Real numbers and other completions

Fred Richman
Florida Atlantic University
Boca Raton, FL 33431

11 March 2007

Abstract

A notion of completeness and completion suitable for use in the absence of countable choice is developed. This encompasses the construction of the real numbers as well as the completion of an arbitrary metric space. The real numbers are characterized as a complete archimedean Heyting field, a terminal object in the category of archimedean Heyting fields.

1 Introduction

I want to address two topics in constructive mathematics without countable choice:

- completeness of metric spaces,
- axioms for the real numbers, and a construction of the real numbers that is appropriate for those axioms.

The two topics are related because completeness is a key axiom for the real numbers.

How are we to define completeness? Sequential completeness is natural if one defines the real numbers, as Bishop does in [2], to be regular sequences of rational numbers: $|q_m - q_n| \leq 1/m + 1/n$. However, without countable choice, one cannot even show that these regular Cauchy reals are sequentially complete (see [8]). So sequential completeness is probably the wrong notion.

We will want a stronger notion of completeness both to develop the real numbers and to complete a metric space.

To construct an element r of the completion of a space X, it should suffice to show how, for each n, to construct an element x in X that is within $1/n$ of r. Symbolically, $d(x,r) \leq 1/n$. Countable choice would then let you construct a sequence x_n in X such that $d(x_n,r) \leq 1/n$ for all n. The triangle inequality implies that $d(x_m,x_n) \leq 1/m + 1/n$ for all m and n, so we arrive at the idea of a regular sequence. The set of regular sequences that converge to a fixed r is exactly an equivalence class of regular sequences under the equivalence $x \equiv y$ defined by $d(x_m,y_n) \leq 1/m + 1/n$ for all m and n.

Bishop used regular sequences both to define a real number and to define an element in the completion of a metric space. Actually, Bishop used the equivalence $d(x_n,y_n) \leq 2/n$, rather than $d(x_m,y_n) \leq 1/m + 1/n$, but these are the same for regular sequences. In fact, all that is needed is that $d(x_n,y_n)$ converge to zero, even unmodulated convergence. Thus a regular sequence that converges to r is simply a choice function for the sequence of sets

$$S_n = \{x \in X : d(x,r) \leq 1/n\}$$

When operating without choice, it is natural to focus on the sequence S_n itself, which has the property that if $x \in S_m$ and $y \in S_n$, then $d(x,y) \leq 1/m+1/n$. (In the spirit of Heyting and Brouwer, we could think of a regular sequence x not as specified by a rule but as an infinitely proceeding sequence, or a choice sequence, such that $x_n \in S_n$.) This idea of using regular sequences of subsets to construct completions was sketched in a short paragraph in [10], with an additional reference to [12]. Part of the purpose of this paper is to expand on that short paragraph. The detailed development of the completion of a metric space X in [10] was based on the notion of a *location*, a certain kind of continuous function on X that ends up being the distance from x in X to the point r in the completion of X. This idea seems of only academic interest because, in practice, one constructs approximations to r, not the distance function to r.

In his axiomatic treatment of the real numbers in [3, Axiom sets R1 and R2], Bridges uses a least upper bound principle for his completeness axiom—essentially Dedekind completeness. Unlike sequential completeness, it is quite adequate for a choiceless development of the real numbers. It is also quite elegant. However, it cannot be used to define completeness in arbitrary metric spaces. Partly for this reason, I don't think it is the right condition to impose. Another reason is that constructivists don't seem to use the (constructive) least upper bound principle a lot. To be sure, it is a substitute for the classical least upper bound principle, but it doesn't come up often in constructive practice. In classical mathematics, you can use the least upper bound principle to prove that a series converges without having to figure out how far out you have to go to get a good approximation, or you can use it to define the lower integral of a continuous function. We don't have any similar uses for the constructive least upper bound principle. We normally show directly how to compute good approximations.

2 Premetric spaces and completions

Metric spaces presuppose the real numbers, so if we want a notion of completeness that will apply to the construction of the real numbers as well as to metric spaces, we need a more general concept. What exactly is the right level of generality? Uniform spaces seem a little too general to me, so I have settled on the notion of what I will call a *premetric space*.

The data needed to turn a set X into a premetric space is a family E_q of symmetric subsets of $X \times X$ indexed by nonnegative rational numbers q. These are the *entourages* of a uniform structure on X. We will mostly use the more suggestive notation $d(x, y) \leq q$ to stand for $(x, y) \in E_q$ without committing ourselves to any entity $d(x, y)$. We impose the following conditions:

- $d(x, y) \leq 0$ if and only if $x = y$ (separated)
- for all x, y, there exists q such that $d(x, y) \leq q$ (no points at infinity)
- $d(x, y) \leq p$ if and only if $d(x, y) \leq q$ for all $q > p$ (upper continuous)
- if $d(x, y) \leq p$ and $d(y, z) \leq q$, then $d(x, y) \leq p + q$ (triangle)

Classically this allows us to define a metric on X by letting $d(x, y)$ be the real number $\inf \{q \in \mathbf{Q} : d(x, y) \leq q\}$. For this to define a finite-valued metric we need the condition that there be no points at infinity, a condition that otherwise seems unimportant. If we impose the classically trivial condition

- if $p < q$ then either $d(x, y) \leq q$ or not $d(x, y) \leq p$ (located points) (see [6]), then we get a metric, provided, of course, that we have already constructed the real numbers. Without located points we can think of $d(x, y)$ as a generalized real number (an uppercut) [9]. If we do this, then a premetric is simply a metric where the distances are generalized real numbers. Any metric space is a premetric space with located points in the obvious way. The rational numbers are a premetric space with located points if we define $d(x, y) \leq q$ to mean $|x - y| \leq q$. So we've covered our two fundamental examples.

We don't need located points for most of the theory, although it's not clear how interesting premetric spaces without located points are. Here's an example of one. Let P be a proposition and $X = \{0, 1, x\}$. Define

$$\begin{array}{ll} d(0, x) \leq q & \text{if } q \geq 1 \text{ or } P \\ d(1, x) \leq q & \text{if } q \geq 1 \text{ or } \neg P \\ d(0, 1) \leq q & \text{if } q \geq 1 \end{array}$$

If $d(0, x) \leq 1/2$, then P, while if not $d(0, x) \leq 0$, then $\neg P$, so this space has located points only if P or not P. (We will consider the point $1 \in X$ below.)

