Dedekind Cuts

Ruochen Gu

August 2025

Abstract

Dedekind cuts is a way of constructing $\mathbb{R}$ from $\mathbb{Q}$. It directly proves Theorem 1.19 in Rudin's PMA (page 8/18).

Theorem 0.1. *(Existence Theorem) There exists an ordered field $\mathbb{R}$ which has the least-upper-bound property. Moreover, $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield.*

The construction consists of several steps. Note that this is merely a verbose version of Rudin's PMA, with omitted parts of the proof filled in.

1 Step I: Define Cuts

We start with the definition of a cut.

Definition 1.1. *A cut is any subset of $\mathbb{Q}$ (cut usually denoted in Greeks) that satisfies the following 3 properties:*

1. *α is nonempty, $\alpha \neq \mathbb{Q}$*
2. *If $p \in \alpha$, $q \in \mathbb{Q}$, and $q < p$, then $q \in \alpha$*
3. *If $p \in \alpha$, then $\exists r \in \alpha$, s.t. $p < r$*

We can quite easily see the following two corollaries from 1.1.

Corollary 1.1.1. *Let $p, q \in \mathbb{Q}$. If $p \in \alpha$, $q \notin \alpha$, then $p < q$*

Proof. Suppose for contradiction that $p \geq q$.
We first observe $p \neq q$, otherwise $q \in \alpha$.
Second, by definition 1.1 II, if $q < p$ and given $p \in \alpha$, then $q \in \alpha$. ※
Hence, $p < q$. □

Corollary 1.1.2. *Let $r, s \in \mathbb{Q}$. If $r \notin \alpha$, $r < s$, then $s \notin \alpha$*

Proof. Suppose for contradiction that $s \in \alpha$.
Then, by definition 1.1 II, $r \in \alpha$ as $r < s$. ※
Hence, $s \notin \alpha$. □

For the following steps, we show that **the collection of all such cuts, denoted** $\mathbb{R}$, satisfies our construction goal.

2 Step II: Define Order on $\mathbb{R}$

Definition 2.1. *(Order on $\mathbb{R}$) Let α, β be cuts. $\alpha < \beta \iff \alpha$ is a proper subset of β.*

Now, we need to show trichotomy and transitivity.

Corollary 2.1.1. *(Transitivity) If $\alpha < \beta$, $\beta < \gamma$, then $\alpha < \gamma$.*

Proof. Obviously, a proper subset of a proper subset is a proper subset. (trivial proof omitted) □

Corollary 2.1.2. *(Trichotomy) For any pair of α, β, only one of the three relations hold: $\alpha < \beta$, $\alpha = \beta$, $\alpha > \beta$.*

Proof. It's clear that at most one relation can hold. Now, it S.T.S. that at least one relation will hold. We prove that by assuming two relations to be false. Note also that two cuts cannot be disjoint. With the below three cases, we show that all three relations cannot fail at the same time.

Case 1: (1), (2) fail, i.e. α is not a subset of β.

$$\implies \exists a \in \alpha, \text{ s.t. } a \notin \beta \implies \forall b \in \beta, b < a \text{ since } a \neq b \text{ and a cannot be smaller than b}$$

$$\implies \forall b \in \beta, b \in \alpha \implies \beta \subsetneq \alpha \implies \beta < \alpha$$

Case 2: (1), (3) fail.
Given (1) fails, i.e. α is not a proper subset of $\beta \implies$ Either $\alpha = \beta$, or by (Case 1) $\alpha > \beta$.
Given (3) fails, i.e. β is not a proper subset of $\alpha \implies$ Either $\beta = \alpha$, or by (Case 3) $\beta > \alpha$. Hence, $\alpha = \beta$.

Case 3: (2), (3) fail. Observe this case is the opposite symmetry to case 1.

Hence, Trichotomy is satisfied and $\mathbb{R}$ is an ordered set. □

3 Step III: $\mathbb{R}$ has L.U.B.P.

Theorem 3.1. *($\mathbb{R}$'s L.U.B.P.) Let A be a nonempty subset of $\mathbb{R}$ that is bounded above by some $\beta \in \mathbb{R}$. Then, $\exists sup(A) \in \mathbb{R}$.*

Proof. Take $\gamma \coloneqq \bigcup_{\alpha_i \in A} \alpha_i$. Now, we show γ is a valid cut. Notice γ is nonempty as A is nonempty.
Since β is a cut, $\exists s \in \beta^c$, s.t. $\forall b \in \beta$, $b < s$. As a result, $s \notin \gamma \implies \gamma \neq \mathbb{Q}$. *Condition I check.*
Assume $x \in \gamma$, $\exists \alpha_i \in A$, s.t. $x \in \alpha_i$. If $p < x$, then $p \in \alpha_i \subset \gamma$. *Condition II check.*
Given $x \in \gamma \implies x \in \alpha_i \implies \exists r \in \alpha_i$, s.t. $x < r$. *Condition III check.* Hence, γ is a valid cut.

