Construction of $\mathbb{R}$ from $\mathbb{Q}$ via Dedekind cuts

Contents

The following is mostly paraphrased from the appendix to Chapter 1 of [PMA], with some details filled in and some changes to notation.

1 Construction of $\mathbb{R}$ from $\mathbb{Q}$ via Dedekind cuts

Our aim is to prove the following theorem.

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.

We will assume that $\mathbb{Q}$ has already been constructed from the integers and is known to be an ordered field.

1.1 Defining $\mathbb{R}$

Let A be a subset of $\mathbb{Q}$. Then A is a **Dedekind cut** if it satisfies the following four properties:

(I) A is non-empty;

(II) $A \neq \mathbb{Q}$;

(III) if $p \in A$, $q \in \mathbb{Q}$, and $q < p$, then $q \in A$ (this property is sometimes known as being "closed downwards");

(IV) if $p \in A$, then $p < r$ for some $r \in A$ (in other words, A has no greatest element).

We define $\mathbb{R}$ to be the set of all Dedekind cuts; we will refer to elements of $\mathbb{R}$ as Dedekind cuts or (perhaps prematurely) as real numbers. For any given rational number q, one can verify that the set $\{p \in \mathbb{Q} : p < q\}$ is a Dedekind cut, so that our definition is non-empty. (In fact, this collection of Dedekind cuts will be the subfield $\mathbb{Q}$ inside of $\mathbb{R}$. We will make this more precise in Section 1.6.)

Remark. In general, we will use uppercase letters $A, B, C, \ldots$ to refer to Dedekind cuts and lowercase letters $p, q, r, s, \ldots$ to refer to rational numbers.

1.2 Ordering $\mathbb{R}$

For $A, B \in \mathbb{R}$ (that is, for Dedekind cuts A and B), we define $A < B$ to mean that A is a proper subset of B and $A \leq B$ to mean that $A < B$ or $A = B$; clearly these two are mutually exclusive (we are essentially using the symbol $\leq$ in place of $\subseteq$). We claim that $\leq$ is a total order on $\mathbb{R}$. For all $A, B, C \in \mathbb{R}$, we must verify the following four properties:

(O1) $A \le A$ (**reflexivity**). This certainly holds.

(O2) $A \le B$ and $B \le A$ implies that $A = B$ (**antisymmetry**). A and B cannot both be proper subsets of each other, so if $A \le B$ and $B \le A$ then it must be the case that $A = B$.

(O3) $A \le B$ and $B \le C$ implies that $A \le C$ (**transitivity**). The only interesting case is when each inequality is strict; in that case, transitivity holds since a proper subset of a proper subset is a proper subset.

(O4) $A \le B$ or $B \le A$ (**comparibility**, or the **trichotomy law**). Note that this does not hold for arbitrary sets; we will have to use the properties of Dedekind cuts. It will suffice to show that if A is not a proper subset of B and $A \ne B$, then B is a proper subset of A. Assuming therefore that A is not a subset of B, there must exist some $q \in A$ such that $q \notin B$. Let p be any element of B. We cannot have $p = q$ since $q \notin B$, and $p > q$ would violate property (III), so we must have $p < q$. It then follows from property (III) that $p \in A$. So B is a subset of A but by assumption is not equal to it, i.e. B is a proper subset of A.

1.3 $\mathbb{R}$ has the least-upper-bound property

We will now show that $\mathbb{R}$ with this total ordering has the least-upper-bound property. Let E be a non-empty subset of $\mathbb{R}$ which is bounded above by some $B \in \mathbb{R}$, i.e. for each $A \in E$, A is a subset of B. We must show that such an E always has a supremum in $\mathbb{R}$. Let C be the union of all $A \in E$; our claim is that C is the supremum of E. To see this, we need to show the following:

(S1) $C \in \mathbb{R}$, i.e. C is a Dedekind cut. We shall verify properties (I) - (IV).

- (I) Since E is non-empty, there exists some $A_0 \in E$ which is a Dedekind cut and hence non-empty. Any $A \in E$ is a subset of C, so C has a non-empty subset and hence must be non-empty itself.
- (II) C must be a subset of B since each $A \in E$ is a subset of B. Since B is a Dedekind cut, we have $B \ne \mathbb{Q}$; it follows that $C \ne \mathbb{Q}$.
- (III) Suppose $p \in C, q \in \mathbb{Q}$, and $q < p$. Then there exists some $A_0 \in E$ such that $p \in A_0$. Since A_0 is a Dedekind cut, property (III) implies that $q \in A_0$, from which it follows that $q \in C$.
- (IV) Suppose $p \in C$. Then there exists some $A_0 \in E$ such that $p \in A_0$. Since A_0 is a Dedekind cut, property (IV) implies that there is some $r \in A_0$, which must also belong to C, with $p < r$.

