Constructions of the real numbers a set theoretical approach

Lothar Sebastian Krapp

Mansfield College, University of Oxford

06 March 2014

Table of Contents

1 Introduction

- **2** Construction of the rational numbers
- **3** Classical approaches to completeness
- 4 A non-standard approach
- **5** Contrasting methods

Table of Contents

1 Introduction

2 Construction of the rational numbers

3 Classical approaches to completeness

4 A non-standard approach

5 Contrasting methods

Introduction

 $\mathbb R$ is widely introduced axiomatically as the (unique) complete linearly ordered field

- What is a real number in set theory?
- What makes $\mathbb R$ a linearly ordered field?
- What does completeness mean?
- What ways are there to fill the gaps in \mathbb{Q} ?

Introduction

Advice:

"Please forget everything you have learnt in school; for you have not learnt it."

- Edmund Landau in Grundlagen der Analysis (Foundations of Analysis)

Introduction

Process:

- $\bullet\,$ starting from $\mathbb N$ with addition and multiplication
- $\mathbb Z$ and $\mathbb Q$ obtained from $\mathbb N$ by elementary set operations
- different concepts applied to ${\mathbb Q}$ to obtain ${\mathbb R}$

Table of Contents

1 Introduction

2 Construction of the rational numbers

3 Classical approaches to completeness

4 A non-standard approach

5 Contrasting methods

Tools for the natural numbers

 $(\mathbb{N},+,\cdot)$ forms an ordered semiring:

$$(m+n) + k = m + (n+k)$$

$$m+n = n + m$$

$$n+0 = n$$

$$(m \cdot n) \cdot k = m \cdot (n \cdot k)$$

$$m \cdot n = n \cdot m$$

$$n \cdot 1 = n$$

$$m \cdot (n+k) = (m \cdot n) + (m \cdot k)$$

Tools for the natural numbers

If m < n, then m + k < n + k.

If m < n and 0 < k, then $k \cdot m < k \cdot n$.

If m < n and n < k, then m < k.

Exactly one of the following holds: m < n, m = n, or m < n.

Axiomatically $\ensuremath{\mathbb{Z}}$ can be introduced as the smallest ordered ring:

- addition, multiplication and an order relation are defined on $\ensuremath{\mathbb{Z}}$
- ($\mathbb{Z}, +, \cdot, <$) forms an ordered ring (CRI)
- for every other ordered ring *R*, there exists an injective ring homomorphism from Z to *R*

- crucial property of \mathbb{Z} : existence of additive inverses
- \rightarrow notion of subtraction
 - How can we define subtraction only using the tools for \mathbb{N} ?

- idea: consider ordered pairs of natural numbers
- ightarrow the pair $(n,m)\in\mathbb{N} imes\mathbb{N}$ corresponds to the integer n-m
 - problem: no unique representation of integers (e.g. (0,1) and (2,3) both correspond to -1)
 - solution: define an equivalence relation on $\mathbb{N}\times\mathbb{N}$

Definition

We define an equivalence relation (\sim) on $\mathbb{N} \times \mathbb{N}$ by

$$(n,m) \sim (k,\ell) : \iff n+\ell = k+m.$$

Use a more familiar notation for equivalence classes:

equivalence class of (n, m) denoted by [n - m]

$$[n-m] = [k-\ell] \Leftrightarrow n+\ell = k+m$$

Definition

The set of *integers* \mathbb{Z} is defined as the set of all equivalence classes in $\mathbb{N} \times \mathbb{N}$ under (\sim):

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N} / \sim) = \{[n - m] \mid n, m \in \mathbb{N} \times \mathbb{N}\}.$$

Definition

For $n, m, k, \ell \in \mathbb{N}$, we define

$$[n-m] +_{\mathbb{Z}} [k-\ell] := [(n+k) - (m+\ell)],$$

$$[n-m] \cdot_{\mathbb{Z}} [k-\ell] := [(n \cdot k + m \cdot \ell) - (n \cdot \ell + m \cdot k)],$$

$$[n-m] <_{\mathbb{Z}} [k-\ell] :\iff n+\ell < k+m.$$

Definition

Let $n, m, k, \ell \in \mathbb{N}$. The *negative* of an integer is defined as

$$-[n-m]:=[m-n].$$

We also define a new binary operator $(-\mathbb{Z})$ called *subtraction* on the integers:

$$[n-m] - \mathbb{Z} [k-\ell] := [n-m] + \mathbb{Z} (-[k-\ell]).$$

 \mathbb{N} is not a subset of \mathbb{Z} !