Now, W.T.S. $\gamma = sup(A)$.
By construction, $\alpha \leq \gamma$, $\forall \alpha \in A \implies \gamma$ is an upper bound of A.

Suppose $\delta < \gamma$. W.T.S. δ is not an upper bound of A.
$\exists z \in \alpha' \subset \gamma$, s.t. $z \notin \delta \implies \forall d \in \delta$, $d < z \implies \delta < \alpha' \in A$.

Hence, δ is not an upper bound of A, $\gamma = sup(A)$, and $\mathbb{R}$ has L.U.B.P. □

4 Step IV: Define Addition, Check Field's Additive Axioms

Definition 4.1. *Let $\alpha, \beta \in \mathbb{R}$, we define $\alpha + \beta \coloneqq \{x \in \mathbb{Q} \mid x = r +_{\mathbb{Q}} s,$ for some $r \in \alpha, s \in \beta\}$.*

Definition 4.2. *We define $0^* \coloneqq \{q \in \mathbb{Q} \mid q < 0\}$, trivially a cut.*

We now verify whether $\mathbb{R}$, with addition operation and additive identity (0^*) defined, satisfies field's additive axioms.

Proof. **(A1)** W.T.S. $\alpha + \beta$ is a cut.

Trivially, $\alpha + \beta$ is nonempty. Observe that

$$\exists r' \in \mathbb{Q}, \text{ s.t. } \forall a \in \alpha, a < r'. \text{ Similarly, } \exists s' \in \mathbb{Q}, \text{ s.t. } \forall b \in \beta, b < s'$$

$$\implies \forall r \in \alpha, \forall s \in \beta, r + s < r' + s' \implies \alpha + \beta \neq \mathbb{Q}$$

Condition I check.
Suppose $p \in \alpha + \beta$, $q < p$, $p = r + s$, for some $r \in \alpha, s \in \beta$

$$\implies q < r + s \implies q - r < s \implies q - r \in \beta \implies q = (q - r) + r \in \alpha + \beta$$

Condition II check.
Continuing from above. $\exists \overline{r} \in \alpha$, s.t. $r < \overline{r} \implies p = r + s < \overline{r} + s \in \alpha + \beta$.
Condition III check. Hence, $\alpha + \beta$ is a cut.

(A2) W.T.S. $\alpha + \beta = \beta + \alpha$

$$\alpha + \beta = \{x \in \mathbb{Q} \mid x = r + s, \text{ for some } r \in \alpha, s \in \beta\} = \{x \in \mathbb{Q} \mid x = s + r, \text{ for some } r \in \alpha, s \in \beta\} = \beta + \alpha$$

(A3) W.T.S. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$

$$\begin{aligned}
(\alpha + \beta) + \gamma &= \{x \in \mathbb{Q} \mid x = r + s, \text{ for some } r \in \alpha, s \in \beta\} + \gamma \\
&= \{y \in \mathbb{Q} \mid y = (r + s) + t, \text{ for some } r \in \alpha, s \in \beta, t \in \gamma\} \\
&= \{y \in \mathbb{Q} \mid y = r + (s + t), \text{ for some } r \in \alpha, s \in \beta, t \in \gamma\} \\
&= \alpha + \{x \in \mathbb{Q} \mid x = s + t, \text{ for some } s \in \beta, t \in \gamma\} \\
&= \alpha + (\beta + \gamma)
\end{aligned} \tag{1}$$

(A4) W.T.S. $\alpha + 0^* = \alpha$, i.e. show $\alpha + 0^* \subset \alpha$ and $\alpha \subset \alpha + 0^*$

(First direction is easy) $\forall r \in \alpha, s \in 0^*$, $r + s < r \implies r + s \in \alpha \implies \alpha + 0^* \subset \alpha$

(Right to left) $\forall a \in \alpha$, $\exists t \in \alpha$, s.t. $a < t$.
$\implies a - t < 0$, $a - t \in 0^* \implies a = t + (a - t) \in \alpha + 0^*$.

(A5) W.T.S. Given $\alpha \in \mathbb{R}$, $\exists \beta \in \mathbb{R}$, s.t. $\alpha + \beta = 0^*$.

