r < sq < pq < 1,\ s, p, q > 0\} = \{r | r < 1\} = \hat{1}$.

To complete the proof, assume $\hat{x} < 0$, then $\exists \hat{y}$ such that $(-\hat{x}) \cdot \hat{y} = 1$, thus
$\hat{x} \cdot (-\hat{y}) = -\hat{x}\hat{y} = (-\hat{x}) \cdot \hat{y} = 1$. ■

The set of Real Numbers is a Field

To complete the verification that the real numbers form a field we demonstrate that multiplication distributes over addition.

Theorem 8.12 $\hat{x} \cdot (\hat{y} + \hat{z}) = \hat{x} \cdot \hat{y} + \hat{x} \cdot \hat{z}$.

To prove Theorem 8.12 we need the following lemma.

Lemma If $p \in \hat{x}$ and $q \in \hat{y}$ where $p, q > 0$, then $pq \in \hat{x}\hat{y}$.

Proof $\exists\, r \in \hat{x}$ such that $p < r$, thus $pq < rq$, thus $pq \in \hat{x}\hat{y}$ ■

Proof of Theorem 8.12

i) Assume $\hat{x},\ \hat{y} + \hat{z} > \hat{0}$, then either $\hat{y} > \hat{0}$ or $\hat{z} > \hat{0}$.

$$\hat{x} \cdot (\hat{y} + \hat{z}) = \{t | t < p \cdot s \text{ where } p \in \hat{x}, s \in \hat{y} + \hat{z} \text{ and } p, s > 0\}$$

If $\hat{y}$ and $\hat{z}$ are positive, then for $s \in (\hat{y} + \hat{z})$ we can write $s = q + r$ where $q \in \hat{y},\ r \in \hat{z}$ and $q,\ r > 0$. Thus we have

$$\hat{x} \cdot (\hat{y} + \hat{z}) = \{t | t < p \cdot s = p(q+r) = pq + pr, p, q, r > 0 \text{ with } p \in \hat{x},\ q \in \hat{y},\ r \in \hat{z}\}.$$

Now

$$\begin{aligned} \hat{x}\hat{y} + \hat{x}\hat{z} = &\quad \{t | t < u + v, u \in \hat{x}\hat{y} \text{ and } v \in \hat{x}\hat{z}\} \\ = &\quad \{t | t < pq + p'r,\ p, q, p', r > 0,\ p, p' \in \hat{x},\ q \in \hat{y},\ r \in \hat{z}\}. \end{aligned}$$

Thus $\hat{x} \cdot (\hat{y} + \hat{z}) \subseteq \hat{x}\hat{y} + \hat{x}\hat{z}$.

Now let $p, p' \in \hat{x},\ p, p' > 0$, then $pq + p'r = p(q + \frac{p'}{p}r) = p'(\frac{p}{p'}q + r)$ and either $\frac{p'}{p} \leq 1$ or $\frac{p}{p'} \leq 1$, thus either $\frac{p}{p'}q \in \hat{y}$ or $\frac{p'}{p}r \in \hat{z}$.

Thus $\hat{x}\hat{y} + \hat{x}\hat{z} \subseteq \hat{x} \cdot (\hat{y} + \hat{z})$, and thus $\hat{x}\hat{y} + \hat{x}\hat{z} = \hat{x} \cdot (\hat{y} + \hat{z})$.

Now without loss of generality, assume $\hat{y} > \hat{0}$ and $\hat{z} \leq \hat{0}$. Then we have

$$\hat{x} \cdot (\hat{y} + \hat{z}) = \{t | t < ps, p > 0, s > 0, p \in \hat{x} \text{ and } s \in \hat{y} + \hat{z}\}.$$

Now, $s = q - r$, where $q \in \hat{y}$, $-r \in \hat{z}$, $q, r > 0$. Thus

$$\hat{x} \cdot (\hat{y} + \hat{z}) = \{t | t < ps = p(q - r) = pq - pr, p, q, r > 0\}.$$

Now

$$\hat{x}\hat{y} + \hat{x}\hat{z} = \hat{x}\hat{y} - \hat{x}(-\hat{z}) = \{t | t < p - q, p \in \hat{x}\hat{y}, \text{ and } q \in \hat{x}(-\hat{z})\}.$$

We have $p = su$, $q = rv$, where $s \in \hat{x}, u \in \hat{y}, r \in \hat{x}, v \in -\hat{z}$. Thus

$$\hat{x}\hat{y} + \hat{x}\hat{z} = \hat{x}\hat{y} - \hat{x}(-\hat{z}) = \{t | t < su - rv\}.$$

Thus we again have $\hat{x} \cdot (\hat{y} + \hat{z}) \subseteq \hat{x}\hat{y} + \hat{x}\hat{z}$.