Define an embedding of \mathbb{N} into \mathbb{Z} : $i: n \mapsto \mathbf{n} := [n - 0]$

 $\mathbb{N}_{\mathbb{Z}}$ denotes the image of \mathbb{N} in \mathbb{Z}

Theorem

 $(\mathbb{Z},+_{\mathbb{Z}},\cdot_{\mathbb{Z}},<_{\mathbb{Z}})$ forms an ordered ring.

0 and **1** are the additive and multiplicative identities respectively; the additive inverse of an integer x is -x.

The structure of \mathbb{N} as its embedding $\mathbb{N}_{\mathbb{Z}}$ is preseverved in \mathbb{Z} .

 \implies We can use the same notation as on $\mathbb N.$

Axiomatically, \mathbb{Q} can be introduced as the smallest ordered field:

- addition, multiplication and an order relation are defined on ${\ensuremath{\mathbb Q}}$
- $(\mathbb{Q}, +, \cdot, <)$ forms an ordered field
- for every other ordered field K, there exists an injective field homomorphism from \mathbb{Q} to K

- crucial property of \mathbb{Q} : existence of multiplicative inverses \rightarrow notion of division
 - How can we define division only using the properties of \mathbb{Z} ?

- idea: consider ordered pairs of integers
- \rightarrow the pair $(n,m)\in\mathbb{Z} imes\mathbb{Z}^+$ corresponds to the rational $rac{n}{m}$
 - problem: no unique representation of rationals (e.g. (1,2) and (2,4) both correspond to ¹/₂)
 - \bullet solution: define an equivalence relation on $\mathbb{Z}\times\mathbb{Z}^+$

Definition

We define an equivalence relation (\sim) on $\mathbb{Z}\times\mathbb{Z}^+$ by

$$(n,m) \sim (k,\ell) : \iff n \cdot \ell = k \cdot m.$$

Use a more familiar notation for equivalence classes:

The equivalence class of (n, m) is denoted by $\frac{n}{m}$.

$$\frac{n}{m}=\frac{k}{\ell}\Leftrightarrow n\cdot\ell=k\cdot m.$$

Definition

The set of *rational numbers* \mathbb{Q} is defined as the set of all equivalence classes in $\mathbb{Z} \times \mathbb{Z}^+$ under (\sim):

$$\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^+ / \sim) = \left\{ \frac{n}{m} \mid n \in \mathbb{Z}, m \in \mathbb{Z}^+ \right\}.$$

Definition

For $n, m \in \mathbb{Z}, k, \ell \in \mathbb{Z}^+$, we define

$$\frac{n}{m} +_{\mathbb{Q}} \frac{k}{\ell} := \frac{(n \cdot \ell) + (k \cdot m)}{m \cdot \ell},$$
$$\frac{n}{m} \cdot_{\mathbb{Q}} \frac{k}{\ell} := \frac{n \cdot k}{m \cdot \ell},$$
$$\frac{n}{m} <_{\mathbb{Q}} \frac{k}{\ell} :\iff n \cdot \ell < k \cdot m.$$

Definition

Let $n, k \in \mathbb{Z}$ and $m, \ell \in \mathbb{Z}^+$. The *negative* of a rational is defined as

$$-\frac{n}{m}:=\frac{-n}{m}.$$

As on the integers, subtraction $(-_{\mathbb{Q}})$ is defined as

$$\frac{n}{m} - \mathbb{Q} \frac{k}{\ell} := \frac{n}{m} + \left(-\frac{k}{\ell}\right)$$

Definition

Suppose further that $n \neq 0$. We define the *(multiplicative) inverse* as

$$\left(\frac{n}{m}\right)^{-1} := \begin{cases} \frac{m}{n} & \text{, if } n > 0\\ \frac{-m}{-n} & \text{, if } n < 0 \end{cases}$$

