Constructing the Reals from the Integers

(an Exercise in Mathematical Methodology)

Jean-Raymond Abrial and Dominique Cansell

Marseille and Lessy, France, EBRP

Abstract. This paper contains a formal presentation of the construction of Real Numbers as proposed by various authors some years ago. One insists in presenting this mathematical work in a systematic fashion inherited from the usage of formal methods in system modeling. This work is a preparation for a complete mechanized development with a theorem prover. This work was done in 2012 and proved using Rodin in 2021 in the EBRP project. Some (little) errors are detected and corrected during the proof

1 Introduction

The writing of this paper originated in my frustration. Let me explain why in this introduction.

I discovered recently that besides the well known classical constructions of the Reals (that named after Cauchy or that named after Dedekind) there was another one that was quite attractive. Both Cauchy series approach or Dedekind cuts approach present some constructions of the Reals that are based on the Rationals, themselves based on the Integers, themselves ultimately based on the Natural Numbers. The new approach presents some advantages over the classical ones: it is only based on the Integers and, moreover, it is constructed out of very simple concepts only, namely elementary integer arithmetics, absolute values, intervals, integer order, minimum, maximum, and so on. For all these reasons, this new approach is particularly attractive, specially for people who want to construct the Reals in a purely formal way with a theorem prover.

I was aware that this new approach had been proposed originally by Stephen Schanuel (University at Buffalo, the State University of New York). However, Schanuel did not publish it. This construction was only first made publicly available in a short note [1] by Ross Street in 1985. Street had been introduced to this question by Schanuel. More recently, in 2002, 2003 and 2004, several people ([2], [3], [4], [5], [6]) worked on this subject, sometimes independently as Norbert A'Campo did in [3].

Very attracted by these preliminary investigations, I engaged in the careful reading of the above referenced papers. After a while however, I started to become frustrated. I must admit that I had some difficulties in getting familiar with the material. It was particularly frustrating as there is absolutely no difficult mathematical notions at work in these presentations. As said above, only very simple concepts are in use. So the question is: why was it so difficult (at least for me) to feel at ease with all this?

My main complaint is the following: there is almost no intuitive motivations accompanying these presentations. For instance, proposed constructs for the various classical arithmetic operations on Reals (addition, multiplication, inverses, supremum) are taken out of a hat without any explanations. So, when reading the papers, you "see" (painfully for me) that it works but you don't really understand why. Theorems and lemmas follow each other without any apparent reasons and are often later used without being mentioned explicitly: this makes the verification of some claims highly time consuming. Proofs are sometimes difficult to understand as there are many important steps missing. More seriously, some proofs are simply absent: they are said to be obvious although they are difficult to reconstruct (at least for me). Serious typos make here and there the reading problematic: you spend quite a long time trying to understand some formal development until you discover that there is nothing to understand as the development in question is just a complete misprint. The mathematical style is sometimes difficult to decipher. For instance, one can read some logical statements as "there exists x such that some predicate on x and y hold, for all y": it is not clear whether it means "$\exists x \cdot \forall y \ldots$" or "$\forall y \cdot \exists x \ldots$". And so on ...

However, despite these difficulties, I must say that I remained still very interested by this approach. It is clear that I learned a lot from what I read, in particular from Norbert A'Campo in [3] and Rob Arthan in [4]. So, gradually, I came up with the idea to write a *synthesis* between all these papers, trying (subjectively) to take the best of each of them, while adding my own few contributions. This results in what you are going to read in the sequel.

The paper is organized as follows. I first present some motivations and preliminary investigations in section 2: the idea is to help the reader to later better understand the future construction done in section 4. Such hints are extracted from a few simple things we already know about the Reals. The hurried reader can skip section 2 as it only indicates some clues that help understanding some of the decisions made in section 4. Then I recall the 17 axioms of the Reals in section 3: this dictates exactly what is to be proved in the proposed model of the Reals. Finally, I present it in section 4.

You will notice that the mathematical construction done in section 4 contains lots of details for the proofs. More, in fact, than what is usually the case in similar papers. This is done on purpose in preparation for the complete future formal development done with the Rodin Platform [7].