(S2) C is an upper bound of E. This certainly holds, since any $A \in E$ is a subset of the union of all such A.

(S3) C is the least upper bound of E. To see this, let $D \in \mathbb{R}$ be such that $D < C$. Then there must exist some $p \in C$ such that $p \notin D$. Since $p \in C$, there is an $A_0 \in E$ such that $p \in A_0$. Suppose $q \in D$. Then it cannot be the case that $q > p$, otherwise property (III) would imply that $p \in D$, and it cannot be the case that $q = p$, since $p \notin D$. So we must have $q < p$, which implies by property (III) that $q \in A_0$. Hence D is a subset of A_0. In fact, $D < A_0$ since p belongs to A_0 but not to D, so that D cannot possibly be an upper bound of E. It follows that C is the least upper bound of E.

1.4 Addition in $\mathbb{R}$

So far, we have an ordered set $\mathbb{R}$ with the least-upper-bound property. We will now define the field structure of $\mathbb{R}$, starting with addition. For $A, B \in \mathbb{R}$, define

$$A + B = \{r + s : r \in A, s \in B\}.$$

We will show that with this definition of addition, the five field axioms for addition hold for all $A, B, C \in \mathbb{R}$:

(A1) $A + B \in \mathbb{R}$ (**closure**). In other words, we need to show that $A + B$ is a Dedekind cut. We shall verify properties (I) - (IV).

- (I) $A + B$ is non-empty since A and B are non-empty.
- (II) Neither A nor B contains every rational number, so there exist $p, q \in \mathbb{Q}$ such that $p \notin A$ and $q \notin B$. Then for any $r \in A$ and $s \in B$, property (III) gives us $r < p$ and $s < q$; it follows that $r + s < p + q$, so that $p + q$ is greater than any element of $A + B$ and hence cannot belong to it. We conclude that $A + B \neq \mathbb{Q}$.
- (III) Suppose $r + s \in A + B$, $q \in \mathbb{Q}$, and $q < r + s$. Then $q - s < r$ and so property (III) gives us $q - s \in A$. Hence $q = (q - s) + s$ belongs to $A + B$.
- (IV) Suppose $r + s \in A + B$. Property (IV) implies that there exists $p \in A$ such that $r < p$. It follows that $p + s \in A + B$ and that $r + s < p + s$.

(A2) $A + B = B + A$ (**commutativity**). This follows from commutativity of addition in $\mathbb{Q}$.

(A3) $(A + B) + C = A + (B + C)$ (**associativity**). This follows from associativity of addition in $\mathbb{Q}$.

(A4) There exists an element $0 \in \mathbb{R}$ such that $A + 0 = A$ (**additive identity**). Let 0^* be the set of all negative rational numbers (we are using the notation 0^* to avoid confusion with $0 \in \mathbb{Q}$). As noted in Section 1.1, sets of the form $\{p \in \mathbb{Q} : p < q\}$ for a given rational number q are Dedekind cuts, so we have $0^* \in \mathbb{R}$. We claim that 0^* is the additive identity in $\mathbb{R}$. For the inclusion $A + 0^* \subseteq A$, suppose $r \in A$ and $s \in 0^*$, i.e. $s \in \mathbb{Q}$ with $s < 0$. Then $r + s < r$ and so property (III) implies that $r + s \in A$. For the reverse inclusion $A \subseteq A + 0^*$, suppose $r \in A$. Property (IV) implies that there exists $s \in A$ such that $r - s < 0$; it follows that $r = s + (r - s)$ belongs to $A + 0^*$. Hence $A \subseteq A + 0^*$ and we conclude that $A + 0^* = A$.

(A5) There exists an element $-A \in \mathbb{R}$ such that $A + (-A) = 0^*$ (**additive inverse**). We define our candidate for the additive inverse of A as

$$-A = \{p \in \mathbb{Q} : \text{there exists an } r > 0 \text{ such that } -p - r \notin A\}.$$

First, we will show that $-A$ belongs to $\mathbb{R}$ by verifying properties (I) - (IV).

(I) Since $A \neq \mathbb{Q}$, there is a rational number $p \notin A$. By property (III), we must have $p + 1 = -(-p - 2) - 1 \notin A$. Hence $-p - 2 \in -A$, so that $-A$ is non-empty.

(II) For any $p \in A$, property (III) implies that $p - r \in A$ for any $r > 0$; this is exactly the statement that $-p \notin -A$. It follows that $-A \neq \mathbb{Q}$ since A is non-empty.

(III) Suppose $p \in -A$, $q \in \mathbb{Q}$, and $q < p$. Then there is an $r > 0$ such that $-p - r \notin A$, and the inequality $q < p$ implies that $-q - r > -p - r$. By property (III) we must have $-q - r \notin A$, whence $q \in -A$.

