Dedekind cut

Yulin Liu

September 17, 2017

Theorem 1 *There exists an ordered field $\mathbb{R}$ which has the least-upper-bound property. Moreover, $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield.*

The previous content has proved that $\mathbb{Q}$ is an ordered field which has the least-upper-bound property. Now, we have to show that there exists a bigger set has these properties and it contains $\mathbb{Q}$.

We will make all definitions of concepts clear for us one by one.
The first one is order .

Definition 2 *Let S be a set. An order on S is a relation, denote by $<$, with the following two properties:*

1. *If $x \in S$ and $y \in S$, then one and only one of the statements:*

$$x < y, \quad x = y, \quad y < x$$

is true.

2. *If $x, y, z \in S$, if $x < y$ and $y < z$, then $x < z$.*

The first one tells us that every two elements in an ordered set S can compare with each other. The second one says that "less than" is a transitive property.

Definition 3 *field: A field is a set F with two operations, called addition and multiplication, which satisfy the following so-called "field axioms": (A), (M), and (D):*

Addition:

A1 *If $x \in F$, and $y \in F$, then their sum $x + y$ is in F*

A2 *Addition is commutative: $x + y = y + x$ for all $x, y \in F$*

A3 *Addition is associative: $(x + y) + z = x + (y + z)$ for all $x, y, z \in F$*

A4 *F contains an element 0 such that $0 + x = x$ for every $x \in F$*

A5 *To every $x \in F$ corresponds an element $-x \in F$ such that $x + (-x) = 0$*

Multiplication:

M1 *If $x \in F$, and $y \in F$, then their product xy is in F*

M2 *Multiplication is commutative: $xy = yx$ for all $x, y \in F$*

M3 *Multiplication is associative: $(xy)z = x(yz)$ for all $x, y, z \in F$*

M4 *F contains an element $1 \neq 0$ such that $1x = x$ for every $x \in F$*

M5 *If $x \in F$ and $x \neq 0$ then there exists an element $1/x \in F$ such that $x \cdot (1/x) = 1$*

The distributive law

$$x(y+z) = xy + xz$$

holds for all $x, y, z \in F$

We will skip all the propositions, because the book has explained them in detail.

Now, if a set is ordered and a field, it is called ordered field, such that

1. $x + y < x + z$ if $x, y, z \in F$ and $y < z$
2. $xy > 0$ if $x, y \in F$ and $x > 0, y > 0$

Now, we are going to discuss the definition of least-upper-bound property.

Definition 4 *S is an ordered set, and $E \subset S$. If there exists a $\beta \in S$ such that $x \leq \beta$ for every $x \in E$, we say that E is bounded above, and call β an upper bound of E. Suppose $\exists \alpha \in S$ with the following properties:*

1. *α is an upper bound of E*
2. *If $\gamma < \alpha$ then γ is not an upper bound of E*

Then α is called the least upper bound of E, and we write

$$\alpha = \sup E$$

We also have the definition of infimum of a set, the greatest lower bound of a set.

Definition 5 *Least upper bound property is: If $E \subset S$, E is not empty, and E is bounded above, then sup E exists in S.*

Theorem 1.20 is the theorem about archimedean property of $\mathbb{R}$. But we just can only use the fact that this property holds under $\mathbb{Q}$:
If $x, y \in \mathbb{Q}$, and $x > 0$, then there is a positive integer n such that

$$(n+1)x > y > nx$$

The second part of theorem 1.20 says that rational numbers are dense in real number. We can always find a rational number between any different real numbers. The proof of theorem 1.20 is trivial under rational field.

For now, we have enough background knowledge and tools for proving theorem 1.19. Proving sometimes is finished by calculation, statement, derivation, induction or iteration. Here, the problem is about existence. If we can create something that satisfies all the requirements, then the problem is done.

This construction method to prove theorem 1.19 is invented by Dedekind, and this approach to create real numbers is called Dedekind cut. The whole proof is divided into 9 steps.

Step 1 *First, we define* $\mathbb{R}$. *We say that* $\mathbb{R}$ *is a set, the elements of* $\mathbb{R}$ *will be certain subsets of* $\mathbb{Q}$*, called cuts. A cut is, by definition, any set* $\alpha \subset \mathbb{Q}$ *with following 3 properties:*

I α *is not empty,* $\alpha \neq \mathbb{Q}$

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

III If $p \in \alpha$, *then* $p < r$ *for some* $r \in \alpha$

The first says that α is a nonempty proper subset of $\mathbb{Q}$. The third says that α has no largest element. The second implies the following facts:

If $p \in \alpha$ and $q \notin \alpha$ then $p < q$.
If $r \notin \alpha$ and $r < s$ then $s \notin \alpha$.