And again either $\frac{r}{s} < 1$ or $\frac{s}{r} < 1$. Thus either $\frac{s}{r}u \in \hat{y}$ or $\frac{r}{s}v \in -\hat{z}$. Thus $su - rv = s(u - \frac{r}{s}v) = r(\frac{s}{r}u - v)$, and one is in $\hat{x} \cdot (\hat{y} + \hat{z})$.

Thus $\hat{x}\hat{y} + \hat{x}\hat{z} \subseteq \hat{x} \cdot (\hat{y} + \hat{z})$, and thus $\hat{x}\hat{y} + \hat{x}\hat{z} = \hat{x} \cdot (\hat{y} + \hat{z})$.

ii) Now assume $\hat{x} > \hat{0}$, $\hat{y} + \hat{z} < \hat{0}$. Then

$$\begin{aligned} \hat{x} \cdot (\hat{y} + \hat{z}) &= -(\hat{x} \cdot (-(\hat{y} + \hat{z})) \\ &= -(\hat{x}(-\hat{y} - \hat{z})) \\ &= -(-\hat{x}\hat{y} - \hat{x}\hat{z}) = \hat{x}\hat{y} + \hat{x}\hat{z}. \end{aligned}$$

iii) Assume $\hat{x} < \hat{0}$, $\hat{y} + \hat{z} > \hat{0}$. Then

$$\begin{aligned} \hat{x} \cdot (\hat{y} + \hat{z}) &= -(-\hat{x} \cdot (\hat{y} + \hat{z})) \\ &= -(-\hat{x}\hat{y} - \hat{x}\hat{z}) = \hat{x}\hat{y} + \hat{x}\hat{z}. \end{aligned}$$

iv) Assume $\hat{x} < \hat{0}$, $\hat{y} + \hat{z} < \hat{0}$. Then

$$\begin{aligned}\hat{x} \cdot (\hat{y} + \hat{z}) = & \quad (-\hat{x} \cdot (-(\hat{y} + \hat{z}))) \\ = & \quad (-\hat{x} \cdot (-\hat{y} - \hat{z})) \\ = & \quad (-\hat{x}(-\hat{y}) - \hat{x}(-\hat{z})) \\ = & \quad -(\hat{x}(-\hat{y}) + \hat{x}(-\hat{z}) \\ = & \quad -(-(\hat{x}\hat{y} + \hat{x}\hat{z})) = \hat{x}\hat{y} + \hat{x}\hat{z}\end{aligned}$$

v) If $\hat{y} + \hat{z} = \hat{0}$, then $\hat{z} = -\hat{y}$ and we have $\hat{x} \cdot (\hat{y} + \hat{z}) = \hat{x} \cdot \hat{0} = \hat{0}$ and $\hat{x}\hat{y} + \hat{x}\hat{z} = \hat{x}\hat{y} + \hat{x}(-\hat{y}) = \hat{x}\hat{y} - \hat{x}\hat{y} = \hat{0}$.

vi) Finally, if $\hat{x} = \hat{0}$, then

$$\hat{x} \cdot (\hat{y} + \hat{z}) = \hat{0} \cdot (\hat{y} + \hat{z}) = \hat{0} = \hat{0} \cdot \hat{y} + \hat{0} \cdot \hat{z} = \hat{x}\hat{y} + \hat{x}\hat{z} \qquad \blacksquare$$

The Least Upper Bound Property

The real numbers enjoy a property that is not shared by the rational numbers, known as the least upper bound property.

Definition If X is a set of real numbers and the real number u satisfies the condition that $x \leq u \; \forall x \in X$, then u is said to be an **upper bound** for X. Equivalently if the real number l satisfies the condition that $x \geq l \; \forall x \in X$, then l is said to be a **lower bound** for X. Any set that has an upper bound is said to be bounded above, if the set has a lower bound it is said to be bounded below. If a set has both an upper bound and a lower bound, we say it is **bounded**.

Definition An upper bound, u of a set X, that satisfies the condition, if v is also upper bound, then $u \leq v$, is said to be the **supremum**, or the **least**

upper bound of X. A similar definition can be made for the **greatest lower bound** or **infimum**.

We can now state and prove the following theorem.

Theorem 8.13 *The Supremum Property* Every non-empty set of real numbers bounded above has a supremum.

Proof Let A be a non-empty collection of real numbers that is bounded above by $\hat{u}$. We will show that $\bigcup_{\hat{x}\in A}\hat{x}$ is a real number and is the supremum.