Construct β to be the set of $p \in \mathbb{Q}$, s.t. $\exists r \in \mathbb{Q}^+$, $-p - r \notin \alpha$. We W.T.S. β is a cut, and $\alpha + \beta = 0^*$.

Since α is a cut, $\exists \overline{a} \in \mathbb{Q}$, s.t. $a < \overline{a}, \forall a \in \alpha$.
Consider $p = -(\overline{a} + 1) = -\overline{a} - 1$,

$$-p - 1 = \overline{a} + 1 - 1 = \overline{a} \notin \alpha \implies p = -\overline{a} - 1 \in \beta$$

Hence, β is nonempty.
Now, suppose $s \in \alpha$, then we claim $-s \notin \beta$.
S.F.C. that $-s \in \beta \implies s - r \notin \alpha$, for some $r > 0 \implies s \notin \alpha$, as $s - r < s$. By contradiction, we have *Condition I checked.*

Pick $p \in \beta, r \in Q^+$, so that $-p - r \notin \alpha$.
If $q < p \implies -p < -q$, then $a < -p - r < -q - r, \forall a \in \alpha$. Therefore, $q \in \beta$. *Condition II checked.*

Continue from above. Consider $t = p + \frac{r}{2}$, then $p < t$ and $-t - \frac{r}{2} = -p - r \notin \alpha \implies t \in \beta$. *Condition III checked.*
Hence, β is a cut.

Lastly, we W.T.S. $\alpha + \beta \subset 0^*$ and $0^* \subset \alpha + \beta$.
Take $a \in \alpha$, $b \in \beta$

$$\implies \exists r \in \mathbb{Q}^+, \text{ s.t. } -b - r \notin \alpha \implies a < -b - r \implies a + b < -r < 0 \implies \alpha + \beta \subset 0^*$$

Now, the opposite direction. Pick $v \in 0^*$, let $w = -\frac{v}{2} > 0$.
By $\mathbb{Q}$'s Archimedean Property, we have

$$\exists n \in \mathbb{Z}, \text{ s.t. } nw \in \alpha \text{ and } (n+1)w \notin \alpha$$

Let $p = -(n+2)w \implies p \in \beta$, since $-p - w \notin \alpha$, and

$$v = nw + p \in \alpha + \beta$$

Thus, $0^* \subset \alpha + \beta$. We are done. □

5 Step V: Ordered Field Additive Requirement

Theorem 5.1. *If $\alpha, \beta, \gamma \in \mathbb{R}$ and $\beta < \gamma$, then $\alpha + \beta < \alpha + \gamma$*

Proof. First, we show $\alpha + \beta \subset \alpha + \gamma$.

$$\forall a \in \alpha, b \in \beta \implies b \in \gamma \text{ because } \beta < \gamma \implies a + b \in \alpha + \gamma$$

Second, S.F.C. that $\alpha + \beta = \alpha + \gamma$. Using our proven rules, we add $-\alpha$ on both side and get $\beta = \gamma$.
Contradiction! ※ □

6 Step VI: Define Multiplication, Check Field's Multiplicative Axioms and Distributive Axiom

Multiplication is a little special, as products of negative rationals are positive. As a result, we will first work in $\mathbb{R}^+ := \{\alpha \in \mathbb{R} \mid \alpha > 0^*\}$.

Definition 6.1. *If $\alpha \in \mathbb{R}^+$, $\beta \in \mathbb{R}^+$, then we define $\alpha\beta$ to be*

$$\{p \in \mathbb{Q} \mid p \le rs, \text{ for some } r \in \alpha, s \in \beta \text{ s.t. } r > 0, s > 0\} = \{p \in \mathbb{Q} \mid \exists r \in \alpha\, \exists s \in \beta\, (r > 0 \wedge s > 0 \wedge p \le rs)\}$$

Definition 6.2. $1^* := \{q \in \mathbb{Q} \mid q < 1\}$

We now verify whether $\mathbb{R}^+$, with multiplication operation and multiplicative identity (1^*) defined, satisfies field's multiplicative axioms and distributivity axiom.

Proof. For the following proofs, we take $\alpha, \beta \in \mathbb{R}^+$, i.e. $\alpha, \beta > 0^*$.

(M1) W.T.S. $\alpha\beta$ is a cut.

For (M1) proof, we take $r \in \alpha, s \in \beta$, s.t. $r, s > 0$.

