Lecture 12

Alex Hassett
Applied Analysis

June 23, 2025

Definition 11.3 - For Reference. A *cut* is, by definition, 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 $p < r$ for some $r \in \alpha$.

Note that (iii) says that α has no largest member; (ii) implies two facts which can be used freely:

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

If $r \notin \alpha$ and $r < s$, then $s \notin \alpha$.

Theorem 9.21 - Revisited. There exists an ordered field $\mathbb{R}$ which satisfies Axiom 13 (also known as the least-upper-bound property). Moreover, $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield. The members (elements) of $\mathbb{R}$ are called *real numbers.*

Proof. Theorem 9.21 will be proved by constructing $\mathbb{R}$ from $\mathbb{Q}$. We shall divide the construction into several steps. Note that, intuitively, a cut may be thought of the set of all rational numbers less than the real number that corresponds to that cut. For example, the cut for the real number 2 is the set of all rational numbers less than 2. Thus (intuitively) each real number is the set of all rational numbers less than it and $\mathbb{R}$ is the set of all cuts of $\mathbb{Q}$.

Step 1. The members of $\mathbb{R}$ will be certain subsets of $\mathbb{Q}$, called *cuts.* In this proof the letters $p, q, r, \ldots$ will always denote rational numbers, and $\alpha, \beta, \gamma, \ldots$ will denote cuts.

Step 2. Define "$\alpha < \beta$" to mean: α is a proper subset of β. Let us check that this meets the requirements of Definition 7.15. If $\alpha < \beta$ and $\beta < \gamma$ it is clear that $\alpha < \gamma$ (a proper subset of a proper subset is a proper subset). It is also clear that at most one of the three relations

$$\alpha < \beta, \qquad \alpha = \beta, \qquad \beta < \alpha$$

can hold for any pair α, β. To show that at least one holds, assume that the first two fail. Then α is not a subset of β. Hence there exists a $p \in \alpha$ with $p \notin \beta$. If $q \in \beta$, then it follows that $q < p$ (since $p \notin \beta$), hence $q \in \alpha$ by (ii) of Definition 11.3. Thus $\beta \subset \alpha$. Since $\beta \neq \alpha$, we conclude that $\beta < \alpha$. Thus $\mathbb{R}$ is now an ordered set.

Step 3. The ordered set $\mathbb{R}$ has the least-upper-bound property. To prove this, let A be a nonempty subset of $\mathbb{R}$, and assume that $\beta \in \mathbb{R}$ is an upper bound of A. Define γ to be the union of all $\alpha \in A$ (i.e. $\gamma = \cup_{\alpha \in A} \alpha$). In other words, $p \in \gamma$ if and only if $p \in \alpha$ for some $\alpha \in A$. We shall prove that $\gamma \in \mathbb{R}$ and that $\gamma = \sup A$. Since A is not empty, there exists an $\alpha_0 \in A$. This α_0 is not empty. Since $\alpha_0 \subset \gamma$, we have that γ is not empty. Next, $\gamma \subset \beta$ (since $\alpha \subset \beta$ for every $\alpha \in A$), and therefore $\gamma \neq \mathbb{Q}$. Thus γ satisfies property (i). To prove (ii) and (iii), pick $p \in \gamma$. Then $p \in \alpha_1$ for some $\alpha_1 \in A$. If $q < p$, then $q \in \alpha_1$, hence $q \in \gamma$; this proves (ii). If $r \in \alpha_1$ is so chosen that $r > p$, we see that $r \in \gamma$ (since $\alpha_1 \subset \gamma$), and therefore γ satisfies (iii). Thus $\gamma \in \mathbb{R}$. It is clear that $\alpha \leq \gamma$ for every $\alpha \in A$. Suppose $\delta < \gamma$. Then there exists an $s \in \gamma$ such that $s \notin \delta$. Since $s \in \gamma$, we have that $s \in \alpha$ for some $\alpha \in A$. Hence $\delta < \alpha$, and δ is not an upper bound of A. This gives the desired result: $\gamma = \sup A$.

Step 4. If $\alpha \in \mathbb{R}$ and $\beta \in \mathbb{R}$, then we define $\alpha+\beta$ to be the set of all sums $r+s$, where $r \in \alpha$ and $s \in \beta$, i.e.

$$\alpha + \beta = \{\, r + s \mid r \in \alpha \text{ and } s \in \beta \,\}.$$

We define 0^* to be the set of all negative rational numbers. It is clear that 0^* is a cut. We verify that the axioms for addition hold in $\mathbb{R}$, with 0^* playing the role of 0.