1. For any $\hat{x} \in A\ \exists p \in \hat{x} \;\Rightarrow\; p \in \bigcup_{\hat{x}\in A}\hat{x} \;\Rightarrow\; \bigcup_{\hat{x}\in A}\hat{x} \neq \emptyset$.
   $\hat{x} \leq \hat{u}\ \forall \hat{x} \in A$ and
   $\exists q \notin \hat{u} \Rightarrow q \notin \hat{x}\ \forall \hat{x} \in A \;\Rightarrow\; q \notin \bigcup_{\hat{x}\in A}\hat{x} \;\Rightarrow\; \bigcup_{\hat{x}\in A}\hat{x} \neq \mathbb{Q}$.
2. If $q < p$ where $p \in \bigcup_{\hat{x}\in A}\hat{x} \;\Rightarrow p \in \hat{x}$ for some $\hat{x} \;\Rightarrow q \in \hat{x} \;\Rightarrow q \in \bigcup_{\hat{x}\in A}\hat{x}$.
3. If $p \in \bigcup_{\hat{x}\in A}\hat{x} \;\Rightarrow p \in \hat{x}$ for some $\hat{x} \;\Rightarrow\; \exists q > p$ such that $q \in \hat{x} \;\Rightarrow\; q \in \bigcup_{\hat{x}\in A}\hat{x}$.

Thus $\bigcup_{\hat{x}\in A}\hat{x}$ is a cut and hence a real number.

Now we show that $\bigcup_{\hat{x}\in A}\hat{x}$ is the supremum. If $\hat{x} \in A$, then $\hat{x} \subset \bigcup_{\hat{x}\in A}\hat{x}$, thus $\hat{x} \leq \bigcup_{\hat{x}\in A}\hat{x}$. Hence $\bigcup_{\hat{x}\in A}\hat{x}$ is an upper bound. Now let $\hat{y} < \bigcup_{\hat{x}\in A}\hat{x} \;\Rightarrow \exists p \in \bigcup_{\hat{x}\in A}\hat{x}$ such that $p \notin \hat{y}$. Since $p \in \hat{x}$ for some $\hat{x}$ we have $\hat{y} < \hat{p} < \hat{x}$, thus $\hat{y}$ is not an upper bound. Thus if $\hat{z}$ is an upper bound, we must have $\hat{z} \geq \bigcup_{\hat{x}\in A}\hat{x}$. Thus $\bigcup_{\hat{x}\in A}\hat{x}$ is the supremum. ■

Exercise Show that $\{q \in \mathbb{Q} | q^2 < 2\}$ is bounded above in $\mathbb{Q}$, and does not have a supremum in $\mathbb{Q}$. We conclude that the rational numbers do not have the supremum property.

The Cardinality of the Real Numbers

Theorem 7.10 asserts that the integer and rational numbers are countable. We now investigate the cardinality of the real numbers.

To facilitate our investigation we will develop an alternate representation of the real numbers. We will show that every real number can be represented as the sum of integral powers of 2. However, the computation

$$\begin{aligned} x &= \sum_{i \in \omega} 2^{n-i} = 2^n + 2^{n-1} + \cdots \\ \Rightarrow \quad & 2x = 2^{n+1} + 2^n + \cdots \\ \Rightarrow \quad & x = 2x - x = 2^{n+1} \end{aligned}$$

shows that the representation need not be unique. Thus we must take care not to allow the duplications.

Definition Any function whose domain is an ordinal number is called a **sequence**. If the domain is the ordinal number α we say the sequence is an α-sequence, if the image of a sequence is in a set a, we say that the sequence is an a-valued α-sequence. We use the notation (s_n) to represent the sequence $s : \alpha \to s(\alpha)$ where $n \in \alpha$.

We begin with some terminology.

1. A sequence k_n is **decreasing** if $k_n < k_m$ whenever $n > m$.

2. Let k_n be a decreasing sequence of integers. We say k_n is **inessential** if there exists $N \in \mathbb{N}$ such that $k_{n+1} = k_n - 1\ \forall n \geq N$. We say k_n is **essential** if it is not inessential.

3. We will say any rational number of the form $2^k,\ k \in \mathbb{Z}$ is a **binary**.

Consider the set of all binary-valued sequences on $\alpha \subseteq \omega$ of the form $s_n = 2^{k_n}$ where k_n is an essential decreasing integer-valued sequence, i.e.,
$B = \{(2^{k_n})|(k_n)$ is an essential decreasing integer-valued sequence$\}$.

