The Construction of Real Number System with Dedekind Cuts

Jinxin Wang

1 Abstract

We are going to construct the real number set $\mathbb{R}$ from the rational number set $\mathbb{Q}$ using the Dedekind cuts.

2 Ordered Set and Upper/Lower Bound

Next we need to define the order of elements in a set in a general way. For the number sets that we are already familiar with, such as $\mathbb{N}$ or $\mathbb{Q}$, the order of their elements seems natural. However, as we shall see, the concept of order is abstract in nature. Depending on the operation an order relies, we can define different orders on the same set.

Definition 2.1 (Order)**.** *Let S be a set. An order on S is a relation, denoted by $<$, with the following two properties:*

- *$\forall x, y \in S$, one and only one of the statements is true:*

$$x < y, x = y, y < x$$

- *$\forall x, y, z \in S$, if $x < y$ and $y < z$, then $x < z$.*

Definition 2.2 (Ordered Set)**.** *An ordered set is a set S in which an order is defined.*

Therefore, we can define an order in $\mathbb{Q}$ in the following way based on the addition operation on $\mathbb{Q}$: $\forall x, y \in \mathbb{Q}$, if $x + (-y) < 0$, then $x < y$. In this way, $\mathbb{Q}$ is an ordered set.

With the definition of order and ordered set, we can define upper/lower bound, as well as the least upper bound and the greatest lower bound.

Definition 2.3 (Upper/Lower Bound)**.** *Let S be an ordered set, and a set $E \subset S$. If there exists an $\alpha \in S$ such that $x \leq \alpha$ for every $x \in E$, we say that E is bounded above, and call α an upper bound of E. If there exists a $\beta \in S$ such that $x \geq \beta$ for every $x \in E$, we say that E is bounded below, and β is a lower bound of E.*

Definition 2.4 (Least Upper Bound and Greatest Lower Bound)**.** *Let S be an ordered set, and a set $E \subset S$, and E is bounded above. Suppose that there exists an $\alpha \in S$ with the following properties:*

- *α is an upper bound of E.*
- *$\forall \beta \in S$ and $\beta < \alpha$, β is not an upper bound of E.*

then we say that α is the least upper bound of E, or the supremum of E.

Similarly, a set $E \subset S$, and E is bounded below. Suppose that there exists an $\beta \in S$ with the following properties:

- *β is a lower bound of E.*
- *$\forall \alpha \in S$ and $\beta < \alpha$, α is not a lower bound of E.*

then we say that β is the greatest lower bound of E, or the infimum of E.

3 Number Field and Ordered Field

We need to introduce the concept of a field, which is a kind of algebraic structure. A field specifies the valid way to do the four basic arithmetic operation with its elements, and get the result which still belongs to the field. This complies with our common sense of $\mathbb{Q}$ and $\mathbb{R}$.

Definition 3.1 (Field)**.** *A field F is a set with two binary operations defined on it, namely addition and multiplication. The addition and multiplication should satisfy the following properties:*

- *For addition*
  - *Closed: $\forall x, y \in F$, $x + y \in F$.*
  - *Associative: $\forall x, y, z \in F$, $(x + y) + z = x + (y + z)$.*
  - *Identity element: $\exists 0 \in F$, $\forall x \in F$, $0 + x = x + 0 = x$.*
  - *Inverse element: $\forall x \in F$, $\exists y \in F$, $x + y = y + x = 0$.*
  - *Commutative: $\forall x, y \in F$, $x + y = y + x$.*
- *For multiplication*
  - *Closed: $\forall x, y \in F$, $xy \in F$.*
  - *Associative: $\forall x, y, z \in F$, $(xy)z = x(yz)$.*
  - *Identity element: $\exists 1 \in F$, $\forall x \in F$, $1x = x1 = x$.*
  - *Inverse element: $\forall x \in F \setminus \{0\}$, $\exists \frac{1}{x} \in F$ such that*

$$x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$$

  - *Commutative: $\forall x, y \in F$, $x \cdot y = y \cdot x$*

- *For mixed operation:*
  - *Distributive:* $\forall x, y, z \in F,\ x(y+z) = xy + xz$

For the purpose of this essay, we focus on fields whose elements are numbers, or number fields.