Now, we have the real number set $\mathbb{R}$, but does that satisfy the requirements in theorem 1.19? We need to check. The very first thing we need to know is that what is the definition of order of this set.

Step 2 *Define* $\alpha < \beta$ *to mean:* α *is a proper subset of* β. *Is this definition reasonable? Does it make sense?*

If $\alpha < \beta$, $\beta < \gamma$, *then it is clear that* $\alpha < \gamma$. *To show for each two cuts in* $\mathbb{R}$*, one and only one of following three holds:*

$$\alpha < \beta, \quad \alpha = \beta, \quad \beta < \alpha.$$

We assume that the first 2 fail. $\alpha \nsubseteq \beta$, *so* $\exists p \in \alpha$, $p \notin \beta$. *For every* $q \in \beta$, *we have* $q < p$, $\Rightarrow q \in \alpha \Rightarrow \beta < \alpha$.

Now, $\mathbb{R}$ is an ordered set. Next, we prove $\mathbb{R}$ has least-upper-bound property.

Step 3 *A is an nonempty subset of* $\mathbb{R}$, $\beta \in \mathbb{R}$ *is an upper bound of A. We define*

$$\gamma = \bigcup_{\alpha \in A} \alpha$$

This is saying that $p \in \gamma \Leftrightarrow p \in \alpha$ *for some* α *in A. We will prove that* $\gamma \in \mathbb{R}$*, which means* γ *is a cut. Also, more importantly,* γ *is sup A.*

property I *A is nonempty* $\Longrightarrow \exists \alpha_0 \in A$, *$\alpha_0$ is nonempty.* $\alpha_0 \in \gamma \Longrightarrow \gamma$ *is not empty.*
$\forall \alpha \in A$, *because β is an upper bound of A, we have* $\beta > \alpha \Longrightarrow \beta > \gamma \Longrightarrow \gamma \neq \mathbb{Q}$.

property II *pick* $p \in \gamma \Longrightarrow p \in \alpha_1$, *for some* $\alpha_1 \in A$. *If* $q < p \Longrightarrow q \in \alpha \Longrightarrow q \in \gamma$.

property III *If* $r \in \alpha_1$ *and* $r > p \Longrightarrow r \in \gamma$ *and* $r > p$.

So, $\gamma \mathbb{R}$, γ is a cut.

It is clear that $\alpha \leq \gamma$, γ is an upper bound of A. If $\delta < \gamma$, then $\exists s \in \gamma$, $s \notin \delta$. Because $s \in \gamma$, then $s \in \alpha$, for some $\alpha \in A$, then $\delta < \alpha \Longrightarrow \delta$ is not an upper bound of $A \Longrightarrow \gamma = sup\ A$.

Now, we prove that $\mathbb{R}$ is a field. First we prove addition axioms.

Step 4 *define:* $\alpha + \beta = \{r + s | r \in \alpha, s \in \beta\}$. $0^* = \{p | p \in \mathbb{Q}, p < 0\}$

A1 $\alpha + \beta$ *is a cut*

I *it is clear that $\alpha + \beta$ is not empty, is a proper subset of* $\mathbb{Q}$.

II $p \in \alpha + \beta \Longrightarrow p = r + s$, *if* $q < p$, *then* $q - s < r$, *which means* $q - s \in \alpha$, $q = (q - s) + s \in \alpha + \beta$.

III $t \in \alpha$, $t > r \Longrightarrow p < t + s$ *and* $t + s \in \alpha + \beta$.

A2 *commutative law*

$$\begin{aligned} \alpha + \beta &= \{r + s | r \in \alpha, \quad s \in \beta\} \\ &= \{s + r | s \in \beta, \quad r \in \alpha\} = \beta + \alpha \end{aligned}$$

A3 *associative law*
The proof is the same with A2.

A4 *we need to show* $\alpha + 0^* = \alpha$

$\Longrightarrow$ $\alpha + 0^* \subset \alpha$
$r \in \alpha$, $p \in 0^*$, *then* $r + p < r \in \alpha$.