A natural inequality on a premetric space is obtained by setting $x \neq y$ if $\neg d(x, y) \leq \varepsilon$ for some $\varepsilon > 0$. Note that $x = y$ if $d(x, y) \leq \varepsilon$ for all $\varepsilon > 0$, so this is a stronger inequality than simply $\neg x = y$ because we require a witnessing ε. If points are located, then $x \neq y$ if and only if $d(x, y) > 0$, where d is a metric, so the inequality is a tight apartness.

In the above example, P is equivalent to $x = 0$ and $\neg P$ is equivalent to $x = 1$. If the inequality were tight, then $x = 0$ would be $\neg x \neq 0$, so we would get $P \equiv \neg\neg P$. If the inequality were cotransitive ($a \neq c$ implies $a \neq b$ or $b \neq c$), then we would have $\neg P \vee \neg\neg P$, weak LEM. Later we will be able to observe that this premetric space is complete.

What are the maps between premetric spaces? It depends on what we want, just like for metric spaces. For our purposes, the right definition seems to be that a map is a function that is uniformly continuous on bounded subsets, where a subset S is **bounded** if $S \times S \subset E_q$ for some q. A function f is uniformly continuous on a set S if for each $\varepsilon > 0$ there exists $\delta > 0$ such that $d(s_1, s_2) \leq \delta$ implies $d(f(s_1), f(s_2)) \leq \varepsilon$. Of course.

The natural premetric on $X \times Y$ is the sup premetric: $d((x, y), (x', y')) \leq q$ if $d(x, x') \leq q$ and $d(y, y') \leq q$. This is the categorical product in the category of premetric spaces with the maps being the functions that are uniformly continuous on bounded subsets. It is also the categorical product if we take the maps to be weak contractions, that is, if $d(x_1, x_2) \leq q$, then $d(f(x_1), f(x_2)) \leq q$. In the latter category, isomorphism is isometry.

The **closure** of a subset S of a premetric space X is

$$\bar{S} = \{x \in X : \text{ for each } q > 0 \text{ there is } s \in S \text{ such that } d(x, s) \leq q\}$$

We say that S is **closed** if $\bar{S} = S$, **dense** if $\bar{S} = X$. The subsets E_q are closed in the space $X \times X$ because of the triangle inequality and upper continuity. If f is uniformly continuous on bounded subsets, then $f(\bar{S}) \subset \overline{f(S)}$. The subspace premetric on a subset S of X is given by restricting the relations $d(x, y) \leq q$ to S.

A **regular family** of subsets of X is a family of nonempty subsets S_q indexed by positive rational numbers q with the property that $d(x, y) \leq p+q$ for all $x \in S_p$ and $y \in S_q$. The idea is that S_q will consist of some of the elements of X that are within q of a point in the completion of X. In practice, what happens is that we show how to construct an element of X that is within q of an element of the completion of X. There are typically some choices involved in this construction, so that we are actually constructing a nonempty set of approximations.

Two regular families S and T are **equivalent** if $d(x, y) \leq p + q$ for all $x \in S_p$ and $y \in T_q$. That is, $S_p \times T_q \subset E_{p+q}$. Reflexivity follows by definition and symmetry by the symmetry of $d(x, y) \leq q$. For transitivity, if $S_p \times T_q \subset E_{p+q}$ and $T_q \times U_r \subset E_{q+r}$, then $S_p \times U_r \subset E_{p+q} \circ E_{q+r} \subset E_{p+r+2q}$. This holds for all $q > 0$ so $S_p \times U_r \subset E_{p+r}$.

We will let $\mathbf{Q}^+ = \{q \in \mathbf{Q} : q > 0\}$ and $\mathbf{Q}^- = \{q \in \mathbf{Q} : q < 0\}$.

Define the elements of the **completion** $\hat{X}$ of X to be the equivalence classes of regular families of subsets. The premetric structure on $\hat{X}$ is defined by $d(S, T) \leq q$ if for all $\varepsilon > 0$, there exist $a, b, c \in \mathbf{Q}^+$ and elements $s \in S_a$ and $t \in T_b$ such that $a+b+c < q+\varepsilon$ and $d(s, t) \leq c$. There is a natural map from X to $\hat{X}$ that takes $x \in X$ to the regular family S^x defined by $S^x_q = \{x\}$ for all q. We say that X is **complete** if this natural map is onto. By upper continuity, this says that if T is a regular family, then there exists $x \in X$ such that $d(x, t) \leq q$ for all $t \in T_q$.

Lemma 1 *If T is regular family and $x \in T_q$, then $d(S^x, T) \leq q$.*

Proof. This is an exercise in using the definitions. For $\varepsilon \in \mathbf{Q}^+$, let $a = b = \varepsilon/4$ and $c = q + b$. If $x \in T_q$ and $t \in T_b$, then $d(x, t) \leq q + b = c$. Moreover $a + b + c = q + 3\varepsilon/4 < q + \varepsilon$. ■

Theorem 2 *The completion $\hat{X}$ of a premetric space X is a premetric space. The natural map of X into $\hat{X}$ is a dense embedding and the premetric structure on $\hat{X}$ extends the premetric structure on X. Moreover, if X has located points, then so does $\hat{X}$.*

Proof. Clearly symmetry and upper continuity hold. To verify separation, suppose $d(S,T) \leq 0$. Then for each $\varepsilon \in \mathbf{Q}^+$, there exist $a,b,c \in \mathbf{Q}^+$ and elements $s \in S_a$ and $t \in T_b$ such that $a+b+c < \varepsilon$ and $d(s,t) \leq c$. We will show that $S_p \times T_q \subset E_{p+q+\varepsilon}$ for each $\varepsilon \in \mathbf{Q}^+$, whence $S_p \times T_q \subset E_{p+q}$. Thus S is equivalent to T. Suppose $u \in T_q$ and $v \in S_p$. Then $d(u,t) \leq q+b$ and $d(s,v) \leq p+a$. So $d(u,v) \leq p+q+a+b+c < p+q+\varepsilon$.