We will construct a bijection, b, between B and the positive real numbers, i.e. we construct $b : \mathbb{R}^+ \leftrightarrow B$. If $b(\hat{x}) = (2^{k_n})$, we will say (2^{k_n}) is the binary representation of $\hat{x}$.

We construct b by demonstrating how to compute the image of $\hat{x} \in \mathbb{R}^+$.

$$\hat{x} > \hat{0} \ \Rightarrow\ 0 \in \hat{x} \ \Rightarrow\ \exists p > 0,\ p \in \hat{x}.$$

Thus

$$\exists k \in \mathbb{Z} \text{ such that } 2^k < p.$$

Now

$$\exists q \notin \hat{x} \text{ and } \exists m \text{ such that } 2^{k+m} \geq q.$$

Thus

$$\exists n \text{ such that } \hat{2}^{k+n} > \hat{x}.$$

Consider $\{m|\hat{2}^{k+m} > \hat{x}\} \subseteq \omega$. Pick the least element,n, thus $\hat{2}^{k+n} > \hat{x}$ and $\hat{2}^{k+n-1} \leq \hat{x}$, thus 2^{k+n-1} is the largest element of the form 2^m in $\hat{x}$. Set $k + n - 1 = k_0$.

Now consider $\hat{x} - \hat{2}^{k_0}$. There exists a largest element of the form 2^m in $\hat{x} - \hat{2}^{k_0}$, call that element 2^{k_1}.

We show $2^{k_1} < 2^{k_0}$.

$$\hat{2}^{k_1} \leq \hat{x} - \hat{2}^{k_0} \Rightarrow \hat{2}^{k_1} + \hat{2}^{k_0} \leq \hat{x}$$

If $2^{k_0} \leq 2^{k_1}$, then we have

$$\hat{2}^{k_0} + \hat{2}^{k_0} \leq \hat{2}^{k_1} + \hat{2}^{k_0} < \hat{x}.$$

Thus

$$\hat{2}^{k_0+1} = \hat{2} \cdot \hat{2}^{k_0} < \hat{x}.$$

Since 2^{k_0} is the largest binary in $\hat{x}$ we have a contradiction, thus $2^{k_1} < 2^{k_0}$.

We pick 2^{k_2} to be the largest binary in $\hat{x} - \hat{2}^{k_0} - \hat{2}^{k_1} = \hat{x} - (\hat{2}^{k_1} + \hat{2}^{k_1})$. Again $2^{k_2} < 2^{k_1}$. We continue in this fashion to construct the sequence. This construction process defines our map b. We now need to show that b is well defined, one to one and onto.

To demonstrate that b is well defined we need only show that the maximal binary in any real number is unique. If 2^m and 2^n are maximal binaries in $\hat{x}$, then $2^m = 2^n \Rightarrow m = n$. Thus the maximal binary is unique and b is well defined.

To show that b is onto, we need to define some notation and prove a lemma.

Let (a_n) be an α-sequence, where $\alpha \subseteq \omega$.

Let $\sum_{k \in n} a_k = a_0 + a_1 + \cdots + a_n$ for $n \in \alpha$. Then we have $\left(\sum_{k \in n} a_k\right)$ is an α-sequence. Which we call the **sequence of partial sums** of (a_n).

Now let (a_n) be an α-sequence of non-negative rational numbers, $\alpha \subset \omega$. Each element of $\left(\sum_{k \in n} a_k\right)$ is a rational number since each sum is finite. Also $\sum_{k \in n} a_k \leq \sum_{k \in m} a_k$ if $n < m$, since each $a_i \geq 0$.

If the associated sequence of real numbers $\left(\widehat{\sum_{k\in n} a_k}\right)$ is bounded above, then we define

$$\widehat{\sum_{n\in\alpha} a_n} = sup\Big\{\widehat{\sum_{k\in n} a_n}\Big\}.$$

Lemma If $(a_n) = (2^{k_n})$ where $k_n \in \mathbb{Z}$, $n \in \alpha \subset \omega$ and $k_n < k_m$ if $n > m$, then $\left(\widehat{\sum_{i\in n} 2^{k_i}}\right)$ is bounded above.

Proof

$$\sum_{i\in n} 2^{k_i} \leq \sum_{i\in n} 2^{k_0-i} \leq \sum_{i\in\omega} 2^{k_0-i} = 2^{k_0+1}$$

Thus

$$\sum_{i\in n} 2^{k_i} < 2^{k_0+1}\ \forall n \in \alpha \Rightarrow \widehat{\sum_{i\in n} 2^{k_i}} \leq \widehat{2^{k_0+1}}\ \forall n \in \alpha$$

Thus $\left(\widehat{\sum_{i\in n} 2^{k_i}}\right)$ is bounded above. ■

Now let (2^{k_n}) be a sequence where (k_n) is a decreasing essential sequence of integers. Since k_n is essential $\sum_{n\in\mathbb{N}-\{0\}} 2^{k_{m+n}} < 2^{k_m}\ \forall m \in \mathbb{N}$. Thus we see that (2^{k_n}) is the binary representation of the real number $\widehat{\sum 2^{k_n}}$.