(A1) We have to show that $\alpha+\beta$ is a cut. It is clear that $\alpha+\beta$ is a nonempty subset of $\mathbb{Q}$. Take $r' \notin \alpha$ and $s' \notin \beta$. Then $r'+s' > r+s$ for all choices of $r \in \alpha, s \in \beta$. Thus $r'+s' \notin \alpha+\beta$. It follows that $\alpha+\beta$ has property (i). Pick $p \in \alpha+\beta$. Then $p = r+s$, with $r \in \alpha$, $s \in \beta$. Thus (ii) holds. Choose $t \in \alpha$ so that $t > r$. Then $p < t+s$ and $t+s \in \alpha+\beta$. Thus (iii) holds.

(A2) $\alpha+\beta$ 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 $s+r$. Since $r+s = s+r$ for all $r \in \mathbb{Q}, s \in \mathbb{Q}$, we have $\alpha+\beta = \beta+\alpha$.

(A3) As above, this follows from the associative law in $\mathbb{Q}$.

(A4) If $r \in \alpha$ and $s \in 0^*$, then $r+s < r$, hence $r+s \in \alpha$. Thus $\alpha + 0^* \subset \alpha$. To obtain the opposite inclusion, pick $p \in \alpha$, and pick $r \in \alpha$ such that $r > p$. Then $p-r \in 0^*$, and $p = r+(p-r) \in \alpha+0^*$. Thus $\alpha \subset \alpha + 0^*$. We conclude that $\alpha + 0^* = \alpha$.

(A5) Fix $\alpha \in \mathbb{R}$. Let β be the set of all p with the following property: there exists $r > 0$ such that $-p-r \notin \alpha$, i.e.

$$\beta = \{\, p \mid \exists r \in \mathbb{Q} \text{ such that } -p-r \notin \alpha \,\}.$$

In other words, some rational number smaller than $-p$ fails to be in α. We show that $\beta \in \mathbb{R}$ and that $\alpha+\beta = 0^*$. If $s \notin \alpha$ and $p = -s-1$, then $-p-1 \notin \alpha$, hence $p \in \beta$. So β is not empty. If $q \notin \alpha$, then $-q \notin \beta$. So $\beta \neq \mathbb{Q}$. Hence β satisfies (i). Pick $p \in \beta$, and pick $r > 0$, so that $-p-r \notin \alpha$. Thus $q \in \beta$, and (ii) holds. Put $t = p + \frac{r}{2}$. Then $t > p$, and $-t - \frac{r}{2} = -p-r \notin \alpha$, so that $t \in \beta$. Hence β satisfies (iii). We have proved that $\beta \in \mathbb{R}$. If $r \in \alpha$ and $s \in \beta$, then $-s \notin \alpha$, hence $r < -s$, $r+s < 0$. Thus $\alpha+\beta \subset 0^*$. To prove the opposite inclusion, pick $v \in 0^*$, put $w = -\frac{v}{2}$. Then $w > 0$, and there is an integer n such that $nw \in \alpha$ but $(n+1)w \notin \alpha$ (note that this depends on the fact that $\mathbb{Q}$ has the archimedean property - see Theorem 10.7). Put $p = -(n+2)w$. Then $p \in \beta$, since $-p-w \notin \alpha$, and

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

Thus $0^* \subset \alpha+\beta$. We conclude that $\alpha+\beta = 0^*$. This β will, of course, be denoted by $-\alpha$.

Step 5. Having proved that the addition defined in Step 4 satisfies Axioms (A) of Definition 7.14, it follows that the properties of addition proved in Lecture 9 are valid in $\mathbb{R}$, and we can prove one of the requirements of Definition 7.16:

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

Indeed, it is obvious from the definition of $+$ in $\mathbb{R}$ that $\alpha+\beta \subset \alpha+\gamma$; if we had $\alpha+\beta = \alpha+\gamma$, the cancellation law (Theorem 9.15) would imply that $\beta = \gamma$. It also follows that $\alpha > 0^*$ if and only if $-\alpha < 0^*$.

