UNIQUENESS OF $\mathbb{R}$ AND CONTAINMENT OF $\mathbb{Q}$

As I mentioned in lecture, we will unfortunately not be able to go over the proof of Theorem 1.19 in lecture. Also, the version I stated is a bit different from the version in the book. The version I presented in lecture is:

Theorem 1.19. *There exists a unique ordered field having the least upperbound property. Moreover, this field contains $\mathbb{Q}$ (up to isomorphism).*

In the book there is an appendix to Chapter 1 that proves existence. The purpose of this post is to discuss uniqueness and also containment of $\mathbb{Q}$.

Note. This is long so its fairly likely I made a few typos in what I wrote. If a detail seems wrong then it might be – feel free to ask in the comments.

Proof of containment. Let F be an ordered field (not necessarily having the least upperbound property). To avoid ambiguity, let's denote the multiplicative identity of F by 1_F and we will let 1 denote the number $1 \in \mathbb{Q}$. Similarly let 0_F denote the additive identify of F.

Define $2_F = 1_F + 1_F$, $3_F = 2_F + 1_F$, etc. Also let -1_F denote the additive inverse of 1_F, let $-2_F = -1_F + -1_F$ denote the additive inverse of 2_F, etc.

Step 1. *Check that $n_F + k_F = (n + k)_F$ for all $n, k \in \mathbb{Z}$.*

Notice that for every integer $n \in \mathbb{Z}$ we have $n_F + 0_F = n_F$ and $n_F + 1_F = (n+1)_F$. Now let $k \geq 1$ be an integer and inductively assume that $n_F + k_F = (n + k)_F$ for every $n \in \mathbb{Z}$. Then for every $n \in \mathbb{Z}$ we have

$$n_F + (k + 1)_F = n_F + k_F + 1_F = (n + k)_F + 1_F = (n + k + 1)_F.$$

By induction, it follows that $n_F + k_F = (n + k)_F$ for all $n \in \mathbb{Z}$ and all integers $k \geq 0$.

Let $k < 0$ be an integer and let $n \in \mathbb{Z}$. By the previous paragraph, $(n + k)_F + (-k)_F = n_F$. Adding k_F to both sides and using the fact that $(-k)_F + k_F = 0_F$, we obtain $(n+k)_F = n_F + k_F$. Thus for all integers $n, k \in \mathbb{Z}$ we have $n_F + k_F = (n+k)_F$.

Step 2. *Check that $n_F \cdot k_F = (n \cdot k)_F$ for all $n, k \in \mathbb{Z}$.*

Since 1_F is the multiplicative identity we have $n_F \cdot 1_F = n_f = (n \cdot 1)_F$ for all $n \in \mathbb{Z}$. Now inductively assume that $k \geq 1$ is an integer with the property that $n_F \cdot k_F = (n \cdot k)_F$ for all $n \in \mathbb{Z}$. Then for every $n \in \mathbb{Z}$ we can apply the conclusion of Step 1 to obtain

$$n_F \cdot (k+1)_F = n_F \cdot (k_F + 1_F) = n_F \cdot k_F + n_F \cdot 1_F = (n \cdot k)_F + n_F = (n \cdot k + n)_F = (n \cdot (k+1))_F.$$

By induction we conclude that $n_F \cdot k_F = (n \cdot k)_F$ for every $n \in \mathbb{Z}$ and $k \in \mathbb{N}$.

Since 0_F is the additive identity we have $n_F \cdot 0_F = 0_F = (n \cdot 0)_F$ for all $n \in \mathbb{Z}$ by Prop. 1.16(a).

From Step 1 it is immediate that $-n_F = (-n)_F$ for all $n \in \mathbb{Z}$. So if $k \geq 1$ is an integer and $n \in \mathbb{Z}$ then we can apply Prop. 1.16(d) and the previous paragraph to obtain

$$n_F \cdot (-k)_F = n_F \cdot (-(k_F)) = -(n_F \cdot k_F) = -(n \cdot k)_F = (-n \cdot k)_F = (n \cdot (-k))_F.$$

We conclude that $n_F \cdot k_F = (n \cdot k)_F$ for all $n, k \in \mathbb{Z}$.

Step 3. *Check that if $m > k$ are integers then $m_F > k_F$. In particular, $m_F \neq k_F$.*

By Prop. 1.18(d) we have $1_F > 0_F$. Adding 1_F to both sides, we obtain $2_F > 1_F > 0_F$ by Definition 1.17(i). In general, if $n \in \mathbb{N}$ and $n_F > 0_F$ then by adding 1_F to both sides we obtain $(n+1)_F > 1_F > 0_F$. It follows from induction that $n_F > 0_F$ for all $n \in \mathbb{N}$. Finally, if $m > k$ are integers then $m - k \in \mathbb{N}$ so the previous sentence implies $m_F - k_F = (m-k)_F > 0_F$ and thus $m_F > k_F$.