For the triangle inequality, suppose $d(S,T) \leq p$ and $d(T,U) \leq q$. We want to show that $d(S,U) \leq p+q$. For each $\varepsilon \in \mathbf{Q}^+$ there exist $a,b,c \in \mathbf{Q}^+$ and elements $s \in S_a$ and $t \in T_b$ such that $a+b+c < p+\varepsilon/2$ and $d(s,t) \leq c$. Also there exist $a',b',c' \in \mathbf{Q}^+$ and elements $t' \in T_{a'}$ and $u \in U_{b'}$ such that $a'+b'+c' < q+\varepsilon/2$ and $d(t',u) \leq c'$. So $a+a'+b+b'+c+c' < p+q+\varepsilon$ and $s \in S_a$ and $u \in U_{b'}$ with $d(s,u) \leq c+b+a'+c'$. Let $c'' = c+b+a'+c'$. Then $a+b'+c'' < p+q+\varepsilon$ and $s \in S_a$ and $u \in U_{b'}$ with $d(s,u) \leq c''$.

To show that the premetric structure on $\hat{X}$ extends that on X, we must show that $d(S^x,S^y) \leq q$ exactly when $d(x,y) \leq q$. Note that $d(S^x,S^y) \leq q$ exactly when for all $\varepsilon \in \mathbf{Q}^+$, there exist a,b,c such that $a+b+c < q+\varepsilon$ and $d(x,y) \leq c$. If $d(x,y) \leq q$, then we can choose $a = b = \varepsilon/3$ and $c = q$ to show that $d(S^x,S^y) \leq q$. Conversely, suppose $d(S^x,S^y) \leq q$. To show that $d(x,y) \leq q$, it suffices to show that $d(x,y) \leq q+\varepsilon$ for all ε. But $d(x,y) \leq q+\varepsilon-a-b$.

That X is embedded densely in $\hat{X}$ is immediate from Lemma 1.

Finally, we show that if X has located points, then so does $\hat{X}$. In fact, we will show that if X is a dense subset of Y, and X has located points, then Y has located points. Suppose $p < q$ and $y_1, y_2 \in Y$. Choose $x_1, x_2 \in X$ such that $d(x_i,y_i) \leq a < (q-p)/4$. If $d(x_1,x_2) \leq q-2a$, then $d(y_1,y_2) \leq q$. If $d(y_1,y_2) \leq p$, then $d(x_1,x_2) \leq p+2a$. But if X has located points, then either $d(x_1,x_2) \leq q-2a$ or not $d(x_1,x_1) \leq p+2a$. ■

Each regular family T gives rise to a largest equivalent family C defined by

$$C_q = \{x \in X : d(S^x,T) \leq q\}$$

Lemma 1 shows $T_q \subset C_q$. It remains to show that C is a regular family, that is, if $x \in C_p$ and $y \in C_q$, then $d(x,y) \leq p+q$. This is immediate from the triangle inequality in $\hat{X}$. So each element of $\hat{X}$ has a canonical representative.

Theorem 3 *If X is a dense subset of a premetric space Y, and Z is a complete premetric space, then any (uniformly continuous) map from X to Z extends uniquely to a (uniformly continuous) map from Y to Z.*

Proof. Let $f : X \to Z$ be uniformly continuous on bounded subsets. We will extend f to $g : Y \to Z$. It suffices to look at f on bounded subsets of X, so we may assume that f is uniformly continuous. For each $y \in Y$, define a regular family of subsets of Z by

$$S_q(y) = \left\{ f(x) : d(x,y) \leq p \text{ and } f(E_{p+\varepsilon}) \subset E_q \text{ for some } p, \varepsilon \in \mathbf{Q}^+ \right\}$$

In a typical proof we might say, or hint at, something like this: To define $g(y)$ in the complete space Z, we need to approximate $g(y)$ within q. Choose p and ε so that $f(E_{p+\varepsilon}) \subset E_q$. Choose x so that $d(x,y) \leq p$. Then $f(x)$ is a q-approximation to $g(y)$. Here we will fill in the details.

To show that $S(y)$ is a regular family, suppose $f(x) \in S_q(y)$ and $f(x') \in S_{q'}(y)$ with the corresponding witnessing $p, \varepsilon, p', \varepsilon'$. Choose x'' so that $d(x'', y) \leq \min(\varepsilon, \varepsilon')$. Then $d(x, x'') \leq p+\varepsilon$ and $d(x', x'') \leq p'+\varepsilon'$, so $d(f(x), f(x'')) \leq q$ and $d(f(x'), f(x'')) \leq q'$, whence $d(f(x), f(x')) \leq q + q'$. So the family $S(y)$ is regular. Because Z is complete, there exists a unique $z \in Z$ so that $d(s,z) \leq q$ for each $s \in S_q(y)$. Define $g(y) = z$.

To show that g extends f, suppose $y \in X$ and $s \in S_q(y)$. Then $s = f(x)$ where $d(x,y) \leq p$ and $f(E_{p+\varepsilon}) \subset E_q$. Thus $d(s, f(y)) \leq q$ for each $s \in S_q(y)$ so $g(y) = f(y)$ by the definition of $g(y)$.

We will show that g is uniformly continuous by showing that if $f(E_p) \subset E_q$, then $g(E_{p-\varepsilon}) \subset E_q$ for any $\varepsilon > 0$. It suffices to show that $g(E_{p-\varepsilon}) \subset E_{q+\delta}$ for any $\delta > 0$. There is positive $\theta \leq \varepsilon/2$ so that $f(E_{2\theta}) \subset E_{\delta/2}$. Suppose $d(y,y') \leq p - \varepsilon$. There exist $x, x' \in X$ so that $d(x,y) \leq \theta$ and $d(x',y') \leq \theta$ because X is dense in Y. So $f(x) \in S_{\delta/2}(y)$ and $f(x') \in S_{\delta/2}(y')$ whence $d(f(x), g(y)) \leq \delta/2$ and $d(f(x'), g(y')) \leq \delta/2$. Note that $d(x,x') \leq p$ because $\theta \leq \varepsilon/2$, so $d(f(x), f(x')) \leq q$ whence $d(g(y), g(y')) \leq q + \delta$, which is what we wanted to show. ■

3 Archimedean ordered Heyting fields

To axiomatize the real numbers, we start with the notion of an ordered Heyting field. The definition is fairly routine: simply write down the arithmetic and order properties of subfields of the real numbers. It appears essentially in [3, Axiom sets R1 and R2]. We want to use a slight variant of the usual axioms. First define an **ordered abelian group** to be an abelian group A together with a subset $P \subset A$, the (strictly) positive elements satisfying

- $P + P \subset P$
- $A \subset P - P$ (directed)
- $P \cap -P = \emptyset$
- If $a \notin P \cup -P$, then $a = 0$ (tight)
- If $a + b \in P$, then $a \in P$ or $b \in P$ (cotransitive)

The strict order on an ordered abelian group is obtained by setting $x < y$ if $y - x \in P$; the weak order by setting $x \leq y$ if $x - y \notin P$. The subset P is reconstructed as $\{x \in A : x > 0\}$. Note that $0 \notin P$ because $P \cap -P = \emptyset$. If tightness is replaced by its classical equivalent, $A = P \cup \{0\} \cup -P$, then A is totally ordered by $x \leq y$ in the usual sense, and $x \leq y$ if and only if $x < y$ or $x = y$. In any event, A is partially ordered by $x \leq y$, the strict order $x < y$ is transitive, cotransitive, and asymmetric, and both $x \leq y$ and $x < y$ are translation invariant. We define an inequality on A by $x \neq y$ if $x < y$ or $y < x$, that is, $x - y \in P \cup -P$. This inequality is a (tight) apartness.