(IV) Suppose $p \in -A$, i.e. there is an $r > 0$ such that $-p - r \notin A$. Then $p + \frac{r}{2} > p$ also belongs to $-A$, since $-p - r = -\left(p + \frac{r}{2}\right) - \frac{r}{2} \notin A$.

Next, we will show that $A + (-A) = 0^*$. For the inclusion $A + (-A) \subseteq 0^*$, suppose $r \in A$ and $s \in -A$, so that there is a $u > 0$ such that $-s - u \notin A$. Property (III) implies that $r - u \in A$, and furthermore that $r - u < -s - u$; it follows that $r + s < 0$, i.e. $r + s \in 0^*$. For the reverse inclusion $0^* \subseteq A + (-A)$, suppose that $r \in 0^*$, i.e. r is a negative rational number. We claim that there must exist some $p \in A$ such that $p - \frac{r}{2} \notin A$. To see this, suppose by way of contradiction that $p - \frac{r}{2} \in A$ for all $p \in A$. An induction argument then gives $p - \frac{nr}{2} \in A$ for all $p \in A$ and all positive integers n. Let $q \in \mathbb{Q}$ be given. Since $-\frac{r}{2} > 0$, we may invoke the Archimedean property of $\mathbb{Q}$ to obtain a positive integer N such that $p - \frac{Nr}{2} > q$; but since $p - \frac{Nr}{2} \in A$, property (III) gives $q \in A$. Since q was arbitrary, the conclusion is that $A = \mathbb{Q}$, which is a contradiction. Hence there must exist a $p \in A$ such that $p - \frac{r}{2} \notin A$. This implies that $r - p \in -A$, since $-(r - p) - (-\frac{r}{2}) = p - \frac{r}{2} \notin A$, and it follows that $r = p + (r - p)$ belongs to $A + (-A)$. We conclude that $0^* \subseteq A + (-A)$ and hence that $A + (-A) = 0^*$.

Now that we have shown that addition in $\mathbb{R}$ satisfies the field axioms for addition, we can present the following theorem, given without proof (see, for example, Proposition 1.14 of [PMA]). It contains four statements which are true in any set with a definition of addition which satisfies the field axioms for addition, although we state them in particular for $\mathbb{R}$.

Theorem 2. For all $A, B, C \in \mathbb{R}$, the following statements hold.

(a) If $A + B = A + C$ then $B = C$.

(b) If $A + B = A$ then $B = 0^*$.

(c) If $A + B = 0^*$ then $B = -A$.

(d) $-(-A) = A$.

Part (a) of Theorem 2 allows us to prove the following statement, which is the first requirement for $\mathbb{R}$ to be an **ordered field**:

(OF1) For all $A, B, C \in \mathbb{R}$, $B < C \implies A + B < A + C$.

Indeed, for any $r \in A$ and $s \in B$ we also have $s \in C$, so that $r + s \in A + C$. Hence $A + B$ is a subset of $A + C$, and $A + B \neq A + C$ follows from the contrapositive of part (a) of Theorem 2.

1.5 Multiplication in $\mathbb{R}$

To complete the field structure of $\mathbb{R}$, we need to define multiplication of real numbers; this is somewhat more involved than addition. Let $\mathbb{R}_+ = \{A \in \mathbb{R} : 0^* < A\}$, i.e. the set of those Dedekind cuts which contain the negative rational numbers as a strict subset. We will first define multiplication of elements in $\mathbb{R}_+$, show that this definition satisfies the five field axioms for multiplication (with a slight change to the statement on multiplicative inverses; we need not consider 0^* since it does not belong to $\mathbb{R}_+$), and then extend our definition to all of $\mathbb{R}$. For $A, B \in \mathbb{R}_+$, define

$$AB = \{p \in \mathbb{Q} : p \leq rs \text{ for some choice of } r \in A, s \in B, r > 0, s > 0\}.$$

(M1) $AB \in \mathbb{R}_+$ (**closure**). First, let us show that AB is a Dedekind cut by verifying properties (I) - (IV).

(I) Note that A must contain some non-negative rational number r since 0^* is a strict subset of A, and furthermore we may assume that r is positive by invoking property (IV) if necessary. So we can always find positive rationals $r \in A, s \in B$, and there are certainly rational numbers less than rs; it follows that AB is non-empty.

(II) Since A and B are not equal to $\mathbb{Q}$, there exist rationals $u \notin A$ and $v \notin B$. For any choice of positive rationals $r \in A$ and $s \in B$, property (III) implies that $r < u$ and $s < v$, from which we obtain $rs < uv$. It follows that $uv \notin AB$ since

$$(AB)^{\mathsf{C}} = \{p \in \mathbb{Q} : p > rs \text{ for all choices of } r \in A, s \in B, r > 0, s > 0\}.$$

Hence $AB \neq \mathbb{Q}$.