It is obvious that $\mathbb{Q}$ is a field. (TODO: prove that $\mathbb{Q}$ is a field)

Since a field is a set, it is natural to think about bringing the concept of order to a field, which leads to the definition of an ordered field.

Definition 3.2 (Ordered Field)**.** *An ordered field is a field F that has an order defined in it, which satisfies:*

- *If $x, y, z \in F$ and $y < z$, then $x + y < x + z$.*
- *If $x, y \in F$ and $x > 0$ and $y > 0$, then $xy > 0$.*

Proposition 3.1. *The following statements are true in every ordered field:*

(1) If $x > 0$, then $-x < 0$, and vice versa.

(2) If $x > 0$ and $y < z$, then $xy < xz$.

(3) If $x < 0$ and $y < z$, then $xy > xz$.

(4) If $x \neq 0$, then $x^2 > 0$. In particular, $1 > 0$.

(5) If $0 < x < y$, then $0 < \frac{1}{y} < \frac{1}{x}$.

Proof. **(1)** If $x > 0$, then $-x + x > -x + 0$, $0 > -x$, $-x < 0$. If $-x < 0$, then $x + (-x) < x + 0$, $0 < x$, $x > 0$.

(2) Since $y < z$, then $-y + y < -y + z$, $0 < z - y$. Hence $x(z - y) > 0$, $xz - xy > 0$, $xz - xy + xy > 0 + xy$ $xz > xy$.

□

4 Archimedean Property

We can discuss the Archimedean property on some number groups with an order and the multiplication operation defined in it, such as $\mathbb{Z}$ or $\mathbb{Q}$. It is stated as follows:

Theorem 4.1. *If $x \in S$, $y \in S$, and $x > 0$, then there is a positive integer n such that*

$$nx > y$$

Proposition 4.1. *$\mathbb{Q}$ has the archimedean property.*

Proof. For every $y \in \mathbb{Q}$ that $y \leq 0$, let $n = 1$, then

$$nx = x > 0 \geq y$$

For every $y \in \mathbb{Q}$ that $y > 0$, $\exists a_1, b_1 \in \mathbb{N}^+$ and $(a_1, b_1) = 1$ such that $y = \frac{a_1}{b_1}$. Similarly, $\exists a_2, b_2 \in \mathbb{N}^+$ such that $x = \frac{a_2}{b_2}$. Let $n = [\frac{a_1}{b_1} \cdot \frac{b_2}{a_2}] + 1$, then

$$\begin{aligned} nx &> \frac{a_1}{b_1} \cdot \frac{b_2}{a_2} x \\ &= \frac{a_1}{b_1} \cdot \frac{b_2}{a_2} \cdot \frac{a_2}{b_2} \\ &= \frac{a_1}{b_1} \\ &= y \end{aligned}$$

□

5 Real Number Set Defined with Dedekind Cuts

5.1 Specify the Members of the Real Number Set

Definition 5.1. *A Dedekind cut on $\mathbb{Q}$ is any set $\alpha \subset \mathbb{Q}$ with the following three properties:*

(I) α is not empty, and $\alpha \neq \mathbb{Q}$.

(II) If $p \in \alpha$, $q \in \mathbb{Q}$, and $q < p$, then $q \in \alpha$.

(III) If $p \in \alpha$, then $\exists r \in \alpha$ such that $p < r$.

Remark 5.1. 1 *For a Dedekind cut, a rational number q either belongs to it or not so.*

2 *For a Dedekind cut α, if $q \in \mathbb{Q}$ and $q \notin \alpha$, then $\forall p \in \alpha$, $p < q$. This is the contraposition of the property (II).*

3 *For a Dedekind cut α, if $q \notin \alpha$ and $p > q$, then $p \notin \alpha$. The reason is that $\forall r \in \alpha$, $p > q > r$.*