$\Longleftarrow$ $\alpha + 0^* \supset \alpha$
pick $p, r \in \alpha$ *and* $p < r$, *then* $p - r \in 0^*$, *then* $p = r + (p - r) \in \alpha + 0^*$.

A5 *For every fixed α, we need to find a cut $-\alpha$ that satisfies* $\alpha + (-\alpha) = 0^*$.
Define $\beta = \{p | \exists r > 0, \quad -p - r \notin \alpha\}$, *which means some rational numbers smaller than $-p$ fail to be in α. First, β is a cut.*

property I *If* $s \notin \alpha$, $p = -s - 1$, *then* $-p - 1 = s \notin \alpha$, *then* $p \in \beta$, *which means β is not empty. If* $q \in \alpha$, *then* $-q \notin \beta$. *(If* $-q \in \beta$, *then* $\exists r > 0$, $q - r \notin \alpha$, *this is impossible!). So,* $\beta \neq \mathbb{Q}$.

property II *pick* $p \in \beta$, $\exists r > 0$, $-p - r \notin \alpha$. *If* $q < p$, *then* $-q - r > -p - r$, *this means* $-q - r \notin \alpha$, *so* $q \in \beta$.

property III $t = p + r/2 > p$, *then* $-t - r/2 = -p - r \notin \alpha$, *then* $t \in \beta$.

β *is a cut, then* $\beta \in \mathbb{R}$.

Now we prove $\alpha + \beta = 0^*$

$\Longrightarrow$ $\alpha + \beta \subset 0^*$

$r \in \alpha$, $s \in \beta$, *then* $-s \notin \alpha$, *then* $r < -s$, *this means* $r + s < 0$.

$\Longleftarrow$ $\alpha + \beta \supset 0^*$

pick $v \in 0^*$, $w = -v/2 > 0$, *then* $\exists$ *integer* n *that satisfies* $nw \in \alpha$ *and* $(n+1)w \notin \alpha$, *let* $p = -(n+2)w$, *then* $-p - w = (n+1)w \notin \alpha$, *then* $p \in \beta$, *so* $v = nw + p = -2w \in \alpha + \beta$.

From above, we have $\alpha + \beta = 0^*$, *and we denote* $\beta = -\alpha$.

Step 5 *Since addition axioms hold in* $\mathbb{R}$, *proposition 1.14 also holds in* $\mathbb{R}$. *so, if* α, β, $\gamma \in \mathbb{R}$, *and* $\beta < \gamma$, *then* $\alpha + \beta < \alpha + \gamma$.
Also $\alpha > 0^*$, *then* $-\alpha < 0^*$. *(*$\alpha + 0^* > \alpha + (-\alpha)$*)*

Multiplication is very bothersome than addition in the present context, since we have products of negative rationals are positive. We need to break this problem into many many cases. So, Rudin confined himself to $\mathbb{R}^+$, the set of all $\alpha \in \mathbb{R}$ with $\alpha > 0^*$.

Step 6 *Define* α, $\beta \in \mathbb{R}$, $\alpha\beta = \{p | p \le rs, r \in \alpha, s \in \beta, r > 0, s > 0\}$. $1^* = \{q | q < 1\}$.

M1 $\alpha\beta$ *is a cut*

property I $r_0 \in \alpha$, $s_0 \in \beta$, $r_0 s_0 \in \alpha\beta$, $\alpha\beta$ *is not empty.* $r \notin \alpha$, $s \notin \beta$, $rs > r_0 s_0 \in \alpha\beta$, $rs \notin \alpha\beta$.

property II $rs \in \alpha\beta$, $q \in \mathbb{Q}$, *if* $q < rs$, *then* $q \in \alpha\beta$, *this is trivial.*

property III $p \le rs \in \alpha\beta$, $r < r_1 \in \alpha$, $s < s_1 \in \beta$, $p < r_1 s_1 \in \alpha\beta$.

M2 $\alpha\beta = \{p | p \le rs\} = \{p | p \le sr\} = \beta\alpha$

M3 the same as M2

M4 $1^*\alpha = \alpha$

$\Longrightarrow$ $1^*\alpha \subset \alpha$

$q \in 1^*$, $r \in \alpha$, *then* $q \cdot r < 1 \cdot r \in \alpha$

$\Longleftarrow$ $1^*\alpha \supset \alpha$

r, $p \in \alpha$ *and* $r < p$, *then* $r/p < 1$, *so* $r/p \in 1^*$. *So,* $r = r/p \cdot p \in 1^*\alpha$

M5 if $\alpha \in \mathbb{R}^+$, *then* $\exists 1/\alpha \in \mathbb{R}^+$, *so that* $\alpha \cdot 1/\alpha = 1^*$.