(III) Suppose $p \in AB, q \in \mathbb{Q}$, and $q < p$; it immediately follows that $q \in AB$.

(IV) Suppose $p \in AB$, so that $p \leq rs$ for some choice of $r \in A, s \in B, r > 0, s > 0$. Property (IV) implies that there is a $q \in A$ with $0 < r < q$, which gives $rs < qs$. Then $p < qs$ and $qs \in AB$.

Now let us show that $0^* < AB$. As noted above, we can always find positive rationals $r \in A, s \in B$, and it is certainly the case that all non-positive rational numbers p satisfy $p \leq rs$; it follows that 0^* is a strict subset of AB. This also proves that $\mathbb{R}$ satisfies the second and last requirement to be an ordered field:

(OF2) For all $A, B \in \mathbb{R}$, $A > 0^*$ and $B > 0^* \implies AB > 0^*$.

(We showed that $\mathbb{R}$ satisfies the first requirement to be an ordered field at the end of Section 1.4; once we have finished defining multiplication on $\mathbb{R}$ and verifying the field axioms for multiplication and distributivity, it will follow that $\mathbb{R}$ is an ordered field.)

(M2) $AB = BA$ (**commutativity**). This follows from commutativity of multiplication in $\mathbb{Q}$; one has $p \leq rs \iff p \leq sr$.

(M3) $(AB)C = A(BC)$ (**associativity**). Suppose $p \in (AB)C$, i.e. $p \leq rs$ for some choice of $r \in AB, s \in C, r > 0, s > 0$. Then $r \leq uv$ for some choice of $u \in A, v \in B, u > 0, v > 0$, so that $p \leq uvs$. But note that $vs \in BC$, so that $p \in A(BC)$. The reverse inclusion is similar. (We have of course used that multiplication in $\mathbb{Q}$ is associative.)

(M4) There exists an element $1 \in \mathbb{R}_+$ such that $1A = A$ (**multiplicative identity**). Let 1^* be the set of all rational numbers less than 1; it is clear that $1^* \in \mathbb{R}_+$ (again, we are using the notation 1^* to avoid confusion with $1 \in \mathbb{Q}$). We claim that 1^* is the multiplicative identity in $\mathbb{R}_+$. For the inclusion $1^*A \subseteq A$, suppose that $p \in 1^*A$, so that $p \leq rs$ for some $0 < r < 1$ and $s \in A$ with $s > 0$. It follows that $p < s$, and property (III) then implies that $p \in A$. For the reverse inclusion $A \subseteq 1^*A$, suppose $p \in A$. Combining property (IV) with the fact that $A > 0^*$, we see that there is an $s \in A$ such that $s > 0$ and $s > p$. It follows that $0 < 1 - \frac{p}{s}$. Using the Archimedean property of $\mathbb{Q}$, let N be a positive integer such that $\frac{1}{N+1} \leq 1 - \frac{p}{s}$. After some algebra, we obtain $p \leq \frac{N}{N+1}s$. Since $0 < \frac{N}{N+1} < 1$, it follows that $p \in 1^*A$.

(M5) There exists an element $A^{-1} \in \mathbb{R}_+$ such that $AA^{-1} = 1^*$ (**multiplicative inverse**). Let

$$A^{-1} = \{p \in \mathbb{Q} : p \leq 0 \text{ or there exists } r > 0 \text{ such that } \tfrac{1}{p} - r \notin A\}.$$

We claim that A^{-1} is the multiplicative inverse to A. First, we will show that A^{-1} is a Dedekind cut by verifying properties (I) - (IV).

(I) A^{-1} contains all non-positive rational numbers, so certainly it is non-empty.

(II) We have

$$\left(A^{-1}\right)^{\mathsf{C}} = \{p \in \mathbb{Q} : p > 0 \text{ and } \tfrac{1}{p} - r \in A \text{ for all } r > 0\}.$$

Since $A \in \mathbb{R}_+$, there exists $p \in A$ with $p > 0$. It follows from property (III) that $p - r \in A$ for all $r > 0$, and $\frac{1}{p} > 0$, so $\frac{1}{p} \notin A^{-1}$. Hence $A^{-1} \neq \mathbb{Q}$.

(III) Suppose $p \in A^{-1}, q \in \mathbb{Q}$, and $q < p$. If $q \leq 0$ then $q \in A^{-1}$, so suppose $q > 0$. Then $p > 0$, so there must be some $r > 0$ such that $\frac{1}{p} - r \notin A$. Observe that

$$0 < q < p \iff 0 < \tfrac{1}{p} - r < \tfrac{1}{q} - r.$$

It follows from property (III) that $\frac{1}{q} - r \notin A$, so that $q \in A^{-1}$.