Step 4. *Let $a, b, n, m \in \mathbb{Z}$ with $b \neq 0 \neq m$. Check that if $\frac{a}{b} = \frac{n}{m}$ then $\frac{a_F}{b_F} = \frac{n_F}{m_F}$.*

From Step 3 we know that $b_F \neq 0_F \neq m_F$ and thus the multiplicative inverses $\frac{1_F}{b_F}$ and $\frac{1_F}{m_F}$ exist. From $\frac{a}{b} = \frac{n}{m}$ we obtain $a \cdot m = n \cdot b$. So step 2 tells us that

$$a_F \cdot m_F = (a \cdot m)_F = (n \cdot b)_F = n_F \cdot b_F.$$

By looking at the left-most and right-most terms of this equation and dividing everything by $b_F \cdot m_F$ we obtain $\frac{a_F}{b_F} = \frac{n_F}{m_F}$ as desired.

Step 5. *Define an injection $\phi : \mathbb{Q} \to F$ that respects addition, multiplication, and is order-preserving.*

For $p \in \mathbb{Q}$ pick $a, b \in \mathbb{Z}$ satisfying $p = \frac{a}{b}$ and define $\phi(p) = \frac{a_F}{b_F}$. By Step 4, the value of $\phi(p)$ does not depend upon the choice of a and b.

We check ϕ is an injection. Suppose that $\phi(p) = \phi(q)$. Pick $a, b, n, m \in \mathbb{Z}$ satisfying $p = \frac{a}{b}$ and $q = \frac{n}{m}$. Then

$$\frac{a_F}{b_F} = \phi(p) = \phi(q) = \frac{n_F}{m_F}.$$

From clearing denominators and moving everything to the left side we obtain $a_F \cdot m_F - n_F \cdot b_F = 0_F$. Using Steps 1 and 2 we obtain

$$(a \cdot m - n \cdot b)_F = (a \cdot m)_F - (n \cdot b)_F = a_F \cdot m_F - n_F \cdot b_F = 0_F.$$

From Step 3 we conclude that $a \cdot m - n \cdot b = 0$ and hence $p = \frac{a}{b} = \frac{n}{m} = q$. So ϕ is injective.

We check that ϕ is order-preserving. Suppose $p < q$. Again, pick integers a, b, n, m with $p = \frac{a}{b}$, $q = \frac{n}{m}$, and $b, m \geq 1$. From $p < q$ we multiply both sides by the positive quantity $b \cdot m$ to get $a \cdot m < n \cdot b$. From Steps 2 and 3 we obtain

$$a_F \cdot m_F = (a \cdot m)_F < (n \cdot b)_F = n_F \cdot b_F.$$

Also Step 3 tells us that $b_F, m_F > 0_F$, and thus the multiplicative inverses of b_F and m_F are positive by Prop. 1.18(e). So from the above inequality we can divide by $b_F \cdot m_F$ to obtain

$$\phi(p) = \frac{a_F}{b_F} < \frac{n_F}{m_F} = \phi(q).$$

We conclude that ϕ is order-preserving.

We check that ϕ respects addition. Let $p, q \in \mathbb{Q}$. By choosing a common denominator for p and q, we can find $a, b, n \in \mathbb{Z}$ with $p = \frac{a}{b}$ and $q = \frac{n}{b}$. Then $p + q = \frac{a+n}{b}$. Applying Step 1 we obtain

$$\phi(p) + \phi(q) = \frac{a_F}{b_F} + \frac{n_F}{b_F} = \frac{a_F + n_F}{b_F} = \frac{(a+n)_F}{b_F} = \phi(p+q).$$

We check that ϕ respects multiplication. Let $p, q \in \mathbb{Q}$ and let a, b, n, m be integers with $p = \frac{a}{b}$ and $q = \frac{n}{m}$. Then $p \cdot q = \frac{a \cdot n}{b \cdot m}$. Using Step 2 we obtain

$$\phi(p) \cdot \phi(q) = \frac{a_F}{b_F} \cdot \frac{n_F}{m_F} = \frac{a_F \cdot n_F}{b_F \cdot m_F} = \frac{(a \cdot n)_F}{(b \cdot m)_F} = \phi(p \cdot q).$$

We conclude that F contains $\mathbb{Q}$ up to isomorphism. □

Tip. If you want to understand the construction in the Appendix to Chapter 1 but are having difficulty with the intuition, read the first seven paragraphs of the proof below while using your intuitive conception of the real numbers for the field F.

Proof of Uniqueness. Let F be an ordered field having the least upperbound property. By the above, we can assume that $\mathbb{Q}$ is contained in F (up to isomorphism). It suffices to show that F is isomorphic to the ordered field that is constructed in the book in the appendix to Chapter 1. Notice that Theorem 1.20 applies to every ordered field having the least upperbound property; in particular, this theorem applies to F.