Since $rs \le rs$, $rs \in \alpha\beta \implies \alpha\beta$ is nonempty.
Consider $r' \notin \alpha$, $s' \notin \beta$, we know

$$r < r', \forall r \in \alpha^+; \text{ and } s < s', \forall s \in \beta^+$$

$\implies rs < r's' \implies r's' \notin \alpha\beta \implies \alpha\beta \neq \mathbb{Q}$. *Condition I check.*

Let $p, q \in \alpha\beta$, $q < p$. Since $p \in \alpha\beta$, we have

$$p \leq rs, \text{ for some } r \in \alpha^+, s \in \beta^+ \implies q < p \leq rs \implies q \in \alpha\beta$$

Condition II check.

Taking the aforementioned $p \in \alpha\beta$,

$$\exists r' \in \alpha, \text{ s.t. } r < r' \implies p \leq rs < r's \implies \exists t \in \mathbb{Q}, \text{ s.t. } p \leq rs < t < r's \implies \exists t \in \alpha\beta$$

Condition III check. Hence, $\alpha\beta$ is a cut. And, $\alpha\beta \in \mathbb{R}^+$.

(M2) W.T.S. $\alpha\beta = \beta\alpha$

$$\begin{aligned}
\alpha\beta &= \{p \in \mathbb{Q} \mid p \leq rs, \text{ for some } r \in \alpha, s \in \beta \text{ s.t. } r > 0, s > 0\} && (2)\\
&= \{p \in \mathbb{Q} \mid p \leq sr, \text{ for some } r \in \alpha, s \in \beta \text{ s.t. } r > 0, s > 0\} && (3)\\
&= \beta\alpha && (4)
\end{aligned}$$

(M3) W.T.S. $(\alpha\beta)\gamma = \alpha(\beta\gamma)$

$$\begin{aligned}
(\alpha\beta)\gamma &= \{p \in \mathbb{Q} \mid p \leq rs, \text{ for some } r \in \alpha, s \in \beta \text{ s.t. } r > 0, s > 0\} \cdot \gamma && (5)\\
&= \{p \in \mathbb{Q} \mid p \leq (rs)t, \text{ for some } r \in \alpha, s \in \beta, t \in \gamma \text{ s.t. } r > 0, s > 0, t > 0\} && \text{Lemma 1}\\
&= \{p \in \mathbb{Q} \mid p \leq r(st), \text{ for some } r \in \alpha, s \in \beta, t \in \gamma \text{ s.t. } r > 0, s > 0, t > 0\} && \text{Lemma 1}\\
&= \alpha \cdot \{p \in \mathbb{Q} \mid p \leq st, \text{ for some } s \in \beta, t \in \gamma \text{ s.t. } s > 0, t > 0\}\\
&= \alpha(\beta\gamma)
\end{aligned}$$

Lemma 1.

$$\{p \in \mathbb{Q} \mid p \leq rs\}\text{(, for all } r \in \alpha^+, s \in \beta^+) \cdot \gamma = \{p \in \mathbb{Q} \mid p \leq (rs)t\}\text{(, for all } r \in \alpha^+, s \in \beta^+, t \in \gamma^+)$$

Proof. Since we have shown above that $\alpha\beta \in \mathbb{R}^+$, this product is defined.

First, $(\subset)$ direction.

Take $k \in \{p \in \mathbb{Q} \mid p \leq rs\}$(, for all $r \in \alpha^+, s \in \beta^+) \cdot \gamma$
$\implies \exists q \in \{p \in \mathbb{Q} \mid p \leq rs\}$, $\exists t \in \gamma$, s.t. $q > 0$, $t > 0$, and $k \leq qt$
$\implies \exists r \in \alpha^+$, $\exists s \in \beta^+$, s.t. $q \leq rs \implies k \leq qt \leq (rs)t$, for some $r \in \alpha^+, s \in \beta^+, t \in \gamma^+$
$\implies k \in \{p \in \mathbb{Q} \mid p \leq (rs)t\}$(, for all $r \in \alpha^+, s \in \beta^+, t \in \gamma^+$)

Second, $(\supset)$ direction.

Take $m \in \{p \in \mathbb{Q} \mid p \leq (rs)t\}$(, for all $r \in \alpha^+, s \in \beta^+, t \in \gamma^+$)
$\implies \exists r' \in \alpha^+, s' \in \beta^+, t' \in \gamma^+$, s.t. $m \leq (r's')t'$
Observe $r's' \in \{p \in \mathbb{Q} \mid p \leq rs\}$(, for all $r \in \alpha^+, s \in \beta^+$)
$\implies m \in \{p \in \mathbb{Q} \mid p \leq rs\}$(, for all $r \in \alpha^+, s \in \beta^+) \cdot \gamma$

And we're done. □

(M4) W.T.S. $\alpha \cdot 1^* = \alpha$, i.e. show $\alpha \cdot 1^* \subset \alpha$ and $\alpha \subset \alpha \cdot 1^*$

Intuition for non-positive rationals: suppose $q \in 0^* \cup \{0\}$, then $q \in \alpha, 1^*, \alpha \cdot 1^*$. We worry much more about the positive rationals.