We also define a new binary operator $(/_{\mathbb{Q}})$ called *division* on the rationals:

$$\frac{k}{\ell} /_{\mathbb{Q}} \frac{n}{m} := \frac{k}{\ell} \cdot_{\mathbb{Q}} \left(\frac{n}{m}\right)^{-1}$$

 $\mathbb Z$ is not a subset of $\mathbb Q!$

Define an embedding of \mathbb{Z} into \mathbb{Q} : $i: n \mapsto \mathbf{n} := \frac{n}{1}$

 $\mathbb{Z}_{\mathbb{Q}}$ denotes the image of \mathbb{Z} in \mathbb{Q}

Theorem

 $(\mathbb{Q},+_{\mathbb{Q}},\cdot_{\mathbb{Q}},<_{\mathbb{Q}})$ forms an ordered field.

0 and **1** are the additive and multiplicative identities respectively; the additive and multiplicative inverses of a rational **x** are $-\mathbf{x}$ and \mathbf{x}^{-1} respectively.

The structure of \mathbb{Z} as its embedding $\mathbb{Z}_{\mathbb{Q}}$ is preseverved in \mathbb{Q} .

 \implies We can use the same notation as on $\mathbb{Z}.$

Table of Contents

1 Introduction

2 Construction of the rational numbers

3 Classical approaches to completeness

4 A non-standard approach

5 Contrasting methods

A Dedekind cut on $\mathbb Q$ is a subset of $\mathbb Q$ satisfying the following properties:

- It contains a rational number, but it does not contain all rational numbers.
- 2 Every rational number of the set is smaller than every rational number not contained in the set.
- **3** It does not contain a greatest rational number.

We can formalise this as follows:

Definition (Dedekind cuts)

A set $\mathbf{r} \subset \mathbb{Q}$ is called a *(Dedekind) cut* (on \mathbb{Q}) if and only if it satisfies the following three conditions:

$$\emptyset \neq \mathbf{r} \neq \mathbb{Q}$$

$$\forall p \in \mathbf{r} \ \forall q \in \mathbb{Q} \setminus \mathbf{r} : \ p < q$$

$$\forall p \in \mathbf{r} \ \exists q \in \mathbf{r} : \ p < q$$

Definition

The set of real numbers $\mathbb R$ is defined as the set of all Dedekind cuts on $\mathbb Q.$

Check list:

- define addition, multiplication and an order relation
- define additive and multiplicative inverses
- define a structure preserving embedding of ${\mathbb Q}$ into ${\mathbb R}$
- check that ${\mathbb R}$ is an ordered field
- check that \mathbb{R} is complete
 - But what does that mean?

Structure preserving embedding:

$$i: \mathbb{Q} \to \mathbb{R}, \quad q \mapsto \mathbf{q} = \{p \in \mathbb{Q} \mid p < q\}.$$

Natural copy of \mathbb{Q} in \mathbb{R} :

 $\mathbb{Q}_{\mathbb{R}} := \{\mathbf{q} \mid q \in \mathbb{Q}\}$
Order relation on \mathbb{R} :

$$\mathbf{r} <_{\mathbb{R}} \mathbf{s} :\iff \mathbf{r} \subsetneq \mathbf{s}$$

Addition on \mathbb{R} :

$$\mathsf{r} +_{\mathbb{R}} \mathsf{s} := \{ p + q \mid p \in \mathsf{r}, q \in \mathsf{s} \}$$

Negative of a real number **r**:

$$-\mathbf{r} := \{ q \in \mathbb{Q} \mid \exists p > q : -p \in \mathbb{Q} \setminus \mathbf{r} \}.$$

Modulus:

$$|\mathbf{r}| := \mathbf{r} \cup (-\mathbf{r})$$

Multiplication on \mathbb{R} for $\mathbf{r}, \mathbf{s} \geq_{\mathbb{R}} \mathbf{0}$:

$$\mathsf{r} \cdot_{\mathbb{R}} \mathsf{s} := \{ p \cdot q \mid p \in \mathsf{r} \setminus \mathbf{0}, q \in \mathsf{s} \setminus \mathbf{0} \} \cup \mathbf{0}.$$