Let $\mathbb{R}$ be the set of cuts of $\mathbb{Q}$ as defined in the appendix. Define $\phi : F \to \mathbb{R}$ by setting $\phi(x) = \{p \in \mathbb{Q} : p < x\}$ for $x \in F$. For this defintion to make sense, we need to check that $\phi(x) \subseteq \mathbb{Q}$ is a cut for every $x \in F$. So fix $x \in X$. We will check properties (I), (II), and (III) for being a cut.

(I). Since $1 > 0$ we can apply Theorem 1.20(a) to find $n \in \mathbb{N}$ with $n > x$. Then $n \in \mathbb{Q}$ but $n \notin \phi(x)$, so $\phi(x) \neq \mathbb{Q}$. By the same reasoning we can find $m \in \mathbb{N}$ with $m > -x$ and hence $-m < x$. Then $-m \in \phi(x)$ so $\phi(x) \neq \varnothing$.

(II). This is obvious.

(III). This follows immediately from Theorem 1.20(b).

Thus ϕ indeed maps F into $\mathbb{R}$ as desired. Moreover, if $x < y \in F$ then by Theorem 1.20(b) there is $p \in \mathbb{Q}$ with $x < p < y$ and hence $p \in \phi(y)$ but $p \in \phi(x)$. This shows that $\phi(x) \neq \phi(y)$ whenever $x \neq y$. Thus ϕ is injective.

To see that ϕ is surjective, let $\alpha \in \mathbb{R}$ be a cut. Then $\alpha \subseteq \mathbb{Q}$. Viewing α as a subset of F, we see that α is nonempty and bounded above (indeed, it has an upperbound in $\mathbb{Q} \subseteq F$) and therefore $x = \sup \alpha \in F$ exists since F has the least upperbound property. We claim that $\phi(x) = \alpha$. By definition of supremum and condition (III) of being a cut, every $p \in \alpha$ satisfies $p < x$. Thus $\alpha \subseteq \phi(x)$. On the other hand, if $p \in \phi(x)$ then $p < x$. Since x is the least upperbound to α, it must be that p is not an upperbound to α. So there is $q > p$ with $q \in \alpha$. It follows from clause (II) of being a cut that $p \in \alpha$. Thus $\phi(x) = \alpha$ and ϕ is a bijection.

From the definition of the ordering on $\mathbb{R}$ given in Step 2 in the Appendix, it is easily seen that ϕ is order-preserving.

We check that ϕ respects addition. Recall (as defined in Step 4 in the Appendix) that

$$\phi(x) + \phi(y) = \{p + q : p \in \phi(x),\ q \in \phi(y)\}.$$

Clearly if $p \in \phi(x)$ and $q \in \phi(y)$ then $p < x$ and $q < y$ and hence $p + q < x + y$, implying $p + q \in \phi(x + y)$. Thus $\phi(x) + \phi(y) \subseteq \phi(x + y)$. For the reverse inclusion, consider $t \in \phi(x + y)$. Then $t < x + y$ so $t - y < x$. By Theorem 1.20(b) there is a rational number p with $t - y < p < x$. Notice that $p \in \phi(x)$. From $t - y < p$ we obtain $t - p < y$. Setting $q = t - p$ we have that q is rational and $q \in \phi(y)$. Therefore $t = p + q \in \phi(x) + \phi(y)$. We conclude that $\phi(x + y) = \phi(x) + \phi(y)$.

We check that ϕ respects multiplication. When $x, y \in F$ are positive, we can repeat the same argument from the previous paragraph, but replacing addition with multiplication throughout, to obtain $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$.

Notice that $\phi(-x) = \{p \in \mathbb{Q} : p < -x\} = \{p \in \mathbb{Q} : -p > x\}$. From Theorem 1.20(b) it can be seen that the condition $-p > x$ is equivalent to the condition that there is positive $r \in \mathbb{Q}$ with $-p-r \geq x$, or equivalently $-p-r \notin \phi(x)$. We therefore see that $\phi(-x) = -\phi(x)$ (see Step 4(A5) in the Appendix).

Combining the two above paragraphs with Step 7 in the Appendix and Prop. 1.16(c)(d) we see that $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ for all $x, y \in F$. Thus ϕ respects multiplication.

We conclude that ϕ is an isomorphism of ordered fields. Moreover, from our definition of ϕ and Steps 8 and 9 in the Appendix, we see that ϕ identifies the copy of $\mathbb{Q}$ in F with the copy of $\mathbb{Q}$ in $\mathbb{R}$. We conclude that every ordered field with the least upperbound property is isomorphic to $\mathbb{R}$ (in a manner preserving the respective copies of $\mathbb{Q}$). □