$(\alpha \cdot 1^* \subset \alpha)$
$\alpha \cdot 1^* = \{p \in \mathbb{Q} \mid p \leq rs\}$, for all $r \in \alpha^+, s \in 1^{*^+}$.

$$\forall p \in \alpha \cdot 1^*,\ \exists r \in \alpha^+,\ s \in 1^{*^+}, \text{ s.t. } p \leq rs < r \implies p \in \alpha \implies \alpha \cdot 1^* \subset \alpha$$

$(\alpha \subset \alpha \cdot 1^*)$
As the intuition covers the non-positive rationals, we consider the positive rational case.
$\forall r \in \alpha^+,\ \exists r' \in \alpha^+,\ s.t.\ 0 < r < r'$

$$\implies \frac{r}{r'} < 1 \implies \frac{r}{r'} \in 1^* \implies r = \frac{r}{r'} \cdot r' \in 1^* \cdot \alpha \implies \alpha \subset \alpha \cdot 1^*$$

Hence, $\alpha = \alpha \cdot 1^*$

(M5) W.T.S. Given $\alpha \in \mathbb{R}^+$, $\exists \beta \in \mathbb{R}^+$, s.t. $\alpha \cdot \beta = 1^*$.

Let γ be the set of $p \in \mathbb{Q}^+$, s.t. $\exists r \in \mathbb{Q}$, $r > 1$, $\frac{1}{p} \cdot \frac{1}{r} \notin \alpha$.
Construct $\beta \coloneqq \gamma \cup 0^* \cup \{0\}$.
We W.T.S. β is a cut, and $\alpha \cdot \beta = 1^*$.

Since α is a cut, $\exists \overline{a} \in \mathbb{Q}^+$, s.t. $a < \overline{a}$, $\forall a \in \alpha$.
Consider $p = \frac{1}{\overline{a}} \cdot \frac{1}{2} > 0$,

$$\frac{1}{p} \cdot \frac{1}{2} = 2\overline{a} \cdot \frac{1}{2} = \overline{a} \notin \alpha \implies p \in \gamma \subset \beta$$

Hence, β is nonempty.
Now, suppose $s \in \alpha^+$, then we claim $\frac{1}{s} \notin \beta$.
S.F.C. that $\frac{1}{s} \in \beta \implies s \cdot \frac{1}{r} \notin \alpha$, for some $r > 0 \implies s \notin \alpha$, as $s \cdot \frac{1}{r} < s$.
By contradiction, we have *Condition I checked.*

Pick $p \in \beta^+$, $r \in \mathbb{Q}$, $r > 1$, so that $\frac{1}{p} \cdot \frac{1}{r} \notin \alpha$.
If $0 < q < p \implies \frac{1}{p} < \frac{1}{q} \implies \forall a \in \alpha$, $a < \frac{1}{p} \cdot \frac{1}{r} < \frac{1}{q} \cdot \frac{1}{r}$.
Therefore, $q \in \beta$. And all non-positive rationals automatically fall in β. *Condition II checked.*

Continue from above. Consider $t = p \cdot r'$, where $1 < r' < r$, then $p < t$ and

$$\frac{1}{t} \cdot \frac{1}{\frac{r}{r'}} = \frac{1}{pr'} \cdot \frac{1}{\frac{r}{r'}} = \frac{1}{p} \cdot \frac{1}{r} \notin \alpha \implies t \in \beta$$

Condition III checked. Hence, β is a cut.

Again, non-positive rationals are all well-behaved, so we only discuss the set of positive rationals below.
$(\alpha \cdot \beta \subset 1^*)$
$\forall q \in (\alpha \cdot \beta)^+$, $q \leq ab$, for some $a \in \alpha^+$, $b \in \beta^+$.

$$\implies \exists r \in \mathbb{Q}, r > 1, \text{ s.t. } \frac{1}{b} \cdot \frac{1}{r} \notin \alpha \implies a < \frac{1}{b} \cdot \frac{1}{r} \implies q \leq ab < abr < 1 \implies q \in 1^* \implies \alpha \cdot \beta \subset 1^*$$