4 *For a Dedekind cut α, the distance between $p \in \alpha$ and $q \notin \alpha$ can be smaller than any positive rational number. We can prove it by constructing a series of p and q with gradually smaller distance. Since α is not empty and not $\mathbb{Q}$, there exists $p \in \alpha$ and $q \notin \alpha$, with their distance $d(p, q) = q - p > 0$. Next we check the rational number $\frac{p+q}{2}$. If $\frac{p+q}{2} \in \alpha$, we replace p with $\frac{p+q}{2}$; otherwise, we replace q with $\frac{p+q}{2}$. We repeat this process of checking the arithmetic average and replacing p or q endlessly. Notice that with each iteration, the distance becomes a half of the previous one. Therefore, it can be anyhow small.*

5 *The property (III) tells us there is no maximum in a Dedekind cut.*

We define every member of the real number set $\mathbb{R}$ is a Dedekind cut on $\mathbb{Q}$.

5.2 Specify the Order in the Real Number Set

Definition 5.2. *$\forall \alpha, \beta \in \mathbb{R}$, $\alpha < \beta$ is true if and only if α is a property subset of β.*

We need to prove that the above definition is a valid order in a set.

Proof. First, we need to prove that for any $\alpha, \beta \in \mathbb{R}$, only one of the following three relations holds:

$$\alpha < \beta, \alpha = \beta, \alpha > \beta$$

α cannot be both a subset of β and not a subset of β, and vice versa. Therefore, at most one of the above relations holds.

Then we need to prove at least one of the above relations holds. Suppose the first two relations is false, then $\exists p \in \alpha$ such that $p \notin \beta$, which means $\forall q \in \beta$, $q < p$ (the reason why not $q \leq p$ is that if $\exists q \in \beta$ such that $q = p$, then $\exists r \in \beta$ such that $r > q = p$, then $p \in \beta$ which is contradictory to our condition). Hence $\forall q \in \beta$, $q \in \alpha$. Therefore β is a subset of α, i.e. $\beta < \alpha$.

Since a proper subset of a proper subset is still a proper subset, it is obvious that if $\alpha < \beta$, $\beta < \gamma$, then $\alpha < \gamma$. □

Now $\mathbb{R}$ is an ordered set.

5.3 Prove the Real Number Set Has the Least-Upper-Bound Property

We claim that the real numbet set $\mathbb{R}$ defined as above has the least-upper-bound property.

Proof. Let A be a nonempty subset of $\mathbb{R}$, and $\beta \in \mathbb{R}$ be an upper bound of A. Define γ to be the union of all $\alpha \in A$. We shall prove that $\gamma \in \mathbb{R}$ and $\gamma = \sup A$.

First, we need to prove $\gamma \in \mathbb{R}$.

(I) Since A is nonempty, A contains at least one element $\alpha_0 \in \mathbb{R}$. α_0 is nonempty subset of $\mathbb{Q}$, hence γ is a nonempty subset of $\mathbb{Q}$. Since $\alpha < \beta$ or $\alpha \subset \beta$ for every $\alpha \in A$, then $\gamma \subset \beta$, hence $\gamma \neq \mathbb{Q}$.

(II) Given $p \in \gamma$, p belongs to at least one element of A, let's say α_0, which is a Dedekind cut on $\mathbb{Q}$. Since $p \in \alpha_0$, $q < p$, then $q \in \alpha_0$. Hence $q \in \gamma$.

(III) Given $p \in \gamma$, p belongs to at least one element of A, let's say α_0, which is a Dedekind cut on $\mathbb{Q}$. Since $p \in \alpha_0$, then $\exists r \in \alpha_0$ such that $p < r$. Therefore, $r \in \gamma$ such that $p < r$.

Next, we need to prove γ is an upper bound of A. Since $\gamma = \bigcup_{\alpha \in A} \alpha$, $\forall \alpha \in A$, $\alpha \subset \gamma$, i.e. $\alpha \leq \gamma$.

Last, we need to prove any $\delta \in \mathbb{R}$ such that $\delta < \gamma$ is not an upper bound of A. $\delta < \gamma$ means that $\exists p \in \gamma$ and $p \notin \delta$. p belongs to at least one element of A, let's say α_0. Therefore $p \in \alpha_0$ and $p \notin \delta$. Therefore, $\delta < \alpha_0$.