In the remaining cases:

$$\mathbf{r} \cdot_{\mathbb{R}} \mathbf{s} := \begin{cases} -(\mathbf{r} \cdot_{\mathbb{R}} |\mathbf{s}|), & \text{ if } \mathbf{r} \geq_{\mathbb{R}} \mathbf{0}, \mathbf{s} <_{\mathbb{R}} \mathbf{0} \\ -(|\mathbf{r}| \cdot_{\mathbb{R}} \mathbf{s}), & \text{ if } \mathbf{r} <_{\mathbb{R}} \mathbf{0}, \mathbf{s} \geq_{\mathbb{R}} \mathbf{0} \\ |\mathbf{r}| \cdot_{\mathbb{R}} |\mathbf{s}|, & \text{ if } \mathbf{r}, \mathbf{s} <_{\mathbb{R}} \mathbf{0}. \end{cases}$$

Multiplicative inverse:

If $s >_{\mathbb{R}} 0$, then

$$\mathbf{s}^{-1} := \left\{ q^{-1} \in \mathbb{Q} \mid \exists p \in \mathbb{Q} \setminus \mathbf{s} : p < q
ight\} \cup \mathbf{0}.$$

If $\boldsymbol{s} <_{\mathbb{R}} \boldsymbol{0},$ then

$$s^{-1} := -|s|^{-1}.$$

Theorem

 $(\mathbb{R},+_{\mathbb{R}},\cdot_{\mathbb{R}},<_{\mathbb{R}})$ forms an ordered field.

0 and **1** are the additive and multiplicative identities respectively; the additive and multiplicative inverses of a real x are -x and x^{-1} respectively.

Definition (Dedekind completeness)

A complete ordered field F is Dedekind complete if and only if every Dedekind cut on F has a least upper bound in F.

Theorem

The Dedekind real number system is Dedekind complete.

Outline of proof:

Let $\boldsymbol{\mathsf{A}}$ be a Dedekind cut on $\mathbb R$ $\boldsymbol{\mathsf{a}}:=\bigcup \boldsymbol{\mathsf{A}}$

- show that \mathbf{a} is a Dedekind cut on \mathbb{Q}
- show that $\boldsymbol{b} \leq_{\mathbb{R}} \boldsymbol{a}$ for all $\boldsymbol{b} \in \boldsymbol{\mathsf{A}}$
- show that $\mathbf{a} \leq_{\mathbb{R}} \mathbf{c}$ for every upper bound \mathbf{c} of \mathbf{A}

Definition

An ordered field F is supremum complete if and only if every non-empty subset of F which is bounded above has a least upper bound in F.

Dedekind completeness and supremum completeness are equivalent.

Idea:

Every real number is the limit point of a rational Cauchy sequence.

Once we have established the real numbers, we want that every real Cauchy sequence converges to a real number.

Let C be the set of all Cauchy sequences in \mathbb{Q} . Note that C is a ring.

When do two rational Cauchy sequences represent the same real number?

 \rightarrow Whenever they converge to the same limit.

Equivalently without mentioning limits: Whenever they only differ by a zero sequence.

Let I be the subset of C of all zero sequences.

$$I:=\left\{(a_n)\in C\mid \lim_{n\to\infty}a_n=0\right\}.$$

Note: (a_n) and (b_n) in C represent the same real number if and only if $(a_n) - (b_n) \in I$.

Theorem

I is a maximal ideal in C.

Corollary

The quotient ring C/I is a field.

Definition

The Cantor real number system \mathbb{R} is defined as the quotient of *C* with its maximal ideal *I*:

$$\mathbb{R}:=C/I.$$

Addition, multiplication, additive identity and inverses, and multiplicative identity are induced by C.

The natural embedding of ${\mathbb Q}$ into ${\mathbb R}$ is given by constant sequences.

Order on \mathbb{R} :

 $[(a_n)] <_{\mathbb{R}} [(b_n)] :\iff (\exists \delta \in \mathbb{Q}_{>0} \ \exists N \in \mathbb{N} \ \forall n \ge N : a_n > b_n + \delta).$

Theorem

 $(\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, <_{\mathbb{R}})$ forms an ordered field.