The condition that $A \subset P - P$ implies that P is nonempty. So this is really a definition of a *nontrivial* ordered abelian group, the only kind we are interested in here. An ordered abelian group is said to be **archimedean** if whenever $x, y \in P$, then there exists a positive integer n such that $x < ny$. Note that we need not assume that $x \in P$ in this definition because $A \subset P - P$.

An **ordered Heyting field** is a commutative ring k whose additive group is an ordered abelian group and whose positive elements form a group under multiplication.

Proposition 4 *Let k be an ordered Heyting field and P its group of positive elements. Then the identity of the group P is the multiplicative identity of k, and the invertible elements of k are exactly the elements of $P \cup -P$.*

Proof. That the identity of P is the identity of k follows from $k \subset P - P$. Clearly $P \cup -P$ consists of invertible elements of k. Conversely, suppose

$ab = 1$. Then $a \in P$ or $1 - a \in P$, by cotransitivity, and the same for b. So either $a \in P$ or $1 - a$ and $1 - b$ are in P. Replacing a by $-a$ and b by $-b$, we see that either $a \in -P$ or $1 + a$ and $1 + b$ are in P. Thus either $a \in P \cup -P$ or $b - a = (1 - a)(1 + b) \in P$ and $a - b = (1 + a)(1 - b) \in P$, which contradicts $P \cap -P = \emptyset$. ■

There is a natural map of the ring $\mathbf{Z}$ of integers into any ordered Heyting field k that takes $m \in \mathbf{Z}$ to $m \cdot 1 \in k$. This map is order preserving because $0 < 1$ and if $x > 0$ and $y > 0$, then $x + y > 0$. As $m \cdot 1$ is invertible for nonzero m, this map extends to a map of the field $\mathbf{Q}$ of rational numbers into k. This map preserves order because $x > 0$ if and only if $nx > 0$. Indeed, by cotransitivity either $nx > 0$ or $nx < x$ in which case $(n - 1)x < 0$ which is impossible. We will identify $\mathbf{Q}$ with its image in k so we consider any ordered Heyting field to contain $\mathbf{Q}$.

We need more axioms to characterize the real numbers. The first one, which essentially appears in [3], has two aspects. An ordered Heyting field is **archimedean** if its additive group is archimedean.

Theorem 5 *Let k be an ordered Heyting field. Then the following two conditions are equivalent*

- *k is archimedean.*
- *$\mathbf{Q}$ is dense in k: If $x < y$, then there exists a rational number q such that $x < q < y$.*

Proof. Suppose k is archimedean and $x < y$. Then $n(y - x) > 1$ for some positive integer n. We can find integers $m < nx$ and $M > ny$. Consider the integers $m, m + 1, m + 2, \ldots, M$. For each integer i such that $m \leq i \leq M$ we have either $i > nx$ or $i < ny$. As $m < nx$ and $M > ny$, we can find an integer i so that $i < ny$ and $i + 1 > nx$. As $ny > nx + 1$, either $i + 1 > nx + 1$ or $i + 1 < ny$. In the latter case, $nx < i + 1 < ny$; in the former case $nx < i < ny$. In either case we have found we have found an integer j so that $nx < j < ny$ and so $x < j/n < y$.

Conversely, suppose $\mathbf{Q}$ is dense in k and $x > 0$. There is a rational number q such that $y/x < q < y/x + 1$, hence a positive integer n such that $y/x < n$. So $nx > y$ because $PP \subset P$ ■

The standard example of a countable discrete Heyting field that is not archimedean is the field $\mathbf{Q}(X)$ of rational functions over the rational numbers, ordered by setting $f(X)/g(X) > 0$ if $\lim_{x\to+\infty} f(x)/g(x) > 0$. Here $1/X > 0$ but $nX < 1$ for every positive integer n.

Any subfield of $\mathbf{R}$ is an archimedean ordered Heyting field, for example, $\mathbf{Q}$ or $\mathbf{Q}\left[\sqrt{2}\right]$ or the field of all algebraic real numbers. By a subfield of $\mathbf{R}$ we mean a subring R such that if $x \in R$ and $x \neq 0$ in $\mathbf{R}$, then $x^{-1} \in R$. Archimedean ordered Heyting fields need not have finite infima. For $a \in \mathbf{R}$, the subfield $\mathbf{Q}(a)$ of $\mathbf{R}$ consists of all quotients of polynomials $p(a)/q(a)$ where $q(a) > 0$. Suppose $a \wedge 0$ is in $\mathbf{Q}(a)$. So $a \wedge 0 = p(a)/q(a)$ with $q(a) > 0$. So $a \geq 0$ if and only if $p(a) = 0$. If $p = 0$, then $a \geq 0$. Otherwise either $a > 0$ or $a < r$ for each of the finite number of positive roots r of p. But if $a < r$ for every positive root r of p, then $a \leq 0$ because if $a > 0$, then a is a positive root of p. So if $a \wedge 0$ is in $\mathbf{Q}(a)$, then either $a \geq 0$ or $a \leq 0$. For a a Cauchy real, that's Bishop's LLPO. Of course, conversely, if $a \geq 0$ or $a \leq 0$ for all real numbers a, then finite infima exist in any subfield of $\mathbf{R}$.

We will need the following technical lemma about archimedean Heyting fields.