Overall, it is proved that $\gamma = \sup A$. □

5.4 Define the Addition Operation on the Real Number Set

For any $\alpha \in \mathbb{R}$ and $\beta \in \mathbb{R}$, we define $\alpha + \beta$ as the set of all sums $r + s$, where $r \in \alpha$ and $s \in \beta$. Besides, we define the identity element 0^* (to differentiate it from the rational number 0) of the addition operation on $\mathbb{R}$ as the set of all negative rational numbers. We shall prove that it holds all properties required for the addition operation of a field.

Proof. First we need to prove that the addition operation is closed in $\mathbb{R}$. In other words, the result of the addition of two Dedekind cuts is also a Dedekind cut.

- Since α and β are both nonempty subset of $\mathbb{Q}$, $\alpha + \beta$ is also nonempty. Pick $r' \notin \alpha$, and $s' \notin \beta$. Hence $\forall r \in \alpha$, $r' > r$, and $\forall s \in \beta$, $s' > s$. Therefore $\forall r \in \alpha$, $\forall s \in \beta$, $r' + s' > r + s$, which means $r' + s' \notin (\alpha + \beta)$. Hence $\alpha + \beta \neq \mathbb{Q}$.
- If $q \in \mathbb{Q}$ and $\exists p \in (\alpha + \beta)$ such that $q > p$, $p = r + s > q$ for $r \in \alpha$ and $s \in \beta$. Let $s' = q - r < s$, which follows that $s' \in \beta$. Hence $q = r + s'$ where $r \in \alpha$ and $s' \in \beta$. Therefore, $q \in (\alpha + \beta)$.
- $\forall p \in (\alpha + \beta)$, $p = r + s$ for $r \in \alpha$ and $s \in \beta$. Therefore, $\exists r' \in \alpha$ such that $r' > r$, and $\exists s' \in \beta$ such that $s' > s$. Hence $p' = r' + s' > p$ and $p' \in (\alpha + \beta)$.

It is proved that $\forall x \in \mathbb{R}$ and $\forall y \in \mathbb{R}$, $x + y \in \mathbb{R}$.

Then we need to prove that the addition operation satisfies the associative property. For $\alpha, \beta, \gamma \in \mathbb{R}$, $\alpha + \beta$ is the set of all $r + s$, with $r \in \alpha$, $s \in \beta$. Then $(\alpha + \beta) + \gamma$ is the set of all $(r + s) + t$, with $r \in \alpha$, $s \in \beta$, $t \in \gamma$. By the same definition, $\alpha+(\beta+\gamma)$ is the set of all $r+(s+t)$, with $r \in \alpha$, $s \in \beta$, $t \in \gamma$. Since the addition operation in $\mathbb{Q}$ satisfies the associative property, $(r+s)+t = r+(s+t)$ for all choices of $r \in \alpha$, $s \in \beta$, $t \in \gamma$. Therefore, $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

Similarly, we can prove that the addition operation satisfies the commutative property. For $\alpha, \beta \in \mathbb{R}$, $\alpha + \beta$ is the set of all $r + s$, with $r \in \alpha$, $s \in \beta$. By the same definition, $\beta + \alpha$ is the set of all $s + r$, with $r \in \alpha$, $s \in \beta$. Since the addition operation in $\mathbb{Q}$ satisfies the commutative property, $r + s = s + r$ for all choices of $r \in \alpha$, $s \in \beta$. Therefore, $\alpha + \beta = \beta + \alpha$.

Next we prove that 0^* we defined serves as an identity element in the addition operation in $\mathbb{R}$.

- It is clear that 0^* is not empty and not equal to $\mathbb{Q}$. Any rational number smaller than a negative one is also negative. $\forall r \in 0^*$, which means $r < 0$, $\frac{r}{2} < 0$ and $\frac{r}{2} > r$. Therefore, $0^* \in \mathbb{R}$.
- Given $\alpha \in \mathbb{R}$, $\forall r \in \alpha$ and $\forall s \in 0^*$, $r + s < r$, which means $(r + s) \in \alpha$. Hence $\alpha + 0^* \subset \alpha$. Conversely, $\forall r \in \alpha$, $\exists r' \in \alpha$ such that $r' > r$. Then $r = r' + (r - r')$ where $r' \in \alpha$ and $r - r' < 0$ and thus $(r - r') \in 0^*$. Hence $\alpha \subset (\alpha + 0^*)$. Therefore, $\alpha + 0^* = \alpha$.