2 Intuitive Motivations and Preliminary Investigations

In the introduction, I said that I had difficulties in finding intuitive motivations in the referenced papers. This is not entirely true. Here is a little one that is quoted from [2]:

> Notice that a real number α determines a function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = \text{ip}(\alpha n)$ where "ip" denotes "integer part". Then $f(n)/n \to \alpha$ as $n \to \infty$ and $|f(m+n) - f(m) - f(n)| \leq 3$. From this motivation we attempt to construct the real number system directly from the set of integers and quasi-homomorphism functions in $\mathbb{Z}^{\mathbb{Z}}$.[1]

This is very interesting. It pushes me to investigate about this function f, mentioned in [2]. It yields an *approximation* of the real α. It emphasizes, as we know, that a real number is definitely an *infinite object*. It is the result of an infinite refinement process going from finite integer or rational abstractions down to an ultimate infinite concrete "real" object.

Again, this section is not indispensable for the main construction done in section 4. We suppose here that we already have the set $\mathbb{R}$ of Real Number (given to us either by the axiomatic definition of section 3 or by the classical constructions of Cauchy or Dedekind), and we study how such numbers can be approximated in various ways. Such approximations will give us some clues for the construction done in section 4.

This section is organized as follows: in section 2.1, I recall the definition and properties of the "integer part" function. Then, in section 2.2, I define the approximation function approx (that called f in [2]). In subsequent sections, I study some of the properties of the function approx. I also envisage how this function can itself be approximated.

2.1 Reminder: Floor, Ceiling and Integer Part Functions

As shown below, the "integer part" function is defined in terms of the well known "floor" and "ceiling" functions. So, let us define these ones first. The *floor*, $\lfloor x \rfloor$, the ceiling, $\lceil x \rceil$, and the *integer part*, $\lfloor x \rceil$, of a

[1] The statement $|f(m+n) - f(m) - f(n)| \leq 3$ is a bit weak. It should be $|f(m+n) - f(m) - f(n)| \leq 1$ as we show below in section 2.3.

real number x are defined as follows:

$$\boxed{\begin{array}{l} \lfloor x \rfloor \;\widehat{=}\; \max\left(\{n \mid n \in \mathbb{Z} \;\wedge\; n \leq x\}\right) \\ \lceil x \rceil \;\widehat{=}\; \min\left(\{n \mid n \in \mathbb{Z} \;\wedge\; n \geq x\}\right) \\ \lfloor x \rceil \;\widehat{=}\; \begin{cases} \lfloor x \rfloor & \text{if } x \geq 0 \\ \lceil x \rceil & \text{if } x \leq 0 \end{cases} \end{array}}$$

Definition 1

Examples:

$$\lfloor 3.2 \rfloor = 3 \quad \lceil 3.2 \rceil = 4 \quad \lfloor -3.2 \rfloor = -4 \quad \lceil -3.2 \rceil = -3 \quad \lfloor 3.2 \rceil = 3 \quad \lfloor -3.2 \rceil = -3$$

These functions are members of $\mathbb{R} \to \mathbb{Z}$. They enjoy the following properties:

$$0 \leq x - \lfloor x \rfloor < 1 \qquad \underline{0 \leq \lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \leq 1} \qquad x < 0 \Rightarrow \lfloor x \rfloor < 0 \qquad x > 0 \Rightarrow \lfloor x \rfloor \geq 0$$

$$-1 < x - \lceil x \rceil \leq 0 \qquad -1 \leq \lceil x+y \rceil - \lceil x \rceil - \lceil y \rceil \leq 0 \qquad x < 0 \Rightarrow \lceil x \rceil \leq 0 \qquad x > 0 \Rightarrow \lceil x \rceil > 0$$

$$-1 < x - \lfloor x \rceil \leq 1 \qquad -1 \leq \lfloor x+y \rceil - \lfloor x \rceil - \lfloor y \rceil \leq 1 \qquad x < 0 \Rightarrow \lfloor x \rceil \leq 0 \qquad x > 0 \Rightarrow \lfloor x \rceil \geq 0$$

$$x \leq y \;\Rightarrow\; \lfloor x \rfloor \leq \lfloor y \rfloor \;\wedge\; \lceil x \rceil \leq \lceil y \rceil \;\wedge\; \lfloor x \rceil \leq \lfloor y \rceil$$

$$\lfloor x \rfloor = -\lceil -x \rceil \qquad \lceil x \rceil = -\lfloor -x \rfloor \qquad \lfloor x \rceil = -\lfloor -x \rceil$$