Lemma 6 *Let k be an archimedean Heyting field.*

1. *If $a_1, a_2 \in k$, and q is a rational number such that $q < a_1 + a_2$, then there exist rational numbers q_1 and q_2 such that $q_1 < a_1$ and $q_2 < a_2$ and $q = q_1 + q_2$.*

2. *If a_1, a_2 are positive elements of k, and $q \in \mathbf{Q}^+$ such that $q < a_1 a_2$, then there exist $q_1, q_2 \in \mathbf{Q}^+$ such that $q_1 < a_1$ and $q_2 < a_2$ and $q = q_1 q_2$.*

3. *If $x, y \in k$, and $q < x$ implies $q < y$ for each rational number q, then $x \leq y$.*

4. *For $p, q \in \mathbf{Q}^+$ and $x, y \in k$, if $-p \leq x \leq p$ and $-q \leq y \leq q$, then $-pq \leq xy \leq pq$.*

Proof. Suppose $q < a_1 + a_2$. Choose q_1 so that $q - a_2 < q_1 < a_1$ and set $q_2 = q - q_1$. For 2, suppose $q < a_1 a_2$. Choose q_1 so that $q/a_2 < q_1 < a_1$ and set $q_2 = q/q_1$. For the third claim we must show that the assumption that $y < x$ leads to a contradiction. But if $y < x$, then there exists a rational number q such that $y < q < x$, and this rational number is less than x but not less than y.

To prove 4, we will prove the precontrapositive that if $pq < xy$, then $p < x$ or $p < -x$ or $q < y$ or $q < -y$. Replacing x by $-x$ we get the same conclusion from $xy < -pq$. So suppose $pq < xy$. Then $xy > 0$ so either $x > 0$ and $y > 0$, or $x < 0$ and $y < 0$. Replacing x by $-x$ and y by $-y$, if necessary, we may assume that we are in the first case. From 2 there exist $p', q' \in \mathbf{Q}^+$ such that $p'q' = pq$ and $p' < x$ and $q' < y$. Either $p \leq p'$ or $q \leq q'$, so either $p < x$ or $q < y$. ∎

Part 4 of the lemma says essentially that multiplication is continuous. The statement corresponding to 4 for addition is obviously true.

We will characterize $\mathbf{R}$ as a terminal object in the category of all archimedean ordered Heyting fields. We need to say what a map in this category is. A map should respect all the structure, so it should be a homomorphism of rings, and it should preserve the relation $x < y$. But what does it mean to preserve the relation $x < y$? It could mean that if $x < y$, then $\varphi x < \varphi y$, or it could mean the converse. We will show that these two conditions are equivalent. Note that any ring homomorphism φ between rings containing $\mathbf{Q}$ is the identity map on $\mathbf{Q}$. That's because in the category of rings with 1, every homomorphism takes 1 to 1.

Theorem 7 *Let k_0 and k_1 be archimedean ordered Heyting fields, and $\varphi : k_0 \to k_1$ a function that is the identity on $\mathbf{Q}$. Then the following two conditions are equivalent:*

1. *For all x and y in k_0, if $x < y$, then $\varphi x < \varphi y$.*
2. *For all x and y in k_0, if $\varphi x < \varphi y$, then $x < y$.*

If these conditions are met, then φ is a ring homomorphism.

Proof. Suppose 1 and $\varphi x < \varphi y$. There exist rational numbers q, q', and q'' such that $\varphi x < q < q' < q'' < \varphi y$. Now either $x < q'$ or $x > q$. In the latter case, $\varphi x > q$ by 1, a contradiction. So $x < q'$. Similarly $q' < y$, so $x < y$. Now suppose 2 and $x < y$. There exist rational numbers q, q', and q'' such that $x < q < q' < q'' < y$. Either $\varphi x < q'$ or $\varphi x > q$. In the latter case, $x > q$ by 2, a contradiction. So $\varphi x < q'$. Similarly $q' < \varphi y$ so $\varphi x < \varphi y$.

To show that $\varphi(x + y) = \varphi(x) + \varphi(y)$, it suffices to show weak inequality in each direction. Suppose that $q < \varphi(x + y)$ for some rational number q. Then $q < x + y$ so from Lemma 6 part 1 there exist rational numbers $q_1 < x$ and $q_2 < y$ such that $q = q_1 + q_2$. Then $q_1 < \varphi(x)$ and $q_2 < \varphi(y)$ so $q < \varphi(x) + \varphi(y)$. Thus Lemma 6 part 3 says that $\varphi(x + y) \leq \varphi(x) + \varphi(y)$.

For the other inequality, suppose $q < \varphi(x) + \varphi(y)$. Then $q = q_1 + q_2$ where $q_1 < \varphi(x)$ and $q_2 < \varphi(y)$. So $q_1 < x$ and $q_2 < y$ whence $q < x + y$ so $q < \varphi(x+y)$. Hence $\varphi(x) + \varphi(y) \leq \varphi(x+y)$.

The same argument shows that if x and y are positive, then $\varphi(xy) = \varphi(x)\varphi(y)$. Now $\varphi(-a) = -\varphi(a)$ because φ is a homomorphism of additive groups. So φ is a ring homomorphism because every element of k is a difference of positive elements and φ is a homomorphism of additive groups.

■

By a map in the category of archimedean ordered Heyting fields, we mean a ring homomorphism that satisfies either of the equivalent conditions in the preceding theorem (order preserving). We want to define the real numbers to be a terminal object in this category. That is to say, for each archimedean ordered Heyting field k, there is a unique map $k \to \mathbf{R}$. Such an object is clearly unique up to isomorphism. Because maps between archimedean Heyting fields are one-to-one (in a strong sense), the fact that $\mathbf{R}$ is terminal can be viewed as saying that $\mathbf{R}$ is as big as possible, hence complete—indeed this is the sense in which Hilbert meant that $\mathbf{R}$ was a complete archimedean field, see [7] and [1].

So we need to construct a terminal archimedean ordered Heyting field. The premetric structure on any archimedean Heyting field, in particular on $\mathbf{Q}$, is obtained by setting $d(x,y) \leq q$ if $-q \leq x - y \leq q$. We will show that a complete archimedean Heyting field is a terminal object in the category of archimedean Heyting fields (Corollary 11), and construct one by completing $\mathbf{Q}$ (Theorem 14).