Finally, we shall prove that every element $\alpha \in \mathbb{R}$ has an inverse element $-\alpha \in \mathbb{R}$ such that $\alpha + (-\alpha) = 0^*$. We define $-\alpha$ as the set of all rational numbers p with the following properties: there exists $r > 0$ such that $-p-r \notin \alpha$. In other words, all rational numbers with some rational numbers smaller than its negative that fails to be in α. Let's first prove that $-\alpha \in \mathbb{R}$.

- Since $\alpha \neq \mathbb{Q}$, $\exists s \notin \alpha$. Let $p = -s - 1$, then $-p - 1 = s \notin \alpha$. Hence $p \in -\alpha$. $-\alpha$ is not empty. Since α is not empty, $\exists s' \in \alpha$. Let $p' = -s'$, then $\forall r > 0$, $-p' - r < s'$ and thus $-p' - r \in \alpha$. Hence $p' \notin -\alpha$. $-\alpha \neq \mathbb{Q}$.
- For $p \in (-\alpha)$, $\exists r > 0$ such that $-p - r \notin \alpha$, which means $-p - r > s$ for all $s \in \alpha$. If $q \in \mathbb{Q}$ and $q < p$, then $-q - r > -p - r$. Hence $-q - r \notin \alpha$, which follows that $q \in (-\alpha)$.
- For $p \in (-\alpha)$, $\exists r > 0$ such that $-p - r \notin \alpha$. Let $p' = p + \frac{r}{2} > p$, then $-p' - \frac{r}{2} = -p - r \notin \alpha$. Hence $p' \in (-\alpha)$.

Following that, we prove that $\alpha + (-\alpha) = 0^*$.

- For $p \in (-\alpha)$, $\exists r > 0$ such that $-p - r \notin \alpha$, which means $-p - r > q$ for all $q \in \alpha$. Hence for all choices of $p \in (-\alpha)$ and $q \in \alpha$, $\exists r > 0$ such that $p + q < -r < 0$. Therefore, $\alpha + (-\alpha) \subset 0^*$.
- For any negative rational number s, put $s' = -\frac{s}{2} > 0$. Based on the archimedean property of $\mathbb{Q}$, there exists an integer n such that $ns' \in \alpha$ but $(n+1)s' \notin \alpha$. Let $p = -(n+2)s'$, then $-p - s' = (n+1)s' \notin \alpha$, and thus $p \in (-\alpha)$. Besides, $ns' + p = -2s' = s$. Therefore, $0^* \subset (\alpha + (-\alpha))$.

We conclude that $\alpha + (-\alpha) = 0^*$. □

Remark 5.2. *The above proof of the existence of the inverse element of the addition operation relies on the archimedean property of* $\mathbb{Q}$.

5.5 Define the Multiplication Operation on the Positive Real Number Set

We first define the multiplication operation in $\mathbb{R}^+$, the set of all $\alpha \in \mathbb{R}$ such that $\alpha > 0^*$.

If $\alpha, \beta \in \mathbb{R}^+$, we define $\alpha\beta$ as the set of all $p \in \mathbb{Q}$ such that $p < rs$ for some choice of $r \in \alpha$, $s \in \beta$, $r > 0$, $s > 0$. As for the identity element 1^* (to differentiate it from the rational number 1) of the multiplication operation, we define it as the set of all $p \in \mathbb{Q}$ such that $p < 1$. We shall prove that it holds all properties required for the multiplication operation of a field.

Proof. First we need to prove that the multiplication operation is closed in $\mathbb{R}^+$, i.e. if $\alpha \in \mathbb{R}^+$, $\beta \in \mathbb{R}^+$, then $\alpha\beta \in \mathbb{R}^+$.