Define $\beta = \{s \in \mathbb{Q} | \exists r \notin \alpha, s.t., s < r^{-1}\}$. *We want to show* $\alpha\beta = 1^*$, *firstly, we prove* β *is a cut.*

property I $\exists r_0 \notin \alpha$ *and* $1/r_0$, *so* $0 < s_0 < 1/r_0$, *so* $s_0 \in \beta$ *and* β *is not empty. If* $0 < p \in \alpha$, *then* $1/p \notin \beta$. *(pick* $1/p \in \beta$, *then* $\exists r \notin \alpha$, *s.t.,* $1/p < 1/r$, *this means* $r < p$ *and* $p \notin \alpha$*). So,* $\beta \neq \mathbb{Q}$.

property II $p \in \beta$, $q \in \mathbb{Q}$ *and* $0 < q < p$, *under* R^+, $\exists r \notin \alpha$, $q < p < 1/r$, *so* $q \in \beta$.

property III $p > 0$, $p \in \beta$, *so* $\exists r \notin \alpha$ *such that* $p < 1/r$, *so* $pr < 1$, *then* $\exists \varepsilon(p,r) < \varepsilon < 1$, $pr \leq 1 \cdot \varepsilon(p,r) < \varepsilon$. *so,* $p < p \cdot 1/\varepsilon < p \cdot 1/\varepsilon(p,r) \leq 1/r$.

So, β *is a cut. Next, we are going to show* $\alpha\beta = 1^*$

$\Longrightarrow$ $\alpha\beta \subset 1^*$

$p \in \alpha$, $q \in \beta$, *then* $\exists r \notin \alpha$ *such that* $q < 1/r$, *by definition,* $r > p$, *so* $pq < pr < 1$.

$\Longleftarrow$ $\alpha\beta \supset 1^*$

For every α, *we can always find* $a \in \alpha$ *and* $\gamma \notin \alpha$. *We set* $a_0 = a$, $b_0 = \gamma$, *then if* $\frac{a_0+b_0}{2} \in \alpha$, *then we set* $a_1 = \frac{a_0+b_0}{2}$, $b_1 = b_0$, *else we set* $a_1 = a_0$ *and* $b_1 = \frac{a_0+b_0}{2}$, *and we keep doing so. This means that we always have one of* a_n *and* b_n *in* α *and the other not. And the distance between* a_n *and* b_n *is less than* $\frac{1}{2^n}$.

We want to prove for every $a \in \alpha$ *and* $b \in \beta$, $ab \geq s$, $s = 1 - \varepsilon$, $\varepsilon > 0$. *Let* $a = a_n$, $b = \frac{1}{b_n} - \varepsilon$. *So,* $a \in \alpha$, $b \in \beta$, *and* $ab = a_n(\frac{1}{b_n} - \varepsilon) > (b_n - \delta)(\frac{1}{b_n} - \varepsilon) > 1 - \varepsilon_0$.

And the second part of definition 1.17 is trivial under $\mathbb{R}^+$.

Step 7 *This step completes the definition of multiplication by setting* $\alpha 0^* = 0^*\alpha = 0^*$.

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

Then we can finish the proof of Step 6, and we skip it. Also distributive law should be divided into cases, and the book has showed a sample proof of one case. We skip this part.

For now, we have fully finish the proof of the existence part of theorem 1.19. And we also need to prove that $\mathbb{Q}$ is a subfield of $\mathbb{R}$.

Step 8 *We connect all rational numbers contained by* $\mathbb{Q}$ *with cuts defined by themselves.*

That is saying, $r^* = \{q | q < r, q \in \mathbb{Q}\}$. *it is easy to show that it is a cut and have all similar propertires.*

Step 9 *in the above step, we connect rational numbers with some cuts, which reserve sums, products, and order, this means* $\mathbb{Q}$ *is isomorphic to the ordered field* $\mathbb{Q}^*$, *they have the same structure and there exists a 1 to 1 mapping or say function from* $\mathbb{Q}$ *to* $\mathbb{Q}^*$. *And this identification of* $\mathbb{Q}$ *with* $\mathbb{Q}^*$ *allows us to regard* $\mathbb{Q}$ *as a subfield of* $\mathbb{R}$