Numbers for Rudin

ℕaproche Formalization: Peter Koepke

July 11, 2023

The ℕaproche system checks the logical correctness of texts written in an input language which ideally is readable like common mathematical language. Proof structures should resemble the style of undergraduate textbooks. To test this idea we have formalized number systems that are assumed or developed in the first chapter of the *Principles of Mathematical Analysis* by Walter Rudin [1] in the LaTeX dialect of the input language ForTheL.

Our approach parallels material on pages 1 to 9 of [1]. The ordered field $\mathbb{R}$ of real numbers is postulated axiomatically. We construe the structures of integer and rational numbers as substructures of $\mathbb{R}$:

$$\mathbb{R} \supseteq \mathbb{Q} \supseteq \mathbb{Z} \supseteq \mathbb{N}.$$

This has the advantage that the real addition and multiplication can be used on those substructures.

Our axioms parallel axioms and the explicit construction of $\mathbb{R}$ from $\mathbb{Q}$ in the Appendix of Chapter 1. A large part of the material of Rudin appears in the formalization in some form but we have restructured the original to simplify the proof checking. E.g., we have turned axioms about general linear orders and fields into axioms for the real numbers. Labels of definitions and theorems refer to similar labels in the original. Checking the formalization with a 10 second time out for the ATP takes 6 or 7 minutes on a modest laptop.

0.1 Importing Set-Theoretic Preliminaries

[timelimit 10]

[readtex preliminaries.ftl.tex]

Let A, B stand for sets. Let x is in A denote x is an element of A.

Definition 1 (1 3). A is nonempty iff A has an element.

1 The Real Field

[synonym number/-s]

Signature 2. A real number is a mathematical object.

Definition 3. $\mathbb{R}$ is the collection of real numbers.

Let x, y, z denote real numbers.

Axiom 4. $\mathbb{R}$ is a set.

Signature 5 (1 12 A1). $x + y$ is a real number.

Let the sum of x and y stand for $x + y$.

Signature 6 (1 12 M1). $x \cdot y$ is a real number.

Let the product of x and y denote $x \cdot y$.

Signature 7 (1 5). $x < y$ is an atom.

Let $x > y$ stand for $y < x$. Let $x \leq y$ stand for $x < y \vee x = y$. Let $x \geq y$ stand for $y \leq x$.

Axiom 8 (1 5 i). $(x < y \wedge x \neq y) \wedge noty < x$ or $notx < y \wedge x = y \wedge noty < x$ or $notx < y \wedge x \neq y \wedge y < x$.

Axiom 9 (1 5 ii). If $x < y$ and $y < z$ then $x < z$.

Proposition 10. $x \leq y$ iff not $x > y$.

Axiom 11 (1 12 A2). $x + y = y + x$.

Axiom 12 (1 12 A3). $(x + y) + z = x + (y + z)$.

Signature 13 (1 12 A4). 0 is a real number such that for every real number x $x + 0 = x$.

Signature 14 (1 12 A5). $-x$ is a real number such that $x + (-x) = 0$.

Axiom 15 (1 12 M2). $x \cdot y = y \cdot x$.

Axiom 16 (1 12 M3). $((x \cdot y)) \cdot z = x \cdot (y \cdot z)$.

Signature 17 (1 12 M4). 1 is a real number such that $1 \neq 0$ and for every real number x $1 \cdot x = x$.

Signature 18 (1 12 M5). Assume $x \neq 0$. $1/x$ is a real number such that $x \cdot (1/x) = 1$.

Axiom 19 (1 12 D). $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Proposition 20 (Dist1). $((y \cdot x)) + (z \cdot x) = (y + z) \cdot x$.

Proposition 21 (1 14 a). If $x + y = x + z$ then $y = z$.

Proof. Assume $x + y = x + z$. Then

$$y = (-x + x) + y = -x + (x + y) = -x + (x + z) = (-x + x) + z = z.$$

□

Proposition 22 (1 14 b). If $x + y = x$ then $y = 0$.

Proposition 23 (1 14 c). If $x + y = 0$ then $y = -x$.

Proposition 24 (1 14 d). $-(-x) = x$.

Proposition 25 (1 15 a). If $x \neq 0$ and $x \cdot y = x \cdot z$ then $y = z$.