- Since $\alpha > 0^*$, $\beta > 0^*$, there exists $r \in \alpha$ and $s \in \beta$ such that $r > 0$ and $s > 0$. Hence $rs > \frac{rs}{2} > 0$, and $\frac{rs}{2} \in \alpha\beta$. Therefore, $\alpha\beta$ is not empty and $\alpha\beta > 0^*$. Pick $r' \notin \alpha$, and $s' \notin \beta$. Hence $\forall r \in \alpha$, $r' > r$, and $\forall s \in \beta$, $s' > s$. Therefore $\forall r \in \alpha$ such that $r > 0$, $\forall s \in \beta$ such that $s > 0$, $r's' > rs$, which means $r's' \notin \alpha\beta$. Hence $\alpha\beta \neq \mathbb{Q}$.

- If $p \in \alpha\beta$, there exists some choice of $r \in \alpha \wedge r > 0$ and $s \in \beta \wedge s > 0$ such that $p < rs$. If $q < p$, then $q < rs$. Hence $q \in \alpha\beta$.

- If $p \in \alpha\beta$, there exists some choice of $r \in \alpha \wedge r > 0$ and $s \in \beta \wedge s > 0$ such that $p < rs$. Consider $q = \frac{p+rs}{2}$. It is clear that $q \in \mathbb{Q}$, $q > p$, $q < rs$ and thus $q \in \alpha\beta$.

Therefore, $\alpha\beta$ is a Dedekind cut on $\mathbb{Q}$ and $\alpha\beta > 0^*$.

Next, we will show that the multiplication operation in $\mathbb{R}^+$ has the associative property. $\forall p \in (\alpha\beta)\gamma$, $p < qt$ for some $q \in \alpha\beta \wedge q > 0$ and $t \in \gamma \wedge t > 0$, where $q < rs$ for some $r \in \alpha \wedge r > 0$ and $s \in \beta \wedge s > 0$. Hence $p < rst$, $p < \frac{p+rst}{2} < rst$. Then $\frac{p+rst}{2r} < st$, which means $\frac{p+rst}{2r} \in \beta\gamma$. Thus $p < r\frac{p+rst}{2r}$ where $r \in \alpha$ and $\frac{p+rst}{2r} \in \beta\gamma$, which follows that $p \in \alpha(\beta\gamma)$. Therefore, $(\alpha\beta)\gamma \subset \alpha(\beta\gamma)$. Conversely, we can prove that $\alpha(\beta\gamma) \subset (\alpha\beta)\gamma$ with the same approach. Therefore, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

What comes next is the commutative property. $\forall p \in \alpha\beta$, $p < rs$ for some $r \in \alpha \wedge r > 0$ and $s \in \beta \wedge s > 0$. Thus $p < sr$, which follows that $p \in \beta\alpha$. Hence $\alpha\beta \subset \beta\alpha$. Conversely, we can prove that $\beta\alpha \subset \alpha\beta$ with the same approach. Therefore, $\alpha\beta = \beta\alpha$.

Then we prove that 1^* we defined serves as the identity element in the multiplication operation in $\mathbb{R}^+$.

- It is clear that 1^* is not empty and is not equal to $\mathbb{Q}$, and $0^* \subsetneq 1^*$. If $p \in 1^*$ and $q < p$, then $q < p < 1$, which follows that $q \in 1^*$. $\forall p \in 1^*$, $p < 1$, then $\exists r = \frac{p+1}{2}$ such that $p < r < 1$ and thus $r \in 1^*$. Therefore, $1^* \in \mathbb{R}^+$.

- Given $\alpha \in \mathbb{R}^+$, $\forall p \in \alpha \cdot 1^*$, $p < qr$ where $q \in \alpha \wedge q > 0$ and $r \in 1^* \wedge r > 0$. Thus $0 < r < 1$, which follows that $p = qr < q$. Hence $p \in \alpha$. Therefore, $\alpha \cdot 1^* \subset \alpha$. On the other hand, $\forall p \in \alpha$, $\exists q, r \in \alpha$ such that $q > 0$ and $p < q < r$. Hence $p < q = r \cdot \frac{q}{r}$ where $0 < \frac{q}{r} < 1$ and thus $\frac{q}{r} \in 1^*$. Therefore, $\alpha \subset \alpha \cdot 1^*$. So we can conclude that $\alpha = \alpha \cdot 1^*$.