(IV) First, note that there exists $u \notin A$ with $u > 0$ (this is true of any Dedekind cut; if this were not the case, then the Dedekind cut would be the entire rational line). It follows that $\frac{1}{2u} \in A^{-1}$, since $2u - u = u \notin A$. So A^{-1} always contains positive rational numbers. Now suppose that $p \in A^{-1}$. If $p \leq 0$, then by the above we can always find a positive $q \in A^{-1}$ with $p < q$. Suppose therefore that $p > 0$, so that there exists an $r > 0$ such that $\frac{1}{p} - r \notin A$. Let $q = \frac{1}{p} - \frac{r}{2}$. Since $A \in \mathbb{R}_+$, it must be the case that $\frac{1}{p} - r > 0$. Observe that

$$0 < \tfrac{1}{p} - r < q < \tfrac{1}{p} \implies 0 < p < \tfrac{1}{q}.$$

It follows that $\frac{1}{q} \in A^{-1}$, since $q - \frac{r}{2} = \frac{1}{p} - r \notin A$, and $p < \frac{1}{q}$.

Since A^{-1} contains all non-positive rationals, we have $A^{-1} > 0^*$. So we have shown that $A^{-1} \in \mathbb{R}_+$; now we need to show that $AA^{-1} = 1^*$. For the inclusion $AA^{-1} \subseteq 1^*$, suppose $p \in AA^{-1}$, i.e. $p \leq rs$ for some choice of $r \in A, s \in A^{-1}, r > 0, s > 0$. Then there exists some $u > 0$ such that $\frac{1}{s} - u \notin A$. Property (III) implies that $\frac{1}{s} \notin A$, and furthermore that $r < \frac{1}{s}$. It follows that $p \leq rs < 1$, so that $p \in 1^*$. For the reverse inclusion $1^* \subseteq AA^{-1}$, suppose $p \in 1^*$. If $p \leq 0$, then any choice of positive $r \in A$ and $s \in A^{-1}$ will do (as noted before, A and A^{-1} always contain positive rational numbers). Suppose therefore that $0 < p < 1$. By the Archimedean property of $\mathbb{Q}$, there exists a positive integer n such that

$$p < 1 - \tfrac{1}{m+1} = \tfrac{m}{m+1} \tag{$*$}$$

for all integers $m \geq n$. Let r be any positive rational number in A, and let $q = \frac{r}{2n}$, so that $0 < q < \frac{r}{n}$; property (III) implies that both q and $nq \in A$. Now we claim the following:

$$\text{there exists a positive integer } m \text{ such that } mq \in A \text{ and } (m+1)q \notin A.$$

To see this, suppose by way of contradiction that the negation of this statement holds:

$$\text{for all positive integers } m, \text{either } mq \notin A \text{ or } (m+1)q \in A.$$

Since $q \in A$, it follows from the negated statement that $2q \in A$. Proceeding by induction, we obtain $mq \in A$ for all positive integers m. Now let $u \in \mathbb{Q}$ be given. By the Archimedean property of $\mathbb{Q}$, there is a positive integer M such that $Mq > u$. Property (III) then implies that $u \in A$. We conclude that $A = \mathbb{Q}$, which contradicts property (II) of Dedekind cuts. Hence there must be some positive integer m such that $mq \in A$ and $(m+1)q \notin A$. Since $nq \in A$, property (III) gives us $nq < (m+1)q$. It follows that $n \leq m$, so that inequality $(*)$ holds for this m. Then observe that

$$0 < p < \tfrac{m}{m+1} \implies 0 < \tfrac{p}{mq} < \tfrac{1}{(m+1)q} \implies 0 < (m+1)q < \tfrac{mq}{p} \implies 0 < \tfrac{mq}{p} - (m+1)q.$$

Hence $\frac{p}{mq} \in A^{-1}$, since $(m+1)q = \frac{mq}{p} - (\frac{mq}{p} - (m+1)q) \notin A$. It follows that $p \in AA^{-1}$, since $p = mq \cdot \frac{p}{mq}$. We conclude that $1^* \subseteq AA^{-1}$ and hence that $AA^{-1} = 1^*$.

We will now show that multiplication distributes over addition in $\mathbb{R}_+$, i.e. for all $A, B, C \in \mathbb{R}_+$, we have $A(B+C) = AB + AC$. For the inclusion $A(B+C) \subseteq AB + AC$, let $p \in A(B+C)$ be given, so that $p \leq rs$ for some choice of $r \in A, s \in B + C, r > 0, s > 0$. Then s is of the form $u + v$ for some $u \in B$ and $v \in C$. Since $B, C > 0^*$, there exist positive rational numbers $u' \in B$ and $v' \in C$ such that $u \leq u'$ and $v \leq v'$. We then have

$$p \leq rs = r(u+v) = ru + rv \leq ru' + rv'.$$

The sum $ru' + rv'$ belongs to $AB + AC$, which we have shown is a Dedekind cut in (A1) and (M1). It follows from property (III) that $p \in AB + AC$. For the reverse inclusion $AB + AC \subseteq A(B+C)$, suppose $p + q \in AB + AC$, i.e.