Theorem 8 *In any archimedean Heyting field, addition is uniformly continuous and multiplication is uniformly continuous on bounded subsets.*

Proof. Addition is uniformly continuous because if $d(x,x') \leq p$ and $d(y,y') \leq q$, then $d(x+y, x'+y') \leq p+q$. Multiplication is uniformly continuous on bounded subsets because if $d(s,0) \leq b$ for all $s \in S$, and if $x, y, x', y' \in S$ with $d(x,x') \leq p$ and $d(y,y') \leq q$, then $d(xy, x'y') \leq b(p+q)$ because $d(xy, x'y) \leq bp$ and $d(x'y, x'y') \leq bq$ from Lemma 6, part 4. ■

We will need the following fact relating the positive elements of an archimedean Heyting field to $\mathbf{Q}^+$.

Theorem 9 *Let k be an archimedean Heyting field and $x \in k$. Then $x > 0$ if and only if there exists $q \in \mathbf{Q}^+$ such that x is in the closure of $[q, \infty) = \{q' \in \mathbf{Q} : q' \geq q\}$ in k.*

Proof. Suppose x is in the closure of $[q,\infty)$. Then x can be approximated within $q/2$ by an element $r \in [q,\infty)$. Either $x > 0$ or $x < r - q/2$, by cotransitivity, but the latter alternative is ruled out because $-q/2 \le x - r \le q/2$.

Conversely, suppose $x > 0$. As k is archimedean, we can find q in $\mathbf{Q}$ such that $0 < q < x$. We will show that x is in the closure of $[q,\infty)$. Suppose $\varepsilon \in \mathbf{Q}^+$. As k is archimedean, there exists $m \ge 2$ such that $x < m\varepsilon/2$. Let $a_k = q + k\varepsilon/2$ for $k = 0,\ldots,m$. Then $a_0 < x < a_m$, so, by cotransitivity, there exists k such that $a_k < x < a_{k+2}$. Then $-\varepsilon < x - a_k \le a_{k+2} - a_k < \varepsilon$ and $a_k \in [q,\infty)$. ■

Corollary 10 *If k and k' are archimedean Heyting fields, and $\varphi : k \to k'$ is a uniformly continuous homomorphism of rings, then φ preserves order, so is a map of archimedean Heyting fields.*

Proof. It suffices to show that if $x > 0$, then $\varphi(x) > 0$. Because φ is a ring homomorphism, it takes $[q,\infty)$ in k to $[q,\infty)$ in k to $[q,\infty)$ in k'. Because φ is uniformly continuous, it takes the closure of $[q,\infty)$ in k into the closure of $[q,\infty)$ in k'. Therefore, by Theorem 9, if $x > 0$, then $\varphi(x) > 0$. ■

Corollary 11 *Any complete archimedean Heyting field is a terminal object in the category of archimedean Heyting fields.*

Proof. If K is a complete archimedean Heyting field, and k is an archimedean Heyting field, then the identity map from $\mathbf{Q} \subset k$ to $\mathbf{Q} \subset K$ extends uniquely to a uniformly continuous map from k to K by Theorem 3. Because the ring operations are continuous (Theorem 8), this map is a ring homomorphism, so is a map of archimedean Heyting fields by Corollary 10. ■

Finally, we need to construct a complete archimedean Heyting field. We do that by completing $\mathbf{Q}$. Addition is uniformly continuous on $\mathbf{Q}$ and multiplication is uniformly continuous on bounded subsets of $\mathbf{Q}$. So these operations extend uniquely to the completion $\mathbf{R}$ of $\mathbf{Q}$, by Theorem 3, where they continue to satisfy the axioms for a commutative ring with identity. The distance "function" on $\mathbf{R}$ is translation invariant in the sense that

Lemma 12 *Let $r_1, r_2, r_3 \in \mathbf{R}$, and $\varepsilon \in \mathbf{Q}^+$. Then*

$$d(r_1, r_2) \le \varepsilon \Leftrightarrow d(r_1 + r_3, r_2 + r_3) \le \varepsilon.$$

Proof. It suffices to show that $d(r_1+r_3, r_2+r_3) \leq \varepsilon + \delta$ for all $\delta \in \mathbf{Q}^+$. Choose $q_1, q_2, q_3 \in \mathbf{Q}$ such that $d(q_i, r_i) \leq \delta/4$ and $d(r_i + r_j, q_i + q_j) \leq \delta/4$. This is possible because $\mathbf{Q}$ is dense in $\mathbf{R}$ and addition is uniformly continuous on $\mathbf{R}$. So $d(q_1, q_2) \leq \varepsilon + \delta/2$ whence $d(q_1 + q_3, q_2 + q_3) \leq \varepsilon + \delta/2$ and so $d(r_1 + r_3, r_2 + r_3) \leq \varepsilon$. ■

We could write $d(s,t) = d(u,v)$ to mean that $d(s,t) \leq \varepsilon$ if and only if $d(u,v) \leq \varepsilon$. So Lemma 12 could be written as

$$d(r_1, r_2) = d(r_1 + r_3, r_2 + r_3) = d(-r_1, -r_2)$$

the latter equation coming from the former by taking $r_3 = -r_1 - r_2$.

To define the order on $\mathbf{R}$ we characterize the positive elements of $\mathbf{R}$.

Lemma 13 *For $r \in \mathbf{R}$, the following are equivalent:*

- *There is $p \in \mathbf{Q}^+$ such that $d(r,p) \leq p/2$,*
- *There is $q \in \mathbf{Q}^+$ such that r is in the closure of $[q, \infty) = \{q' \in \mathbf{Q} : q' \geq q\}$.*

Proof. If $d(r,p) \leq p/2$, let $q = p/4$. We can approximate r arbitrarily closely with elements $q' \in \mathbf{Q}$, and if $d(r,q') \leq p/4$, then $d(p,q') \leq 3p/4$ so $q' \geq q$.

Conversely, if r is in the closure of $[q,\infty)$, then we can find $p \geq q$ so that $d(p,r) \leq q/2 \leq p/2$. ■

Define the set P of (strictly) positive elements of $\mathbf{R}$ to be those r in $\mathbf{R}$ that satisfy the two equivalent conditions of Lemma 13. Note that $P \cap \mathbf{Q} = \mathbf{Q}^+$. The second condition of Lemma 13 seems more natural to me, but the first condition has a much simpler logical form, which can come in handy.

Theorem 14 *With P defined as above, $\mathbf{R}$ is an archimedean Heyting field.*

Proof. We first show that $\mathbf{R}$ is an ordered abelian group. To show that $P + P \subset P$, suppose that $r_1, r_2 \in P$. There exist q_1, $q_2 \in \mathbf{Q}^+$ such that r_i is in the closure of $[q_i, \infty)$, so $r_1 + r_2$ is in the closure of $[q_1 + q_2, \infty)$.