Finally, we shall prove that every element $\alpha \in \mathbb{R}^+$ has an inverse element $\beta \in \mathbb{R}^+$ such that $\alpha\beta = 1^*$. We define β as the set of all rational numbers p with the following properties: there exists $r > 0$ such that $\frac{1}{p+r} \notin \alpha$. Let's first prove that $\beta \in \mathbb{R}^+$:

- Since $\alpha \neq \mathbb{Q}$, $\exists p \notin \alpha$. Let $q = \frac{1}{p} - 1$, then $\frac{1}{q+1} = p \notin \alpha$, which follows that $q \in \beta$. Hence β is not empty. Since $\alpha > 0^*$, $\exists s \in \alpha \wedge s > 0$. Let $t = \frac{1}{s} > 0$, then $\forall r > 0$, $t + r > t > 0$, $0 < \frac{1}{t+r} < \frac{1}{t} < s$, and thus $t + r \in \alpha$. Hence $\beta \neq \mathbb{Q}$.

- If $p \in \beta$, $\exists r > 0$ such that $\forall s \in \alpha$, $\frac{1}{p+r} > s$. If $q < p$, let $r' = r + p - q > 0$, and then $\forall s \in \alpha$, $\frac{1}{q+r'} = \frac{1}{p+r} > s$. Hence $q \in \beta$.
- If $p \in \beta$, $\exists r > 0$ such that $\forall s \in \alpha$, $\frac{1}{p+r} > s$. Let $q = p + \frac{r}{2} > p$, and then $\forall s \in \alpha$, $\frac{1}{q+\frac{r}{2}} = \frac{1}{p+r} > s$. Hence $q \in \beta$.
- Pick $p \notin \alpha$ and $p > 0$. Then $q = \frac{1}{p} - 1 \geq 0$, and in the above we showed that $q \in \beta$. Therefore $\beta > 0^*$.

We verified that $\beta \in \mathbb{R}^+$. Following that, we prove $\alpha\beta = 1^*$.

- $\forall p \in \alpha \wedge p > 0$ and $\forall q \in \beta \wedge q > 0$, $\exists r > 0$ such that $\frac{1}{q+r} \notin \alpha$, which follows that $\frac{1}{q+r} > p$. Hence $pq < p(q + r) < 1$. Therefore, $\alpha\beta \subset 1^*$.
- $\forall t \in 1^* \wedge p > 0$, based on the archimedean property of $\mathbb{Q}$, there exists an integer n_0 such that $n_0(1 - t) > 2t$, which follows that $t < \frac{n_0}{n_0+2} < \frac{n_0}{n_0+1}$. Since the distance between $p \in \alpha$ and $q \notin \alpha$ can be smaller than any positive rational number, there exist some choice of $p \in \alpha \wedge p > 0$ and $q \notin \alpha$ such that $q - p < \frac{p}{n_0}$. The construction method of p and q is as follows: We start with any choice of $p \in \alpha \wedge p > 0$ and $q \notin \alpha$. If they don't satisfy $q - p < \frac{p}{n_0}$, we check whether $\frac{p+q}{2}$ belongs to α. If so, we replace the current value of p with $\frac{p+q}{2}$. Otherwise, we replace the current value of q with it. We repeat this process until $q - p < \frac{p}{n_0}$ holds. The reason why the iterations will terminate is that with each iteration $p - q$ becomes a half of its previous value, and thus can be smaller than any positive rational number. On the other hand, p is increasing with each iteration, and so is $\frac{p}{n_0}$. Therefore, the construction method works. Then we put $w = \frac{p}{n_0} > 0$, and thus $n_0 w = p \in \alpha$, $(n_0 + 1)w > q \notin \alpha$. Let $s = \frac{1}{(n_0+2)w}$, $r = \frac{1}{(n_0+1)(n_0+2)w} > 0$, then $\frac{1}{s+r} = (n_0 + 1)w \notin \alpha$, which follows that $s \in \beta$. Hence $t < \frac{n_0}{n_0+2} = ps$, and $t \in \alpha\beta$. With the property of a Dedekind cut, $\forall t \in 1^* \wedge t \leq 0$, $t \in \alpha\beta$. Therefore, $1^* \subset \alpha\beta$.