Step 6. Multiplication is a little more bothersome than addition in the present context, since products of negative rationals are positive. For this reason we confine ourselves first to $\mathbb{R}^+$, the set of all $\alpha \in \mathbb{R}$ with $\alpha > 0^*$. If $\alpha \in \mathbb{R}^+$ and $\beta \in \mathbb{R}^+$, then we define $\alpha\beta$ to be the set of all p such that $p \leq rs$ for some choice of $r \in \alpha, s \in \beta, r > 0, s > 0$. We define 1^* to be the set of all $q < 1$. Then the axioms (M) and (D) of Definition 7.14 hold, with $\mathbb{R}^+$ in place of F, and with 1^* in the role of 1. The proofs are so similar to the ones given in detail in Step 4 that we omit them. Note, in particular, that requirement (ii) of Definition 9.20 holds:

$$\text{If } \alpha > 0^* \text{ and } \beta > 0^*, \text{ then } \alpha\beta > 0^*.$$

Step 7. We complete the definition of multiplication by setting $\alpha 0^* = 0^*\alpha = 0^*$, and by setting

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

The products on the right were defined in Step 6. Having proved (in Step 6) that the axioms (M) hold in $\mathbb{R}^+$, it is now perfectly simple to prove them in R, by repeated application of the identity $\gamma = -(-\gamma)$. The proof of the distributive law breaks into cases. For instance, suppose $\alpha > 0^*$, $\beta < 0^*$, $\beta + \gamma > 0^*$. Then $\gamma = (\beta + \gamma) + (-\beta)$, and since we already know that the distributive law holds in $\mathbb{R}^+$, we have

$$\alpha\gamma = \alpha(\beta + \gamma) + \alpha \cdot (-\beta).$$

But $\alpha \cdot (-\beta) = -(\alpha\beta)$. Thus

$$\alpha\beta + \alpha\gamma = \alpha(\beta + \gamma).$$

The other cases are handled in the same way. We have now completed the proof that $\mathbb{R}$ is an ordered field with the least-upper-bound property.

Step 8. We associate with each $r \in \mathbb{Q}$ the set r^* which consists of all $p \in \mathbb{Q}$ such that $p < r$, i.e.

$$r^* = \{\, p \in \mathbb{Q} \mid p < r \,\}.$$

It is clear that each r^* is a cut; that is, $r^* \in \mathbb{R}$. These cuts satisfy the following relations:

(a) $r^* + s^* = (r + s)^*$,

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

(c) $r^* < s^*$ if and only if $r < s$.

To prove (a), choose $p \in r^* + s^*$. Then $p = u + v$, where $u < r, v < s$. Hence $p < r + s$, which says that $p \in (r + s)^*$. Conversely, suppose $p \in (r + s)^*$. Then $p < r + s$. Choose t so that $2t = r + s - p$, put

$$r' = r - t, \qquad s' = s - t.$$

Then $r' \in r^*$, $s' \in s^*$, and $p = r' + s'$, so that $p \in r^* + s^*$. This proves (a). The proof of (b) is similar. If $r < s$, then $r \in s^*$, but $r \notin r^*$; hence $r^* < s^*$. If $r^* < s^*$, then there exists a $p \in s^*$ such that $p \notin r^*$. Hence $r \leq p < s$, so that $r < s$. This proves (c).

Step 9. We saw in Step 8 that the replacement of the rational numbers r by the corresponding "rational cuts" $r^* \in \mathbb{R}$ preserves sums, products, and order. This fact may be expressed by saying that the ordered field $\mathbb{Q}$ is *isomorphic* to the ordered field $\mathbb{Q}^*$ whose elements are the rational cuts. Of course, r^* is by no means the same as r, but the properties we are concerned with (arithmetic and order) are the same in the two fields. It is this identification of $\mathbb{Q}$ with $\mathbb{Q}^*$ which allows us to regard $\mathbb{Q}$ as a subfield of $\mathbb{R}$. This is also proven by Theorem 11.1, which states that any two ordered fields with the least-upper-bound property are isomorphic.

□

Remark 12.1. A common notation for the set of all nonnegative real numbers is $\mathbb{R}_{\geq 0}$. Note that the set of all nonnegative real numbers is defined as

$$\mathbb{R}_{\geq 0} = \{\, x \in \mathbb{R} \mid x \geq 0 \,\}.$$

The set of all positive real numbers $\mathbb{R}^+$ is defined as

$$\mathbb{R}^+ = \{\, x \in \mathbb{R} \mid x > 0 \,\}.$$