Definition (Cauchy completeness)

A complete ordered field F is Cauchy complete if and only if *every* Cauchy sequence in F has a limit point in F.

Theorem

The Cantor real number system is Cauchy complete.

Outline of proof:

Let $(\mathbf{a}_n)_n$ be a Cauchy sequence in \mathbb{R} .

Every member of the sequence is of the form $\mathbf{a}_n = \left(a_m^{(n)}\right)_m + I$, where $\left(a_m^{(n)}\right)_m$ is a rational Cauchy sequence.

Choose suitable $\ell_n \in \mathbb{N}$ such that for all $m, m' \ge \ell_n$, $\left|a_m^{(n)} - a_{m'}^{(n)}\right| < \frac{1}{n}$.

• show that $\mathbf{b} = (b_n)_n := \left(a_{\ell_n}^{(n)}\right)_n$ is a rational Cauchy sequence

• show that $(\mathbf{a}_n)_n$ converges to **b**

Table of Contents

1 Introduction

2 Construction of the rational numbers

3 Classical approaches to completeness

4 A non-standard approach

5 Contrasting methods

Non-standard models

Non-standard model of an algebraic construct: satisfies the usual axioms and contains an infinitely large element.

Different approaches to non-standard models of algebraic constructs:

- Internal Set Theory: Extend ZFC by further axioms to create non-standard sets
- Algebraic Extension: Adjoin an infinite element to the field, ring, semiring etc.
- Ultrapower construction: Use sequences on ultrafilters.

Ultrafilters

A set $\mathcal{U} \in \mathcal{P}(\mathbb{N})$ is called a (proper) filter on \mathbb{N} provided:

- $\mathbb{N} \in \mathcal{U}$ and $\emptyset \notin \mathcal{U}$ (properness)
- if $A, B \in U$, then $A \cap B \in U$ (finite intersection property)
- if $A \in \mathcal{U}$ and $A \subseteq B \subseteq \mathbb{N}$, then $B \in \mathcal{U}$ (superset property)

Ultrafilters

A filter is called ultrafilter if it is a maximal filter:

If $A \in \mathcal{P}(\mathbb{N})$, then either $A \in U$ or $\mathbb{N} \setminus A \in \mathcal{U}$.

It is called free if it has the freeness property:

If $A \in \mathcal{U}$, then A is infinite.

Ultrafilters

- a free ultrafilter exists (Tarski 1930)
- the proof requires the Axiom of Choice in the form of Zorn's Lemma
- it is non-constructive!

Let \mathcal{U} be an ultrafilter on \mathbb{N} .

Consider the ring of rational sequences $\mathbb{Q}^{\mathbb{N}}$.

• Define an equivalence relation on $\mathbb{Q}^{\mathbb{N}}$:

$$(a_n) \sim (b_n) : \iff \{n \in \mathbb{N} \mid a_n = b_n\} \in \mathcal{U}$$

- Two sequences are equivalent if and only if they agree on a set in $\ensuremath{\mathcal{U}}.$

Definition

The set of hyperrational numbers ${}^*\mathbb{Q}$ is the set of all equivalence classes in $\mathbb{Q}^{\mathbb{N}}$ under (\sim).

A natural embedding of \mathbb{Q} into $^*\mathbb{Q}$ is given by constant sequences. We denote it by $^{\sigma}\mathbb{Q}$ and its elements by q_{σ} .

Definition

Define an order relation (<_*) on ${}^*\mathbb{Q}$ by

$$[(a_n)] <_* [(b_n)] :\iff \{n \in \mathbb{N} \mid a_n < b_n\} \in \mathcal{U}.$$

• define a sequence $\omega_n = n$ in $\mathbb{Q}^{\mathbb{N}}$

• let
$$\omega = [(\omega_n)] \in {}^*\mathbb{Q}$$

- $\forall q_{\sigma} \in {}^{\sigma}\mathbb{Q}$: $q_{\sigma} <_{*} \omega$
- \Rightarrow an infinite element exists

- To show: ${}^*\mathbb{Q}$ is a field
- note that $(a_n)\sim (b_n)$ if and only if $(a_n)-(b_n)\sim 0_\sigma$
- Idea: express ${}^*\!\mathbb{Q}$ as a quotient of $\mathbb{Q}^{\mathbb{N}}$ with a maximal ideal

 $I := \{(a_n) \in {}^*\mathbb{Q} \mid (a_n) \sim o_n\}$, where (o_n) is the constant zero sequence

Theorem

I is a maximal ideal of $\mathbb{Q}^{\mathbb{N}}$. Hence, $\mathbb{Q}^{\mathbb{N}}/I$ is a field.