$$\begin{aligned} p &\leq r_1 s_1 \text{ for some } r_1 \in A, s_1 \in B, r_1 > 0, s_1 > 0, \\ q &\leq r_2 s_2 \text{ for some } r_2 \in A, s_2 \in C, r_2 > 0, s_2 > 0. \end{aligned}$$

Let $r = \max\{r_1, r_2\}$. Then $r \in A, r > 0$, and $p+q \leq r_1 s_1 + r_2 s_2 \leq r(s_1+s_2)$. Since $s_1+s_2 \in B+C$ and $s_1 + s_2 > 0$, it follows that $p+q \in A(B+C)$. We conclude that $AB + AC \subseteq A(B+C)$ and hence that $A(B+C) = AB + AC$.

We are now in a position to define multiplication on all of $\mathbb{R}$. For $A, B \in \mathbb{R}$, set $A0^* = 0^*A = 0^*$, and

$$AB = \begin{cases} (-A)(-B) & \text{if } A < 0^*, B < 0^*, \\ -[(-A)B] & \text{if } A < 0^*, B > 0^*, \\ -[A(-B)] & \text{if } A > 0^*, B < 0^*. \end{cases}$$

At the end of Section 1.4, we showed that (OF1) holds for elements of $\mathbb{R}$. A consequence of this is that $A > 0^* \implies -A < 0^*$ (add $-A$ to both sides of $A > 0^*$); hence the products on the right-hand side of our extended definition of multiplication are happening in $\mathbb{R}_+$. Showing that the field axioms for multiplication hold in $\mathbb{R}$ with this extended definition of multiplication mostly amounts to casework. For all $A, B, C \in \mathbb{R}$:

(M1) $AB \in \mathbb{R}$ (**closure**). If either of A and B are 0^*, then $AB = 0^* \in \mathbb{R}$. Otherwise, we consider the following cases.

- $A > 0^*, B > 0^*$. We have already shown that a product of positive real numbers is a (positive) real number.
- $A < 0^*, B < 0^*$. Then $AB = (-A)(-B)$, which is again a product of positive real numbers.
- $A < 0^*, B > 0^*$. Then $AB = -[(-A)B]$, which is the additive inverse of a product of positive real numbers and hence is a real number itself.
- $A > 0^*, B < 0^*$. Then $AB = -[A(-B)]$, which is the additive inverse of a product of positive real numbers and hence is a real number itself.

(M2) $AB = BA$ (**commutativity**). This follows from commutativity of products in $\mathbb{R}_+$.

(M3) $A(BC) = (AB)C$ (**associativity**). This follows from associativity of products in $\mathbb{R}_+$.

(M4) There exists an element $1 \in \mathbb{R}$ such that $1A = A$ (**multiplicative identity**). Of course, we claim that 1^* is the multiplicative identity for all of $\mathbb{R}$.

- $A > 0^*$. We have already shown that $1^*A = A$ for positive A.
- $A = 0^*$. Then $1^*0^* = 0^*$.
- $A < 0^*$. Then $1^*A = -[1^*(-A)] = -[(-A)] = A$, where we have used part (d) of Theorem 2 (it is clear from the definitions of 0^* and 1^* that $1^* > 0^*$).

(M5) If $A \neq 0^*$, then there exists an element $A^{-1} \in \mathbb{R}$ such that $AA^{-1} = 1^*$ (**multiplicative inverse**).

- $A > 0^*$. We have already shown that A^{-1} exists in $\mathbb{R}$.
- $A < 0^*$. Then $-A > 0^*$, so $(-A)^{-1}$ exists in $\mathbb{R}_+$. We claim that $A^{-1} = -(-A)^{-1}$ (note that this is negative). Indeed,

$$AA^{-1} = (-A)(-\left(A^{-1}\right)) = (-A)[-[-(-A)^{-1}]] = (-A)(-A)^{-1} = 1^*,$$

where we have used part (d) of Theorem 2.

Finally, we need to show that multiplication distributes over addition in $\mathbb{R}$, i.e. for all $A, B, C \in \mathbb{R}$, $A(B+C) = AB + AC$; we already showed that this holds in $\mathbb{R}_+$. There are a number of cases to check, a couple of which are shown below. The remaining cases are handled similarly.