Proof. Let $x \neq 0$ and $x \cdot y = x \cdot z$.

$$y = 1{\cdot}y = ((1/x){\cdot}x){\cdot}y = (1/x){\cdot}(x{\cdot}y) = (1/x){\cdot}(x{\cdot}z) = ((1/x){\cdot}x){\cdot}z = 1{\cdot}z = z.$$

□

Proposition 26 (1 15 b). If $x \neq 0$ and $x \cdot y = x$ then $y = 1$.

Proposition 27 (1 15 c). If $x \neq 0$ and $x \cdot y = 1$ then $y = 1/x$.

Proposition 28 (1 15 d). If $x \neq 0$ then $1/(1/x) = x$.

Proposition 29 (1 16 a). $0 \cdot x = 0$.

Proposition 30 (1 16 b). If $x \neq 0$ and $y \neq 0$ then $x \cdot y \neq 0$.

Proposition 31 (1 16 c). $(-x) \cdot y = -(x \cdot y)$.

Proof. $((x \cdot y)) + ((-x \cdot y)) = (x + (-x)) \cdot y = 0 \cdot y = 0$. □

Proposition 32. $-x = -1 \cdot x$.

Proposition 33 (1 16d). $(-x) \cdot (-y) = x \cdot y$.

Proof. $(-x) \cdot (-y) = -(x \cdot (-y)) = -((-y) \cdot x) = -(-(y \cdot x)) = y \cdot x = x \cdot y$.
□

Let $x - y$ stand for $x + (-y)$. Let $\frac{x}{y}$ stand for $x \cdot (1/y)$.

2 The Real Ordered Field

Axiom 34 (1 17 i). If $y < z$ then $x + y < x + z$ and $y + x < z + x$.

Axiom 35 (1 17 ii). If $x > 0$ and $y > 0$ then $x \cdot y > 0$.

Definition 36. x is positive iff $x > 0$.

Definition 37. x is negative iff $x < 0$.

Proposition 38 (1 18 a). $x > 0$ iff $-x < 0$.

Proposition 39 (1 18 b). If $x > 0$ and $y < z$ then $x \cdot y < x \cdot z$.

Proof. Let $x > 0$ and $y < z$. $z - y > y - y = 0$. $x \cdot (z - y) > 0$. $x \cdot z = (x \cdot (z - y)) + (x \cdot y)$. $((x \cdot (z - y))) + (x \cdot y) > 0 + (x \cdot y)$ (by 1 17i). $0 + (x \cdot y) = x \cdot y$. □

Proposition 40 (1 18 bb). If $x > 0$ and $y < z$ then $y \cdot x < z \cdot x$.

Proposition 41 (1 18 d). If $x \neq 0$ then $x \cdot x > 0$.

Proof. Let $x \neq 0$. Case $x > 0$. Then thesis. end. Case $x < 0$. Then $-x > 0$. end. □

Proposition 42 (1 18 dd). $1 > 0$.

Proposition 43. $x < y$ iff $-x > -y$.

Proof. $x < y \iff x - y < 0$. $x - y < 0 \iff (-y) + x < 0$. $(-y) + x < 0 \iff (-y) + (-(-x)) < 0$. $(-y) + (-(-x)) < 0 \iff (-y) - (-x) < 0$. $(-y) - (-x) < 0 \iff -y < -x$. □

Proposition 44 (1 18 c). If $x < 0$ and $y < z$ then $x \cdot y > x \cdot z$.

Proof. Let $x < 0$ and $y < z$. $-x > 0$. $(-x) \cdot y < (-x) \cdot z$ (by 1 18b). $-(x \cdot y) < -(x \cdot z)$. □

Proposition 45 (1 18 cc). If $x < 0$ and $y < z$ then $y \cdot x > z \cdot x$.

Proposition 46. $x + 1 > x$.

Proposition 47. $x - 1 < x$.

Proposition 48 (1 18 e). If $0 < y$ then $0 < 1/y$.

Proposition 49 (1 18 ee). Assume $0 < x < y$. Then $1/y < 1/x$.

Proof. Case $1/x < 1/y$. Then

$$1 = x \cdot (1/x) = (1/x) \cdot x < (1/x) \cdot y = y \cdot (1/x) < y \cdot (1/y) = 1.$$

Contradiction. end.