To see that $\mathbf{R} \subset P - P$, let $r \in \mathbf{R}$ and choose $q \in \mathbf{Q}$ such r is in the closure of $[q, \infty)$. Choose $p \in \mathbf{Q}^+$ so that $p + q > 0$. Then $p + r$ is in the closure of $[p + q, \infty)$, hence in P, so $r = (p + r) - p \in P - P$.

If $r \in P \cap -P$, elements in $\mathbf{Q}$ that are close enough to r are both positive and negative, so $P \cap -P = \emptyset$.

Suppose $r \notin P \cup -P$. For $p \in \mathbf{Q}^+$, choose $q \in \mathbf{Q}$ so that $d(q, r) \leq p$ and thus $d(-q, -r) \leq p$. Suppose $q \geq 3p$. If $d(q', r) \leq p$, then $d(q, q') \leq 2p$ whence $q' \geq p$. So r is in the closure of $[p, \infty)$ whence $r \in P$, a contradiction. Thus $q < 3p$. Now suppose $-q \geq 3p$. If $d(q', -r) \leq p$, then $d(q', -q) \leq 2p$ whence $q' \geq p$. So $-r$ is in the closure of $[p, \infty)$whence $r \in -P$, a contradiction. So $|q| < 3p$ whence $d(0, r) \leq 4p$ for any $p > 0$. Thus $r = 0$.

Finally, suppose $r_1 + r_2 \in P$ so there is $p \in \mathbf{Q}^+$ such that $d(r_1 + r_2, p) \leq p/2$. Choose $q_i \in \mathbf{Q}$ so that $d(r_i, q_i) \leq p/16$. Then $d(q_1 + q_2, p) \leq p/2 + p/8 \leq 3p/4$, so $q_{i_0} \geq p/8$ for some $i_0 \in \{1, 2\}$. So $d(r_{i_0}, q_{i_0}) \leq p/16 \leq q_{i_0}/2$ whence $r_{i_0} \in P$.

To show that $\mathbf{R}$ is a Heyting field, we must show that P is a group under multiplication. First we need to show that $PP \subset P$, so suppose $r_1, r_2 \in P$. Then there exists $q_i \in \mathbf{Q}^+$ such that r_i is in the closure of $[q_i, \infty)$. Then $r_1 r_2$ is in the closure of $[q_1 q_2, \infty)$. What about inverses? Suppose r is in the closure of $[q, \infty)$. We may assume $q < 1$. The function x^{-1} is uniformly continuous from $[q, \infty)$ to itself, so extends to the closure (completion) of $[q, \infty)$. Thus there exists s in the closure of $[q, \infty)$, hence in P, such that $rs = 1$.

Finally we want to show that $\mathbf{R}$ is archimedean. Suppose $x, y \in P$. Then x is in the closure of $[q, \infty)$. Let $p \in \mathbf{Q}$ approximate y to within $1/2$ and choose n so that $nq \geq p + 1$. We want to show that $nq - y \in P$. But $d(nq - p, nq - y) \leq 1/2$, because of translation invariance, and $nq - p \geq 1$.

■

4 Remarks on Dedekind reals

A standard way to construct the real numbers is via Dedekind cuts. I like this construction, and I think I have something to say about it, so despite the fact that we can take the real numbers to be the completion of the premetric space of rational numbers, I want to look a little bit at cuts.

In what follows, when we say that a set S is nonempty, or write $S \neq \emptyset$, we mean S is *inhabited*, that is, there is an element in S.

A **Dedekind cut** (in $\mathbf{Q}$) is a pair (L, U) of open subsets of $\mathbf{Q}$ such that

1. L is a nonempty lower set, U is a nonempty upper set, and $L \cap U = \emptyset$.

2. For all $\varepsilon \in \mathbf{Q}^+$ there exist $a \in L$ and $b \in U$ such that $b - a < \varepsilon$.

Some remarks on this definition. Note that 1 implies that if $a \in L$ and $b \in U$, then $a < b$. We could replace $b - a < \varepsilon$ in 2 by $b - a = \varepsilon$. We could reformulate 2 as $(L + \varepsilon) \cap U \neq \emptyset$ for all $\varepsilon \in \mathbf{Q}^+$. We can reconstruct U from L (and vice versa) because U is the interior of the complement of L. However, the symmetric definition is often more convenient. We identify the rational number q with the cut $(\{x \in \mathbf{Q} : x < q\}, \{x \in \mathbf{Q} : x > q\})$. In particular, the rational number 0 is identified with the cut $(\mathbf{Q}^-, \mathbf{Q}^+)$.

Condition 2 is equivalent, given 1, to the property that if $a < b$ are in $\mathbf{Q}$, then $a \in L$ or $b \in U$. That is essentially the property used by Bishop [2, Chapter 2, Problem 6] and Bridges [3]. However 2 is often handier than that property and more suggestive of the idea of a completion because a and b in 2 are both ε-approximations to the number represented by the cut.

Notice that 2 is very close to the idea of defining a real number as a set of pairs of rational numbers, as is done in [4], because the pair of rational numbers (a, b) gives a small open interval that contains the real number. This is an idea that can be generalized to metric spaces, or premetric spaces: the intervals (a, b), or $[a, b]$, can be replaced by balls.

If x is an element of an archimedean Heyting field k, then

$$(\{q \in \mathbf{Q} : q < x\}, \ \{q \in \mathbf{Q} : q > x\})$$

is a Dedekind cut. The two sets are nonempty because k is archimedean. They are open because $\mathbf{Q}$ is dense in k, another aspect of being archimedean. They satisfy 2 because if $a < b$ are in $\mathbf{Q}$, then either $a < x$ or $x < b$ because the order on k is cotransitive.

The set of Dedekind cuts is turned into an abelian group by the definitions

- $(L, U) + (L', U') = (L + L', U + U')$
- $0 = (\mathbf{Q}^-, \mathbf{Q}^+)$
- $-(L, U) = (-U, -L)$

This is easily verified. Note that showing that 2 is inherited by sums is easier than showing that the alternative equivalent property is inherited by sums. To get an ordered abelian group we define the set of positive cuts to be

- $P = \{(L, U) : L \cap \mathbf{Q}^+ \neq \emptyset\}$

To write an arbitrary cut (L, U) as a difference of positive cuts, choose $a \in L$ and let $p = \max(-a, 1)$. Then $p > 0$ and $(L, U) + p > 0$. To verify tightness, we must show that if L contains no positive elements and U contains no negative elements, then $L = \mathbf{Q}^-$. Clearly $L \subset \mathbf{Q}^-$. Conversely, if $q \in \mathbf{Q}^-$, then there exist $a \in L$ and $b \in U$ such that $q + b - a \in \mathbf{Q}^-$. But $b \geq 0$, so $q < a - b \leq a$ is in L.