$(1^+ \subset \alpha \cdot \beta)$
Pick $v \in 1^{*^+}$, let $w = \frac{1}{v} > 1$. Take any $a_0 \in \alpha$, s.t. $a_0 > 0$.
By A.P. for Exponents (in $\mathbb{Q}$, proved in Appendix), we have $\exists n \in \mathbb{Z}$, s.t. $a_0 \cdot w^n \in \alpha$ but $a_0 \cdot w^{n+1} \notin \alpha$.
Since α is a cut, $\exists w' \in \alpha$ s.t. $a_0 \cdot w^n < w'$. Let $s = \frac{w'}{a_0 \cdot w^n} > 1$. Observe $s \cdot (a_0 \cdot w^n) \in \alpha$.
Let $p = \frac{1}{a_0 \cdot w^{n+1} \cdot s} \implies p \in \beta$, since $\frac{1}{p} \cdot \frac{1}{s} = a_0 \cdot w^{n+1} \notin \alpha$.

$$\implies v = \frac{1}{w} = (s \cdot a_0 \cdot w^n) \cdot p \in \alpha\beta \implies 1^* \subset \alpha \cdot \beta$$

Hence, $1^* = \alpha\beta$.

(D) W.T.S. If $\alpha, \beta, \gamma \in \mathbb{R}^+$, *then* $(\alpha+\beta)\cdot\gamma = \alpha\cdot\gamma + \beta\cdot\gamma$.

$$\begin{aligned}(\alpha+\beta)\cdot\gamma &= \{r+s\in\mathbb{Q} \mid r\in\alpha,\ s\in\beta\}\cdot\gamma \\ &= \{p\in\mathbb{Q} \mid p\le (r+s)t\}\ (\text{, for all } r+s\in(\alpha+\beta)^+,\ t\in\gamma^+) \\ &= \{p\in\mathbb{Q} \mid p\le (r+s)t\}\ (\text{, for all } r\in\alpha^+,\ s\in\beta^+,\ t\in\gamma^+) \\ &= \{p\in\mathbb{Q} \mid p\le rt+st\} \\ &= \{p\in\mathbb{Q} \mid p\le rt\} + \{p\in\mathbb{Q} \mid p\le st\} \\ &= \alpha\cdot\gamma + \beta\cdot\gamma\end{aligned} \tag{6}$$

The third equality requires case work, details omitted. □

7 Step VII: Ordered Field Multiplicative Requirement

Theorem 7.1. *If* $\alpha > 0^*,\ \beta > 0^*$, *then* $\alpha\beta > 0^*$.

Proof. By definition, $\alpha\beta = \{q\in\mathbb{Q} \mid q\le rs\}$ (, for all $r\in\alpha^+,\ s\in\beta^+$) $\implies r,s>0 \implies rs>0 \implies rs\in\alpha\beta$. Hence, $\alpha\beta > 0^*$ □

8 Step VIII: Completed Multiplication Definition, Re-check Axioms and Properties

We complete the definition of multiplication by setting $\alpha 0^* = 0^*\alpha = 0^*$, and by setting

$$\alpha\beta = \begin{cases}(-\alpha)(-\beta), & \text{if } \alpha<0^*,\ \beta<0^*. \\ -[(-\alpha)\beta], & \text{if } \alpha<0^*,\ \beta>0^*. \\ -[\alpha(-\beta)], & \text{if } \alpha>0^*,\ \beta<0^*.\end{cases} \tag{7}$$

We have already proved that the axioms (M) and (D) hold in $\mathbb{R}^+$, left to do's are to verify them again in $\mathbb{R}$, by simply repeated application of identity $\gamma = -(-\gamma)$.

Proof. For the following proofs, we take $\alpha, \beta \in \mathbb{R}$, and split into 3 cases.

- $\alpha < 0^*,\ \beta < 0^*$
- $\alpha < 0^*,\ \beta > 0^*$
- $\alpha > 0^*,\ \beta < 0^*$

We denote each case (i), for $i \in \{1,2,3\}$.

(M1) W.T.S. $\alpha\beta$ is a cut.

Case (1): $\alpha\beta = (-\alpha)(-\beta)$, is a cut in $\mathbb{R}^+$.
Case (2): $\alpha\beta = -[(-\alpha)\beta]$. $(-\alpha)\beta$ is a cut in $\mathbb{R}^+$, and $-[(-\alpha)\beta]$ exists in $\mathbb{R}$ by axiom (A5).
Case (3): By symmetry to case (2).

(M2) W.T.S. $\alpha\beta = \beta\alpha$

Case (1): $\alpha\beta = (-\alpha)(-\beta) = (-\beta)(-\alpha) = \beta\alpha$.
Case (2): $\alpha\beta = -[(-\alpha)\beta] = -[\beta(-\alpha)] = \beta\alpha$.
Case (3): By symmetry to case (2).