We can conclude that $\alpha\beta = 1^*$. □

Now we have the addition operation and the multiplication operation in $\mathbb{R}^+$. We need to prove that they obey the distributive law, which is stated as $\forall \alpha, \beta, \gamma \in \mathbb{R}^+$, $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Proof. $\forall p \in \alpha(\beta+\gamma)$, $p < qr$ for some choice of $q \in \alpha \wedge q > 0$ and $r \in (\beta+\gamma) \wedge r > 0$. Further, $r = s + t$ for some choice of $s \in \beta \wedge s > 0$ and $t \in \gamma \wedge t > 0$ (if $s \leq 0$, we can pick $s' \in \alpha \wedge s' > 0$ and put $t' = t - s' + s < t$, hence $r = s' + t'$). Hence $p < q(s + t) = qs + qt$. There exist $s' \in \beta$ such that $s' > s > 0$ and $t' \in \gamma$ such that $t' > t > 0$. Thus $qs < qs'$ and $qt < qt'$, which follows that $qs \in \alpha\beta$ and $qt \in \alpha\gamma$. Hence $qs + qt \in \alpha\beta + \alpha\gamma$, and thus $p \in \alpha\beta + \alpha\gamma$. Therefore, $\alpha(\beta + \gamma) \subset \alpha\beta + \alpha\gamma$.

$\forall p \in \alpha\beta + \alpha\gamma$, $p = q_1 + q_2$ for some choice of $q_1 \in \alpha\beta$ and $q_2 \in \alpha\gamma$. Furthermore, $q_1 < r_1 s$ for some choice of $r_1 \in \alpha \wedge r_1 > 0$ and $s \in \beta \wedge s > 0$, and $q_2 = r_2 t$

for some choice of $r_2 \in \alpha \wedge r_2 > 0$ and $t \in \gamma \wedge t > 0$. Hence $p < q_1 s + q_2 t$. Suppose $q_1 \leq q_2$, then $p < q_1 s + q_2 t < q_2(s+t)$ where $s + t \in \beta + \gamma$. Thus $p \in \alpha(\beta + \gamma)$. Therefore, $\alpha\beta + \alpha\gamma \subset \alpha(\beta + \gamma)$. □

5.6 Expand the Multiplication Operation to the Real Number Set

We expand the multiplication operation in $\mathbb{R}^+$ defined above to $\mathbb{R}$ by adding the following definition:

Definition 5.3.

$$\alpha 0^* = 0^* \alpha = 0^*$$

$$\alpha\beta = \begin{cases} (-\alpha)(-\beta), & \text{if } \alpha < 0^*, \beta < 0^* \\ -((-\alpha)\beta), & \text{if } \alpha < 0^*, \beta > 0^* \\ -(\alpha(-\beta)), & \text{if } \alpha > 0^*, \beta < 0^* \end{cases}$$

Having proved that the multiplication operation we defined in $\mathbb{R}^+$ satisfies the properties required for a field, it is not difficult to prove that the properties also hold in $\mathbb{R}$ using the identity equation $\alpha = -(-\alpha)$. We shall give the proof of the commutative property as an example.

Proof. According to the definition of the multiplication operation, the commutative property holds when 0^* is involved in a multiplication operation.

If $\alpha < 0^*$ and $\beta < 0^*$, then $-\alpha > 0^*$ and $-\beta > 0^*$. Hence $\alpha\beta = (-\alpha)(-\beta) = (-\beta)(-\alpha) = \beta\alpha$.

If $\alpha < 0^*$ and $\beta > 0^*$, then $-\alpha > 0^*$. Hence $\alpha\beta = -((-\alpha)\beta) = -(\beta(-\alpha)) = \beta\alpha$.

If $\alpha > 0^*$ and $\beta < 0^*$, then $-\beta > 0^*$. Hence $\alpha\beta = -(\alpha(-\beta)) = -((-\beta)\alpha) = \beta\alpha$.

We can conclude that the multiplication operation in $\mathbb{R}$ satisfies the commutative property. □

Now we have proved that $\mathbb{R}$ is an ordered field with the least-upper-bound property.

6 Properties of the Defined Real Number Set