What about archimedean? Note that $n(L, U) = (nL, nU)$. If (L, U) is positive, and (L', U') is arbitrary, then there exists a positive rational number q in L, and a positive integer n such that $nq \in U'$, so $n(L, U)$ is greater than (L', U'). Indeed, $n(L, U) + (-U', -L') = (nL - U', nU - L')$ and $(nq - U') \cap \mathbf{Q}^+ \neq \emptyset$ because U' is open.

Nobody ever wants to go through all the details of the development of the real numbers via Dedekind cuts. Even classically, which is a bit easier, Rudin [11] doesn't prove anything about multiplication of cuts. He says he did enough with addition, and the proofs for multiplication are quite analogous except you sometimes have to divide into cases depending on the signs of the factors involved. Conway [5] says "there is a really big problem with signs here, that actually makes it quite hard to define multiplication. Most authors split the argument into cases, which I think is morally wrong". Of course we cannot split into cases constructively whatever our moral compunctions. Troelstra and van Dalen [13] show that any locally uniformly continuous operation on $\mathbf{Q}$ can be extended uniquely to $\mathbf{R}^d$ and then leave the details of arithmetic on $\mathbf{R}^d$ to the reader.

The following algebraic theorem is convenient for defining multiplication of Dedekind cuts. It is a partial adoption of Conway's suggestion in [5] that one should construct the positive reals before constructing any negative numbers (which is what happened historically). More precisely, it allows you to define multiplication at first only on positive numbers, yet still avoid cases and maintain the traditional development.

Theorem 15 *Let A be an ordered abelian group. Suppose there is a multiplicative abelian group structure on the set P of positive elements of A that is distributive over addition in P. Then there is a unique commutative ring structure on A that extends the multiplication on P.*

Proof. For $x, y \in A$, let $a, b, c, d \in P$ so that $x = a - b$ and $y = c - d$. Define

$$xy = ac + bd - (ad + bc)$$

Clearly any ring structure on A extending the multiplication on P must satisfy this equation. We need to show that the product xy is well defined, that is, that it depends only on x and y and not on the particular choices of a, b, c, d. It suffices to show that if $a - b = a' - b'$ with $a', b' \in P$, then

$$ac + bd - (ad + bc) = a'c + b'd - (a'd + b'c)$$

that is

$$(a + b')\,c + (a' + b)\,d = (a' + b)\,c + (a + b')\,d$$

which holds because $a + b' = a' + b$.

Having shown that the product is well defined, it's clear that the multiplication is commutative and distributes over addition, and that the multiplicative identity of P is a multiplicative identity on A. To show that multiplication is associative, let x, y, z be elements of A. We can find $a, b, c, d \in P$ so that $x = a - d$, $y = b - d$, and $z = c - d$. Then

$$(xy)\,z = (abc + (a + b + c)\,d) - (ab + ac + bc + d)\,d^2$$

which is clearly symmetric in a, b, c, so $(xy)\,z = (yz)\,x = x\,(yz)$. ■

The positive cuts can be thought of as cuts in $\mathbf{Q}^+$, identifying the cut (L, U) in $\mathbf{Q}$ with the cut $(L \cap \mathbf{Q}^+, U)$ in $\mathbf{Q}^+$, and the cut (L, U) in $\mathbf{Q}^+$ with the cut (L', U) in $\mathbf{Q}$, where L' is the lower set generated by L. This is in line with Conway's suggestion. For cuts in $\mathbf{Q}^+$, addition is the same as before and we can define multiplication simply by

$$(L, U)\,(L', U') = (LL', UU')$$

Rather than prove that the Dedekind reals are complete, it seems more natural to prove that they constitute a terminal object in the category of archimedean Heyting fields. I won't give the rest of the details as to why the Dedekind reals are an archimedean Heyting field, but I will mention why they are terminal. Recall that if k is an archimedean Heyting field, then each element $x \in k$ gives rise to a cut by setting $L = \{q \in \mathbf{Q} : q < x\}$ and $U = \{q \in \mathbf{Q} : x < q\}$. The map taking x to this cut is the unique map from k to the Dedekind reals.

References

[1] Banaschewski, Bernhard, On proving the existence of complete ordered fields, *Amer. Math. Monthly* **105** (1998), 548–551

[2] Bishop, Errett, *Foundations of constructive analysis*, McGraw-Hill 1968

[3] Bridges, Douglas S., Constructive mathematics: a foundation for computable analysis, *Theoretical computer science*, **219** (1999) 95–109

[4] Bridges, Douglas S. and Luminiţa Simona Viţă, *Techniques of constructive analysis*, Springer, 2006

[5] Conway, John H., The surreals and the reals, in *Real Numbers, Generalizations of the Reals and Theories of Continua* (P. Ehrlich, ed.), pp. 93–106, Kluwer Academic Publishers, Amsterdam, 1994

[6] Grayson, Robin J., Concepts of general topology in constructive mathematics and in sheaves, II, *Annals of Mathematical Logic*, **23** (1982) 55–98.

[7] Hilbert, David, Über den Zahlbegriff, *Jber. Deutsche Math. Verein.* **8** (1900)

[8] Lubarsky, Robert S., *On the Cauchy completeness of the constructive Cauchy reals*, preprint www.math.fau.edu/lubarsky/Cauchyreals.pdf

[9] Richman, Fred, Generalized real numbers in constructive mathematics, *Indagationes Mathematicae*, **9** (1998) 595–606.

[10] ———, The fundamental theorem of algebra: a constructive development without choice, *Pacific Journal of Mathematics*, **196** (2000) 213-230.

[11] Rudin, Walter, *Principles of mathematical analysis*, McGraw-Hill 1964

[12] Stolzenberg, Gabriel, *Sets as limits*, preprint (1988)

[13] Troelstra, Anne and Dirk van Dalen, *Constructivism in mathematics, an introduction*, Volume 1, North-Holland 1988