To show that b is one to one, if $b(\hat{x}) = b(\hat{y})$, then $\{2^{k_n}\} = \{2^{j_n}\}$ only if $2^{k_n} = 2^{j_n}\ \forall n$.

Theorem 8.14 The real numbers are uncountable.

To prove this theorem we need two lemmas and a corollary.

Lemma 1 The set of all bi-valued ω-sequences is uncountable.
That is $S = \{s : \omega \to \{0, 1\}\}$ is uncountable.

Proof The demonstration is by contradiction.

Assume there exists a bijection $b : \omega \to S$. Define a bi-valued ω-sequence s by

$$s(n) = \begin{cases} 0 & \text{if } \big(b(n)\big)(n) = 1 \\ 1 & \text{if } \big(b(n)\big)(n) = 0. \end{cases}$$

Since b is a bijection, $\exists\ k$ where $b(k) = s$. Then we have

$$s(k) = \begin{cases} 0 & \text{if } \big(b(k)\big)(k) = s(k) = 1 \\ 1 & \text{if } \big(b(k)\big)(k) = s(k) = 0 \end{cases}$$

which is a contradiction. ■

Lemma 2 The set of all bi-valued ω-sequences where $s(k) = 0$ for only a finite number of times is countable.
That is, $A = \{s | \exists N \in \omega \text{ such that } s(n) = 1\ \forall n \geq N\}$ is countable.

Proof There is a reasonably obvious bijective map
$j : A \leftrightarrow \bigcup_{n\in\omega} \{s : n \to \{0,1\} | n \in \omega\}$.
Thus $C(A) \leq C\left(\bigcup_{n\in\omega} \{s : n \to \{0,1\} | n \in \omega\}\right)$, and the countable union of finite sets is countable. ■

Corollary The set of all bi-valued ω-sequences where $s(k) = 0$ infinitely often is uncountable.

Proof of Thoerem 8.14

Let $A = \{s : \omega \to \{0,1\}, \text{ where } s_n = 0 \text{ infinitely often}\}$. There exists a bijection

$$b : A \leftrightarrow \left\{ \sum_{n\in\omega} \widehat{s_n \cdot 2^{-n}} | s \in A \right\} \subset \mathbb{R}$$

defined by $b(s) = \sum_{n\in\omega} \widehat{s_n \cdot 2^{-n}}$. Since A is uncountable, so is $\mathbb{R}$. ■

Exercise

Show that $\{s : \omega \to \{0,1\}$, where $s_n = 0$ infinitely often$\} = \{x | 0 \leq x \leq 1\}$.

The Cauchy Sequence Construction of the Real Numbers

We conclude the chapter with a set of exercises that leads to an alternate construction of the real numbers.

Definition The functions $Abs : \mathbb{R} \to \mathbb{R}$ defined by

$$Abs(x) = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

is the **absolute value function**. We abbreviate $Abs(x)$ by $|x|$,
i.e. $Abs(x) = |x|$.

Definition A rational-valued sequence, s_n, that satisfies the following:

$$\forall \epsilon > 0, \epsilon \in \mathbb{Q},\ \exists N \in \mathbb{N} \text{ such that } \forall n, m > N \Rightarrow |s_n - s_m| < \epsilon$$

is called a **Cauchy Sequence**.

We define an equivalence relation on the set of all rational-valued Cauchy Sequences by

$$s_n \equiv t_n \text{ iff } \forall \epsilon > 0\ \exists N \in \mathbb{N} \text{ such that } \forall n \geq N \Rightarrow |s_n - t_n| < \epsilon.$$

We define an order on the equivalence classes of Cauchy Sequences by

$$S \geq T \text{ iff } \exists N \in \mathbb{N} \text{ such that } \forall n > N \Rightarrow s_n - t_n \geq 0\ \forall (s_n) \in S \text{ and } \forall (t_n) \in T.$$

Exercises

1. Show that the relation as defined above is in an equivalence relation.
2. Show that the order defined for the equivalence classes of Cauchy Sequences is a linear order.
3. Show that the set of equivalence classes of rational-valued Cauchy sequences is order isomorphic to the Real Numbers.