Proof of the underlined statement[2]**.** From the definition of $\lfloor x \rfloor$:

$$\lfloor x \rfloor \;\widehat{=}\; \max\left(\{n \mid n \in \mathbb{Z} \;\wedge\; n \leq x\}\right)$$

we obtain:

$$\lfloor x \rfloor \leq x \qquad \lfloor x \rfloor + 1 > x$$

Thus

$$\begin{array}{l} \lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \\ = \\ (\lfloor x+y \rfloor - (x+y)) + (x - \lfloor x \rfloor) + (y - \lfloor y \rfloor) \\ < \\ 0+1+1 = 2 \end{array}$$

and

$$\begin{array}{l} \lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \\ = \\ (\lfloor x+y \rfloor - (x+y)) + (x - \lfloor x \rfloor) + (y - \lfloor y \rfloor) \\ > \\ -1+0+0 = -1 \end{array}$$

Thus

$$-1 < \lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor < 2$$

That is

$$0 \leq \lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \leq 1$$

■

[2] Other statements are proved in a similar way.

As can be seen, the integer part function is more "regular" than the floor or ceiling functions. Examples:

$$\lfloor(-3.2)+2.9\rfloor-\lfloor-3.2\rfloor-\lfloor2.9\rfloor=1 \qquad \lfloor3.2+(-2.9)\rfloor-\lfloor3.2\rfloor-\lfloor-2.9\rfloor=0$$

$$\lceil(-3.2)+2.9\rceil-\lceil-3.2\rceil-\lceil2.9\rceil=0 \qquad \lceil3.2+(-2.9)\rceil-\lceil3.2\rceil-\lceil-2.9\rceil=-1$$

$$\lfloor(-3.2)+2.9\rceil-\lfloor-3.2\rceil-\lfloor2.9\rceil=1 \qquad \lfloor3.2+(-2.9)\rceil-\lfloor3.2\rceil-\lfloor-2.9\rceil=-1$$

When x is an integer, we have:

$$\lfloor x\rfloor=\lceil x\rceil=\lfloor x\rceil=x$$

When x is not an integer, we have:

$$x-1<\lfloor x\rfloor<x<\lceil x\rceil<x+1 \qquad \lceil x\rceil-\lfloor x\rfloor=1 \qquad -1<x-\lfloor x\rceil<1$$

2.2 Approximations of Real Numbers

Real numbers can be approximated to successive rational numbers. For instance, the number π, whose decimal representation is 3.1415926 . . . , can be approximated to its integer part, 3, then to its first decimal, 3.1, then to its second decimal, 3.14, and so on. Each of these approximations is equal to $\frac{\lfloor 10^m\pi\rceil}{10^m}$ for m being 0, 1, 2, and so on. More generally, we define a function approx as follows:

$$\boxed{\begin{array}{l}\mathsf{approx}\in\mathbb{R}\to(\mathbb{Z}\to\mathbb{Z})\\ \mathsf{approx}(r)(n)\ \widehat{=}\ \lfloor r*n\rceil\end{array}}$$

Definition 2

Successive approximations of the real r are then given by the rational $\frac{\mathsf{approx}(r)(n)}{n}$ where n is supposed to be positive. As an example, let us define the function approx for r being equal to $\sqrt{2}$. For n positive, we have:

$$\mathsf{approx}(\sqrt{2})(n)\ =\ \lfloor\sqrt{2}{*}n\rceil\ =\ \max(\{\,k\mid k\in\mathbb{Z}\wedge k\le\sqrt{2}{*}n\,\})\ =\ \max(\{\,k\mid k\in\mathbb{N}\wedge k^2\le 2{*}n^2\,\})$$

Example:

n	1	10	100	1,000	10,000	100,000
$\max(\{\,k\mid k\in\mathbb{N}\ \wedge\ k^2\le 2*n^2\,\})$	1	14	141	1,414	14,142	141,421
$\frac{\max(\{\,k\mid k\in\mathbb{N}\wedge k^2\le 2*n^2\,\})}{n}$	1	1.4	1.41	1.414	1.4142	1.41421

2.3 Properties of the Function approx

The function approx has a number of interesting properties among which some are listed below as P1, P2, P3[3] , and P4. These properties, except the last one, are immediate consequences of the properties of the integer part function already encountered in section 2.1:

[3] P3 is due to the following result stated in section 2.1: $-1\le\lfloor x+y\rceil-\lfloor x\rceil-\lfloor y\rceil\le 1$.