- $A > 0^*, B < 0^*, B + C > 0^*$. Then $C = (B+C) + (-B) > 0^*$, so

$$AC = A[(B+C) + (-B)] = A(B+C) + A(-B),$$

since distributivity holds in $\mathbb{R}_+$. Now observe that

$$AB + A(-B) = -[A(-B)] + A(-B) = 0^*.$$

It follows from part (c) of Theorem 2 that $A(-B) = -(AB)$. Hence we see that

$$AC = A(B+C) + A(-B) \iff AC = A(B+C) + [-(AB)] \iff A(B+C) = AB + AC.$$

- $A > 0^*, B < 0^*, C < 0^*$. Note that by commutativity and associativity of addition, we have

$$(-B) + (-C) + (B+C) = (B + (-B)) + (C + (-C)) = 0^* + 0^* = 0^*.$$

Part (c) of Theorem 2 then implies that $-(B+C) = (-B) + (-C)$. Since B and C are both negative, $B + C$ is also negative. Then

$$A(B+C) = -[A(-(B+C))] = -[A((-B) + (-C))] = -[A(-B) + A(-C)],$$

since distributivity holds in $\mathbb{R}_+$. Similarly to the previous case, it can be verified that $A(-B) = -(AB)$ and $A(-C) = -(AC)$. Hence

$$\begin{aligned} A(B+C) &= -[A(-B) + A(-C)] \\ &= -[-(AB) + (-(AC))] \\ &= -[-(AB)] + (-[-(AC)]) \\ &= AB + AC, \end{aligned}$$

where we have used part (d) of Theorem 2.

We have now shown that $\mathbb{R}$ is an ordered field with the least-upper-bound property. This allows us to present another theorem, given without proof (see, for example, Proposition 1.16 of [PMA]). It contains two statements which are true in any field, although we state them in particular for $\mathbb{R}$.

Theorem 3. For all $A, B, C \in \mathbb{R}$, the following statements hold.

(a) $(-A)B = -(AB) = A(-B)$.

(b) $(-A)(-B) = AB$.

1.6 $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield

Finally, we will prove the last part of Theorem 1, which says that $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield. More precisely, we will demonstrate the existence of a function $\psi : \mathbb{Q} \to \mathbb{R}$ such that the following statements hold for all $p, q \in \mathbb{Q}$:

(H1) $\psi(0) = 0^*$ and $\psi(1) = 1^*$;

(H2) $\psi(p) < \psi(q)$ if and only if $p < q$;

(H3) $\psi(p + q) = \psi(p) + \psi(q)$;

(H4) $\psi(pq) = \psi(p)\psi(q)$.

Such a function is said to be an **ordered field homomorphism**; it preserves both the order and field structure of $\mathbb{Q}$. It can be shown that field homomorphisms are necessarily injective, so ψ will in fact be an ordered field isomorphism onto its image $\psi(\mathbb{Q})$. This permits us to make an identification of $\mathbb{Q}$ with $\psi(\mathbb{Q}) \subseteq \mathbb{R}$, which is what we mean by '$\mathbb{R}$ contains $\mathbb{Q}$ as a subfield'. We will show at the end of this section that ψ cannot be surjective, so that $\mathbb{Q}$ is strictly contained inside of $\mathbb{R}$.

To define ψ, let $\psi(p) = \{u \in \mathbb{Q} : u < p\}$ for $p \in \mathbb{Q}$. One can verify that $\psi(p)$ is a Dedekind cut and that (H1) holds. We will now show that the statements (H2) - (H4) hold.

(H2) Suppose that $p < q$; it is then clear that $\psi(p)$ is a subset of $\psi(q)$. This containment is strict since $\frac{p+q}{2}$ belongs to $\psi(q)$ but not to $\psi(p)$. Hence $\psi(p) < \psi(q)$. Conversely, suppose $\psi(p)$ is a strict subset of $\psi(q)$. Then there must exist some $u \in \mathbb{Q}$ such that $u \in \psi(q)$ and $u \notin \psi(p)$, i.e. $u < q$ and $p \leq u$. It follows that $p < q$.

(H3) We have

$$\begin{aligned}\psi(p+q) &= \{u \in \mathbb{Q} : u < p+q\}, \\ \psi(p)+\psi(q) &= \{r+s : r \in \psi(p), s \in \psi(q)\} \\ &= \{r+s : r < p, s < q\}.\end{aligned}$$

The inclusion $\psi(p)+\psi(q) \subseteq \psi(p+q)$ is clear. For the reverse inclusion, suppose $u \in \psi(p+q)$, i.e. $u < p+q$. Using the Archimedean property of $\mathbb{Q}$, choose a positive integer N such that $\frac{1}{N} < p+q-u$. Then $p - \frac{1}{N} < p$, $u - p + \frac{1}{N} < q$, and

$$u = \left(p - \tfrac{1}{N}\right) + \left(u - p + \tfrac{1}{N}\right) \in \psi(p) + \psi(q).$$

A useful consequence of (H1) and (H2) is the following. For any $p \in \mathbb{Q}$, we have

$$0^* = \psi(0) = \psi(p + (-p)) = \psi(p) + \psi(-p).$$

It follows from Theorem 2 (c) that $\psi(-p) = -\psi(p)$.