(M3) W.T.S. $(\alpha\beta)\gamma = \alpha(\beta\gamma)$

Case (1): $\alpha < 0^*,\ \beta, \gamma > 0^*$:

$$(\alpha\beta)\gamma = \{-[(-\alpha)\beta]\}\gamma = -\{[(-\alpha)\beta]\gamma\} = -\{(-\alpha)(\beta\gamma)\} = \alpha(\beta\gamma)$$

Case (2): $\beta < 0^*,\ \alpha, \gamma > 0^*$: By symmetry to case (1).
Case (3): $\gamma < 0^*,\ \alpha, \beta > 0^*$: By symmetry to case (1).
Case (4): $\alpha, \beta < 0^*,\ \gamma > 0^*$:

$$(\alpha\beta)\gamma = [(-\alpha)(-\beta)]\gamma = (-\alpha)[(-\beta)\gamma] = (-\alpha)[-(\beta\gamma)] = -[(-\alpha)(\beta\gamma)] = \alpha(\beta\gamma)$$

Case (5): $\alpha, \gamma < 0^*,\ \beta > 0^*$: By symmetry to case (4).
Case (6): $\beta, \gamma < 0^*,\ \alpha > 0^*$: By symmetry to case (4).
Case (7): $\alpha, \beta, \gamma < 0^*$:

$$(\alpha\beta)\gamma = [(-\alpha)(-\beta)]\gamma = -\{[(-\alpha)(-\beta)](-\gamma)\} = -\{(-\alpha)[(-\beta)(-\gamma)]\} = -[(-\alpha)(\beta\gamma)] = \alpha(\beta\gamma)$$

(M4) W.T.S. $\alpha \cdot 1^* = \alpha$, i.e. show $\alpha \cdot 1^* \subset \alpha$ and $\alpha \subset \alpha \cdot 1^*$

Case (1)*: $\alpha \geq 0^*$, this case is already shown in previous step.
Case (2)*: $\alpha < 0^* \implies \alpha \cdot 1^* = -[(-\alpha)1^*] = -(-\alpha) = \alpha$.

(M5) W.T.S. Given $\alpha \in \mathbb{R} - \{0^*\}$, $\exists \beta \in \mathbb{R}$, s.t. $\alpha \cdot \beta = 1^*$.

Case (1)*: $\alpha > 0^*$, this case is already shown in previous step.
Case (2)*: $\alpha < 0^* \implies -\alpha > 0^* \implies \exists(-\beta) \in \mathbb{R}^+$ *s.t.* $(-\alpha)(-\beta) = \alpha\beta = 1^*$.

(D) W.T.S. If $\alpha, \beta, \gamma \in \mathbb{R}$, *then* $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$.

□

Proof of (D) breaks into cases, which we will not elaborate. (Read more in **Rudin PMA page 20/30**)

Now, We have now completed the proof that $\mathbb{R}$ is an ordered field with the least-upper-bound property.

9 Step IX: $\mathbb{R}$ Contains $\mathbb{Q}$ as a Subfield

Theorem 9.1. *We associate with each $r \in \mathbb{Q}$ the set $r^* := \{p \in \mathbb{Q} \mid p < r\}$. Observe that r^* is a cut, i.e. $r^* \in \mathbb{R}$. And these rational cuts satisfy the following relations:*

1. $r^* + s^* = (r + s)^*$
2. $r^* s^* = (rs)^*$
3. $r^* < s^* \iff r < s$

Proof. Relation (1)
$\forall p \in r^* + s^*$, $p = u + v$, where $u < r$, $v < s$.
Hence, $p < r + s \implies p \in (r + s)^*$.
Now, the opposite direction. $\forall p \in (r + s)^*$, we have $p < r + s$.
Choose $t := \frac{r+s-p}{2}$, let $r' = r - t$, $s' = s - t$.

$$\implies r' \in r^*,\ s' \in s^* \implies p \in r^* + s^*, \text{ as } p = r' + s'$$

Relation (1) proof completed.