$$\mathsf{P1}: \quad \forall\, r \cdot r \in \mathbb{R} \;\Rightarrow\; \mathsf{approx}(r)(0) = 0$$

$$\mathsf{P2}: \quad \forall\, r, n \cdot r \in \mathbb{R} \;\wedge\; n < 0 \;\Rightarrow\; \mathsf{approx}(r)(n) = -\mathsf{approx}(r)(-n)$$

$$\mathsf{P3}: \quad \forall\, r, m, n \cdot \; r \in \mathbb{R} \;\wedge\; m \in \mathbb{N}_1 \;\wedge\; n \in \mathbb{N}_1 \;\Rightarrow\; |\, \mathsf{approx}(r)(m+n) - \mathsf{approx}(r)(m) - \mathsf{approx}(r)(n) \,| \leq 1$$

$$\mathsf{P4}: \quad \lim_{n\to\infty} \frac{\mathsf{approx}(r)(n)}{n} = r$$

When dealing with the function approx, it is then sufficient to give its value for n positive and use $\mathsf{P2}$ and $\mathsf{P1}$ to define its values for n negative or equal to 0. Property $\mathsf{P4}$ is the most important of all these properties: it shows how $\mathsf{approx}(r)$ can be used to approximate the real r.

2.4 Values of the Function approx for Integers

For an integer i, we have:

$$\mathsf{approx}(i)(n) = \lfloor i * n \rceil = i * n$$

2.5 Approximation of the function $\mathsf{approx}(r)$

As far as limits are concerned and in view of property $\mathsf{P4}$ of section 2.3, the function $\mathsf{approx}(r)$ can itself be approximated by a function f of $\mathbb{Z} \to \mathbb{Z}$. This can be done if $\frac{f(n)}{n}$ yields the same limit as $\frac{\mathsf{approx}(r)(n)}{n}$ does when $n \to \infty$, namely r. This is indeed the case when the absolute value of the difference between the two is *bounded*. More precisely, we have the following:

$$(\exists\, k \cdot k \in \mathbb{N} \;\wedge\; (\forall n \cdot n \in \mathbb{Z} \;\Rightarrow\; |\, f(n) - \mathsf{approx}(r)(n) \,| \leq k)) \;\Rightarrow\; \lim_{n\to\infty} \frac{f(n)}{n} \;=\; r$$

The proof of this very classical property is beyond the scope of this paper. Note that the condition:

$$\exists\, k \cdot k \in \mathbb{N} \;\wedge\; (\forall n \cdot n \in \mathbb{Z} \;\Rightarrow\; |\, f(n) - \mathsf{approx}(r)(n) \,| \leq k)$$

could be equivalently replaced by $f(n) - \mathsf{approx}(r)(n)$ takes *finitely many* values for $n \in \mathbb{Z}$:

$$\mathrm{finite}(\{\, n \cdot n \in \mathbb{Z} \,|\, f(n) - \mathsf{approx}(r)(n) \,\})$$

This condition can also be replaced equivalently by:

$$\exists\, a, b \cdot a \in \mathbb{Z} \;\wedge\; b \in \mathbb{Z} \;\wedge\; (\forall n \cdot n \in \mathbb{Z} \;\Rightarrow\; f(n) - \mathsf{approx}(r)(n) \in a \,..\, b)$$

If the function f enjoys the following additional properties

$$f(0) = 0 \qquad\qquad \forall\, n \cdot n < 0 \;\Rightarrow\; f(n) = -f(-n)$$

then the boundedness could be limited to positive n as it can be extended to n in $\mathbb{Z}$.

In sections 2.6, 2.7, 2.8, and 2.9, we give relevant approximations to $\mathsf{approx}(r + s)$, $\mathsf{approx}(-r)$, $\mathsf{approx}(r * s)$, and $\mathsf{approx}(\frac{1}{r})$. They are based on the proposal made in this section, namely the boundedness of the difference of some functions. Such approximations form *useful hints* that we shall use in the construction of the Reals done in section 4.

2.6 Approximation of the Sum of two Reals

We have:

$$\mathsf{approx}(r+s)(n) = \lfloor (r+s)*n \rceil = \lfloor r*n + s*n \rceil$$

Applying property P3 (section 2.3) yields the following:

$$|\, \mathsf{approx}(r+s)(n) - (\mathsf{approx}(r)(n) + \mathsf{approx}(s)(n)) \,| \leq 1$$

According to what was said in section 2.5, this means that the approximation of the sum of two numbers can be approximated by the sum of their approximations since the difference between the two is *bounded*.

2.7 Approximation of the Negation of a Real

We have:

$$\mathsf{approx}(-r)(n) = \lfloor -r*n \rceil = -\lfloor r*n \rceil = -\mathsf{approx}(r)(n)$$

This means that we can generalize the consequence of property P2: we can always consider $\mathsf{approx}(r)(n)$ for positive r and positive n.