(H4) First, suppose p and q are both positive. It then follows from (H1) and (H2) that both of $\psi(p)$ and $\psi(q)$ are also positive. Hence we have

$$\begin{aligned}\psi(pq) &= \{u \in \mathbb{Q} : u < pq\}, \\ \psi(p)\psi(q) &= \{u \in \mathbb{Q} : u \leq rs \text{ for some choice of } r \in \psi(p), s \in \psi(q), r > 0, s > 0\} \\ &= \{u \in \mathbb{Q} : u \leq rs \text{ for some choice of } 0 < r < p, 0 < s < q\}.\end{aligned}$$

The inclusion $\psi(p)\psi(q) \subseteq \psi(pq)$ is clear. For the reverse inclusion, suppose $u \in \psi(pq)$, i.e. $u < pq$. If $u \leq 0$, then any choice of r and s with $0 < r < p$ and $0 < s < q$ will do, say $r = \frac{p}{2}$ and $s = \frac{q}{2}$. If $0 < u < pq$, then set $r = \frac{1}{2}\left(\frac{u}{q} + p\right)$. It follows that

$$0 < \tfrac{u}{q} < r < p \implies 0 < \tfrac{u}{r} < q.$$

Then since $u = r \cdot \frac{u}{r}$, we have $u \in \psi(p)\psi(q)$, so that $\psi(pq) \subseteq \psi(p)\psi(q)$. Hence we have $\psi(pq) = \psi(p)\psi(q)$ in the special case when both of p and q are positive.

If either of p or q are 0, then the equality $\psi(pq) = \psi(p)\psi(q)$ is clear since $\psi(0) = 0^*$. Suppose that p and q have opposite signs, say $p > 0$ and $q < 0$. Then we have

$$\begin{aligned}\psi(pq) &= \psi(-[p(-q)]) \\ &= -\psi(p(-q)) \\ &= -[\psi(p)\psi(-q)] \\ &= -[\psi(p)(-\psi(q))] \\ &= -(-[\psi(p)\psi(q)]) \\ &= \psi(p)\psi(q),\end{aligned}$$

where we have used Theorem 3 (a) and Theorem 2 (d). Now suppose that $p < 0$ and $q < 0$. Then

$$\psi(pq) = \psi((-p)(-q)) = \psi(-p)\psi(-q) = [-\psi(p)][-\psi(q)] = \psi(p)\psi(q),$$

where we have used Theorem 3 (b). We have now shown that (H4) holds in all cases.

Now we will show that ψ cannot be surjective. One approach is to use the following lemma.

Lemma 1. Suppose A and B are totally ordered sets and $f : A \to B$ is a bijection with the following property: for all $a \in A$ and $b \in B$,

$$a < b \iff f(a) < f(b).$$

Then if A has the least-upper-bound property, so does B.

Proof. Let $E \subseteq B$ be non-empty and bounded above by some $b \in B$. Then since f is a bijection, $f^{-1}(E) \subseteq A$ is also non-empty. Furthermore, it is bounded above by $f^{-1}(b) \in A$:

$$a \in f^{-1}(E) \iff f(a) \in E \implies f(a) < b \iff a < f^{-1}(b).$$

Hence $s = \sup f^{-1}(E)$ exists in A. We claim that $\sup E = f(s)$. To prove this, we need to show two things.

- $f(s)$ is an upper bound for E. This follows since

$$y \in E \iff f^{-1}(y) \in f^{-1}(E) \implies f^{-1}(y) < s \iff y < f(s).$$

- If $y \in B$ is such that $y < f(s)$, then y is not an upper bound of E. For such a y, we have $f^{-1}(y) < s$. Hence $f^{-1}(y)$ is not an upper bound of $f^{-1}(E)$, i.e. there must exist some $x \in f^{-1}(E)$ such that $f^{-1}(y) < x$. It follows that $y < f(x)$, with $f(x) \in E$, so that y cannot be an upper bound of E.

We conclude that $\sup E = f(s)$ and hence that B has the least-upper-bound property. □

This lemma rules out the possibility of ψ being surjective, since this would imply the existence of $\psi^{-1} : \mathbb{R} \to \mathbb{Q}$ satisfying the hypotheses of Lemma 1, which would in turn imply that $\mathbb{Q}$ has the least-upper-bound property; but $\mathbb{Q}$ does not have the least-upper-bound property (see Chapter 1 of [PMA] or here).

Another approach would be to consider square roots of 2. It can be shown that there is a real number whose square is 2 (see Chapter 1 of [PMA] or here). Combining such a real number with the existence of $\psi^{-1} : \mathbb{R} \to \mathbb{Q}$ would imply that there was a rational number whose square is 2; but it is well-known that there is no such rational number.

[PMA] Rudin, W. (1976) *Principles of Mathematical Analysis.* 3rd edn.