Case $1/x = 1/y$. Then

$$1 = x \cdot (1/x) < y \cdot (1/y) = 1.$$

Contradiction. end.

Hence $1/y < 1/x$ (by 1 5 i). □

3 Upper and lower bounds

Let E denote a subset of $\mathbb{R}$.

Definition 50 (1 7). An upper bound of E is a real number b such that for all elements x of E $x \leq b$.

Definition 51 (1 7a). E is bounded above iff E has an upper bound.

Definition 52 (1 7b). A lower bound of E is a real number b such that for all elements x of E $x \geq b$.

Definition 53 (1 7c). E is bounded below iff E has a lower bound.

Definition 54 (1 8). A least upper bound of E is a real number a such that a is an upper bound of E and for all x if $x < a$ then x is not an upper bound of E.

Definition 55 (1 8a). Let E be bounded below. A greatest lower bound of E is a real number a such that a is a lower bound of E and for all x if $x > a$ then x is not a lower bound of E.

Axiom 56 (1 19). Assume that E is nonempty and bounded above. Then E has a least upper bound.

Definition 57. $E^- = \{-x \in \mathbb{R} \mid x \in E\}$.

Lemma 58. E^- is a subset of $\mathbb{R}$.

Lemma 59. x is an upper bound of E iff $-x$ is a lower bound of E^-.

Theorem 60 (1 11). Assume that E is a nonempty subset of $\mathbb{R}$ such that E is bounded below. Then E has a greatest lower bound.

Proof. Take a lower bound a of E. $-a$ is an upper bound of E^-. Take a least upper bound b of E^-. Let us show that $-b$ is a greatest lower bound of E. $-b$ is a lower bound of E. Let c be a lower bound of E. Then $-c$ is an upper bound of E^-. end. □

4 The rational numbers

[synonym number/numbers]

Signature 61 (1 19a). A rational number is a real number.

Let p, q, r denote rational numbers.

Definition 62. $\mathbb{Q}$ is the collection of rational numbers.

Theorem 63. $\mathbb{Q}$ is a set.

Proof. $\mathbb{Q}$ is a subset of $\mathbb{R}$. □

Theorem 1.19 of [1] states that $\mathbb{Q}$ is a subfield of $\mathbb{R}$. We require this axiomatically.

Lemma 64. $\mathbb{Q} \subseteq \mathbb{R}$.

Axiom 65. $p + q$, $p \cdot q$, 0, $-p$, 1 are rational numbers.

Axiom 66. Assume $p \neq 0$. $1/p$ is a rational number.

Axiom 67. There exists a subset A of $\mathbb{Q}$ such that A is bounded above and x is a least upper bound of A.

Theorem 68. $\mathbb{R} = \{x \in \mathbb{R} \mid \text{there exists } A \subseteq \mathbb{Q} \text{ such that } A \text{ is bounded above and } x \text{ is a least upper bound of } A\}$.

5 Integers

[synonym integer/-s]

Signature 69. An integer is a rational number.

Let a, b, i stand for integers.

Definition 70. $\mathbb{Z}$ is the collection of integers.

Theorem 71. $\mathbb{Z}$ is a subset of $\mathbb{R}$.

$\mathbb{Z}$ is a discrete subring of $\mathbb{Q}$:

Axiom 72. $a + b$, $a \cdot b$, 0, $-a$, 1 are integers.

Axiom 73. There is no integer a such that $0 < a < 1$.

Axiom 74. There exist a and b such that $a \neq 0 \wedge p = \frac{b}{a}$.

Theorem 75 (Archimedes1). $\mathbb{Z}$ is not bounded above.

Proof. Assume the contrary. $\mathbb{Z}$ is nonempty. Indeed 0 is an integer. Take a least upper bound b of $\mathbb{Z}$. Let us show that $b - 1$ is an upper bound of $\mathbb{Z}$. Let $x \in \mathbb{Z}$. $x + 1 \in \mathbb{Z}$. $x + 1 \leq b$. $x = (x + 1) - 1 \leq b - 1$. end. □

Theorem 76. $\mathbb{Z}$ is not bounded below.