2.8 Approximation of the Product of two Reals

Given positive reals r and s and a positive integer n, we have:

$$\begin{aligned}
\mathsf{approx}(r*s)(n) &= \lfloor r*s*n \rfloor \\
&= \lfloor r*\lfloor s*n \rfloor + r*s*n - r*\lfloor s*n \rfloor \rfloor \\
&= \lfloor r*\lfloor s*n \rfloor + r*(s*n - \lfloor s*n \rfloor) \rfloor \\
&\leq 1 + \lfloor r*\lfloor s*n \rfloor \rfloor + \lfloor r*(s*n - \lfloor s*n \rfloor) \rfloor && \text{applying a property of floor } (\lfloor x+y \rfloor \leq 1 + \lfloor x \rfloor + \lfloor y \rfloor) \\
&< 1 + \lfloor r*\lfloor s*n \rfloor \rfloor + \lfloor r \rfloor && \text{applying a property of floor } (x - \lfloor x \rfloor < 1) \\
&= \mathsf{approx}(r)(\mathsf{approx}(s)(n)) + 1 + \lfloor r \rfloor
\end{aligned}$$

We also have:

$$\begin{aligned}
\mathsf{approx}(r)(\mathsf{approx}(s)(n)) &= \lfloor r*\lfloor s*n \rfloor \rfloor \\
&\leq \lfloor r*s*n \rfloor && \text{applying two properties of floor } (\lfloor x \rfloor \leq x \quad \text{and} \quad x \leq y \Rightarrow \lfloor x \rfloor \leq \lfloor y \rfloor) \\
&= \mathsf{approx}(r*s)(n)
\end{aligned}$$

From these, we deduce the following:

$$0 \leq \mathsf{approx}(r*s)(n) - \mathsf{approx}(r)(\mathsf{approx}(s)(n)) \leq \lfloor r \rfloor$$

That is:

$$|\, \mathsf{approx}(r*s)(n) - (\mathsf{approx}(r) \circ \mathsf{approx}(s))(n) \,| \leq \lfloor r \rfloor$$

In other words, $\mathsf{approx}(r*s)$ can be approximated by $\mathsf{approx}(r) \circ \mathsf{approx}(s)$ since their difference is *bounded*.

2.9 Approximation of the Inverse of a Real

For a positive real r and a positive integer n, we have:

$$\begin{aligned}
\mathsf{approx}(\tfrac{1}{r})(n) &= \lfloor \tfrac{1}{r} * n \rfloor \\
&= \max(\{\, k \mid k \in \mathbb{N} \ \wedge\ k \leq \tfrac{1}{r} * n \,\}) \\
&= \max(\{\, k \mid k \in \mathbb{N} \ \wedge\ r * k \leq n \,\}) \ =\ A \\
\max(\{\, k \mid k \in \mathbb{N} \ \wedge\ \mathsf{approx}(r)(k) \leq n \,\}) &= \max(\{\, k \mid k \in \mathbb{N} \ \wedge\ \lfloor r * k \rfloor \leq n \,\}) \\
&= \max(\{\, k \mid k \in \mathbb{N} \ \wedge\ r * k < n + 1 \,\}) \ =\ B
\end{aligned}$$

Thus:

$$r * B < n + 1 \leq r * (B + 1) \qquad r * A \leq n < r * (A + 1)$$

Thus:

$$n + r * B < r * (A + 1) + n + 1 \qquad r * A + n + 1 \leq n + r * (B + 1)$$

Thus:

$$-r - 1 < r * A - r * B \qquad r * A - r * B \leq r - 1$$

Thus:

$$-1 - \frac{1}{r} < A - B \leq 1 - \frac{1}{r}$$

That is:

$$|\, \mathsf{approx}(\frac{1}{r})(n) - \max\left(\{\, k \mid k \in \mathbb{N} \ \wedge\ \mathsf{approx}(r)(k) \leq n \,\}\right) | \leq 1 + \frac{1}{r}$$

Again, the difference between the two functions is *bounded*.

3 The Axioms of Reals

Next are the classical axioms of the reals as an algebraic structure. In the sequel we shall refer to each axiom by its number preceded by **Axiom**. This list of axioms dictates what we have to do in the next section, namely to make a formal construction of Real Numbers for these axioms, a model of Real Numbers within which these axioms are mere theorems.