Relation (2). Here we only prove in the condition where $r, s \in \mathbb{R}^+$, as the other three cases follow naturally with minor changes.
$\forall p \in r^* s^* = \{p \in \mathbb{Q} \mid p \leq r's'\}$ (, for all $r' \in r^{*^+}$, $s' \in s^{*^+}$)

$$\implies p \leq r's' < rs \implies p \in (rs)^*$$

Hence, $r^*s^* \subset (rs)^*$.
Now, the opposite direction. Here we don't need to worry about non-positive rationals in $(rs)^*$, as they naturally fall in r^*s^*.
$\forall p \in (rs)^{*^+}, p < rs$. Choose $t = \left(\frac{rs}{p}\right) > 1$.
By Theorem 9.5, $\exists t' \in \mathbb{Q}$ s.t. $1 < t'$ and $(t')^2 < \frac{rs}{p}$. Let $r' = r\frac{1}{t'},\ s' = s\frac{1}{t'}$.

$$\implies r' \in r^*,\ s' \in s^* \implies p = rs \cdot \frac{p}{rs} < rs \cdot \frac{1}{(t')^2} = r's' \implies p \in r^*s^*$$

Hence, $r^*s^* = (rs)^*$

Relation (3)
($\leftarrow$) If $r < s$, then $r \in s^*$, but $r \notin r^* \implies r^* < s^*$.
($\rightarrow$) If $r^* < s^*$, then $\exists p \in s^*$ s.t. $p \notin r^*$.
Hence, $r \leq p < s$. We are done. □

The replacement of rational numbers by their corresponding rational cuts preserves sums, products, and order. In a more formal wording, the ordered field $\mathbb{Q}$ is isomorphic to the ordered field $\mathbb{Q}^*$, which consists of rational cuts.

It is this identification of $\mathbb{Q}$ with $\mathbb{Q}^*$ which allows us to regard $\mathbb{Q}$ as a subfield of $\mathbb{R}$.

Note, the same association occurs with real numbers in complex field, and integers in rational numbers. We will end with a huge theorem without proof.

Theorem 9.2. *Any two ordered fields with the L.U.B.P. are isomorphic.*

Appendix

Theorem 9.3. *(Archimedean Property on $\mathbb{Q}$)*
Given $r \in \mathbb{Q}$ and $r > 0$. $\forall q \in \mathbb{Q}$, $\exists n \in \mathbb{N}$, s.t. $nr > q$.

Proof. If $q \leq 0$, we can take $n = 1$ to trivially satisfy the above statement. Below, we discuss the case when $q > 0$.

Since we are talking about rational numbers, we have

$$r = \frac{n_r}{d_r}, \;\; q = \frac{n_q}{d_q}, \;\; n_r, d_r, n_q, d_q \in \mathbb{N}$$

Consider $n = d_r \cdot n_q \cdot d_q + 1$. We have

$$nr = d_r \cdot n_q \cdot d_q \cdot \frac{n_r}{d_r} + \frac{n_r}{d_r} = n_q \cdot d_q \cdot n_r + \frac{n_r}{d_r} > n_q \geq \frac{n_q}{d_q} = q, \;\; \forall q \in \mathbb{Q}^+$$

□

Theorem 9.4. *(Archimedean Property on $\mathbb{Q}$ for Exponent)*
Given $r \in \mathbb{Q}$ and $r > 0$. $\forall q \in \mathbb{Q}$, s.t. $q > 1$, $\exists n \in \mathbb{N}$ s.t. $q^n > r$.

Proof. Again, the proposition holds trivially when $r \leq 1$.

For $r > 1$. Let $m \in \mathbb{N}$, s.t. $m > r$. So, it S.T.S. $\exists n \in \mathbb{N}$, s.t. $q^n > m$.

$$q = \frac{j}{k}, \;\; j, k \in \mathbb{N}, \;\; where \; j > k \implies j \geq k + 1 \implies q \geq \frac{k+1}{k} = 1 + \frac{1}{k}$$

S.F.C. $\forall n \in \mathbb{N}$, $q^n \leq m$.
$\implies m \geq (1 + \frac{1}{k})^n \geq 1 + \frac{n}{k}$ for all natural number. Contradiction! ※ □

Theorem 9.5. *Given $t \in \mathbb{Q}$, $t > 1$. Let $A \coloneqq \{p \in \mathbb{Q} \mid p^2 < t, \; p > 1\}$. Then A is nonempty.*

Proof. Consider $a = 1 + \frac{1}{n}$. By Theorem 9.3, we know $\exists n \in \mathbb{N}$ s.t. $n > \frac{3}{t-1} > 0$.

$$\begin{aligned}
(1 + \frac{1}{n})^2 &= 1 + \frac{2}{n} + \frac{1}{n^2} && (8)\\
&= 1 + \frac{1}{n}(2 + \frac{1}{n}) && (9)\\
&\leq 1 + \frac{3}{n} && (10)\\
&< 1 + 3 \cdot \frac{1}{3}(t - 1) && (11)\\
&= 1 + (t - 1) = t && (12)
\end{aligned}$$

Observe that $a > 1$ and $a^2 < t \implies a \in A$. Hence, A is nonempty.

□