Proof. Assume the contrary. Take an integer m that is a lower bound of $\mathbb{Z}$. Then $-m$ is an upper bound of $\mathbb{Z}$. Contradiction. □

Theorem 77 (Archimedes2). Let x be a real number. Then there is an integer a such that $x < a$.

Proof by contradiction. Assume the contrary. Then x is an upper bound of $\mathbb{Z}$. Contradiction. □

6 The natural numbers

Definition 78. $\mathbb{N}$ is the collection of positive integers.

Let m, n stand for positive integers.

Lemma 79. $\mathbb{N}$ is a subset of $\mathbb{R}$.

Definition 80. $\{x\} = \{y \in \mathbb{R} \mid y = x\}$.

Lemma 81. $\mathbb{Z} = (\mathbb{N}^{-} \cup 0) \cup \mathbb{N}$.

Theorem 82 (Induction Theorem). Assume $A \subseteq \mathbb{N}$ and $1 \in A$ and for all $n \in A$ $n + 1 \in A$. Then $A = \mathbb{N}$.

Proof. Let us show that every element of $\mathbb{N}$ is an element of A. Let $n \in \mathbb{N}$. Assume the contrary. Define $F = \{j \in \mathbb{N} \mid j \notin A\}$. F is nonempty. F is bounded below. Take a greatest lower bound a of F. Let us show that

$a+1$ is a lower bound of F. Let $x \in F$. $x-1 \in \mathbb{Z}$.

Case $x-1 < 0$. Then $0 < x < 1$. Contradiction. end.

Case $x-1 = 0$. Then $x = 1$ and $1 \notin A$. Contradiction. end.

Case $x-1 > 0$. Then $x-1 \in \mathbb{N}$. $x-1 \notin A$. Indeed $(x-1)+1 = x \notin A$. $x-1 \in F$. $a \leq x-1$. $a+1 \leq (x-1)+1 = x$. end. end.

Then $a+1 > a$. Contradiction. end. □

Lemma 83. There is an integer m such that $m-1 \leq x < m$.

Proof. Assume the contrary. Then for all m such that $x \geq m-1$ we have $x \geq m$. Take an integer n such that $n < x$. Define

$$A = \{i \in \mathbb{N} \mid n + (i-1) \leq x\}.$$

(1) $A = \mathbb{N}$.

Proof. $A \subseteq \mathbb{N}$. $1 \in A$.

For all $i \in A$ $i+1 \in A$.

Proof. Let $i \in A$. Then $n+(i-1) = (n+i)-1 \leq x$ and $n+((i+1)-1) = n+i \leq x$. Hence $i+1 \in A$. qed.

qed.

(2) $x+1$ is an upper bound of $\mathbb{Z}$.

Proof. Let j be an integer. Let us show that $j \leq x+1$.

Case $j \leq n$. Trivial.

Then $j > n$. Take a positive integer i such that $j = n+i$. $i \in A$. Hence $n+(i-1) \leq x$ and $j = n+i \leq x+1$. qed.

qed.

Contradiction. □

7 Archimedian properties

Theorem 84 (1 20 a). Let $x > 0$. Then there is a positive integer n such that

$$n \cdot x > y.$$

Proof. Take an integer a such that $a > \frac{y}{x}$. Take a positive integer n such that $n > a$. $n > \frac{y}{x}$ and $n \cdot x > (\frac{y}{x}) \cdot x = y$. □

Theorem 85 (1 20 b). Let $x < y$. Then there exists $p \in \mathbb{Q}$ such that $x < p < y$.

Proof. We have $y-x > 0$. Take a positive integer n such that $n \cdot (y-x) > 1$

(by 1 20 a). Take an integer m such that

$$m - 1 \leq n \cdot x < m.$$

Then

$$n{\cdot}x < m = (m{-}1){+}1 \leq (n{\cdot}x){+}1 < (n{\cdot}x){+}(n{\cdot}(y{-}x)) = n{\cdot}(x{+}(y{-}x)) = n{\cdot}y.$$

$n > 0$ and

$$x = \frac{n \cdot x}{n} < \frac{m}{n} < \frac{n \cdot y}{n} = y.$$

Let $p = \frac{m}{n}$. Then $p \in \mathbb{Q}$ and $x < p < y$. □

References

[1] Walter Rudin. *Principles of Mathematical Analysis*.