Theorem ${}^*\mathbb{Q} = \mathbb{Q}^{\mathbb{N}}/I$, and ${}^*\mathbb{Q}$ forms an ordered field.

Completeness through a quotient ring

- Problem: *Q contains infinitely large elements.
- → Consider the ring of finite hyperrationals $\mathcal{O} := \{ a \in {}^*\mathbb{Q} \mid \exists p_\sigma \in {}^{\sigma}\mathbb{Q} : a <_* p_\sigma \}$
 - Problem: \mathcal{O} contains infinitely small elements.
- → form the quotient with the ideal of infinitely small hyperrationals and zero $o := \{a \in {}^*\mathbb{Q} \mid \forall p_\sigma \in {}^{\sigma}\mathbb{Q} : |a| <_* |p_\sigma|\} \cup \{0_\sigma\}$

Completeness through a quotient ring

Theorem

o is a maximal ideal of \mathcal{O} . Hence, \mathcal{O}/o is a field.

Definition

Define the set of real numbers obtained by a ultrapower construction by

 $\mathbb{R} := \mathcal{O}/o.$

A non-typical notion of completeness

- What is the naturally arising version of completeness?
- Look at the standard approaches to completeness:
 - Dedekind cuts on ${\mathbb Q}$ correspond to real numbers
 - $\to\,$ completeness: there is a one-one correspondence between Dedekind cuts on $\mathbb R$ and real numbers
 - equivalence classes of Cauchy sequences on ${\mathbb Q}$ correpsond to real numbers
 - $\rightarrow\,$ completeness: every Cauchy sequence in $\mathbb R$ corresponds to a real number

A non-typical notion of completeness

General process:

- find a concept to fill the gaps in ${\mathbb Q}$ to obtain ${\mathbb R}$
- completeness: the same concept applied to ${\mathbb R}$ results in ${\mathbb R}$

⇒ "One cannot make a complete field completer."

A non-typical notion of completeness

Suggestion for a non-typical notion of completeness: Let F be an ordered field.

F is complete if and only if every bounded sequence in F is U-equivalent to a convergent sequence in F.

Table of Contents

1 Introduction

2 Construction of the rational numbers

3 Classical approaches to completeness

4 A non-standard approach



Equivalence of real number systems

- all notions of completeness (Dedekind, Cantor, supremum completeness) are equivalent:
 a field which is complete w.r.t. one version is also complete w.r.t. the others
- How do we know that the Dedekind real number system does not have properties that the Cantor real number system doesn't, or vice versa?

Equivalence of real number systems

Theorem

All sets satisfying the axioms of a complete ordered field are order-isomorphic.

Outline of proof:

Construct an order-isomorphism ϕ from F to K as follows:

- φ maps the subfield Q_F generated by 1_F to the subfield Q_K generated by 1_K (both isomorphic to Q)
- φ maps the least upper bound of a Dedekind cut on Q_F to the least upper bound of the corresponding Dedekind cut on Q_K
- show that ϕ is an order-isomorphism

Conclusion

- The complete ordered field of real numbers ${\mathbb R}$ is unique.
- Why are different notions of completeness useful?
- \to Note that we did not used all the properties of the ordered field $\mathbb Q$ to fill the gaps.
Conclusion

- Dedekind cuts can be performed on partially ordered sets.
- Cauchy sequences only require a notion of distance, not of order. (General applications in Topology.)

Conclusion

"Few mathematical structures have undergone as many revisions or have been presented in as many guises as the real numbers. Every generation re-examines the reals in the light of its values and mathematical objectives." – E Faltin N. Metropolis B. Ross and G.-C. Rota in The Real Numbers as a

– F. Faltin, N. Metropolis, B. Ross and G.-C. Rota in *The Real Numbers as a Wreath Product*