1. Addition is associative: $x + (y + z) = (x + y) + z$
2. Addition is commutative: $x + y = y + x$
3. Addition has an identity: $x + 0 = x$
4. Addition has an inverse: $x + (-x) = 0$
5. Multiplication is associative: $x * (y * z) = (x * y) * z$
6. Multiplication is commutative: $x * y = y * x$
7. Multiplication has an identity: $x * 1 = x$
8. Additive and multiplicative identities are different: $0 \neq 1$
9. Distributivity of multiplication over addition: $x * (y + z) = (x * y) + (x * z)$
10. Multiplication has an inverse: $x \neq 0 \ \Rightarrow\ x * \frac{1}{x} = 1$
11. Reflexivity of order: $x \leq x$
12. Antisymmetry of order: $x \leq y \ \wedge\ y \leq x \ \Rightarrow\ x = y$
13. Transitivity of order: $x \leq y \ \wedge\ y \leq z \ \Rightarrow\ x \leq z$
14. Totality of order: $x \leq y \ \vee\ y \leq x$
15. Addition is compatible with order: $x \leq y \ \Rightarrow\ x + z \leq y + z$

16. Multiplication is compatible with order: $x \leq y \ \wedge \ 0 < z \ \Rightarrow \ x * z \leq y * z$
17. Completeness. Every non empty set of reals with an upper (lower) bound has a least upper (greatest lower) bound:

$$\begin{array}{l} \forall A \cdot A \subseteq \mathbb{R} \\ \quad A \neq \varnothing \\ \quad \exists M \cdot M \in \mathbb{R} \ \wedge \ (\forall x \cdot x \in A \Rightarrow x \leq M) \\ \Rightarrow \\ \quad \exists u \cdot u \in \mathbb{R} \ \wedge \ (\forall x \cdot x \in A \ \Rightarrow \ x \leq u) \ \wedge \ (\forall v \cdot v \in \mathbb{R} \ \wedge \ (\forall x \cdot x \in A \ \Rightarrow \ x \leq v) \ \Rightarrow \ u \leq v) \end{array}$$

4 Constructing the Reals

4.1 Intuition for Constructing the Real Numbers

The purpose of a construction of the reals is to find a set satifying the axioms of section 3. In section 2 we supposed that the set $\mathbb{R}$ of real numbers was "given" to us either by the complete ordered field axioms (section 3) or by the classical Dedekind or Cauchy constructions. Given this, we defined in section 2.2 the approx function:

$$\mathsf{approx} \in \mathbb{R} \rightarrow (\mathbb{Z} \rightarrow \mathbb{Z})$$

The idea of this construction of the reals is to go the other way around, that is:

1. To start from a certain set **R** of functions from $\mathbb{Z}$ to itself: $\mathbf{R} \ \subseteq \ \mathbb{Z} \rightarrow \mathbb{Z}$. Each function in this set will represent a real number, although different functions might represent the same real number.
2. To characterize this set.
3. To define an equivalence relation on this set (this equivalence relation will simulate equality).
4. To define the classical arithmetic operations and order relation on elements of this set.
5. To prove the classical axioms of the reals as mere theorems.

If we succeed in doing this, we can say that the set **R** is a model of the real numbers. Items 2, 3, and 4 above will be elaborated "by analogy" to what we have said of the function approx in sections 2.2 to 2.9.

4.2 Characterization of the Set R

Functions f that are elements of the set **R** have a number of basic properties Q1, Q2, and Q3. These properties are inherited from properties P1, P2, and P3 of the function approx defined in section 2.3. Given a function f in **R**, we have:

$$\mathsf{Q1}: \quad f(0) = 0$$

$$\mathsf{Q2}: \quad \forall m \cdot \mathbb{Z} \setminus \mathbb{N} \ \Rightarrow \ f(m) = -f(-m)$$

$$\mathsf{Q3}: \quad \exists k \cdot k \in \mathbb{N} \ \wedge \ (\forall m, n \cdot m \in \mathbb{N}_1 \ \wedge \ n \in \mathbb{N}_1 \ \Rightarrow \ |f(m+n) - f(m) - f(n)| \leq k)$$

Properties Q1, Q2, and Q3 are *characteristic properties* of the set **R**. As a consequence we have:

$$\boxed{\mathbf{R} \ \widehat{=} \ \{ \, f \mid f \in \mathbb{Z} \rightarrow \mathbb{Z} \ \wedge \ \mathsf{Q1} \ \wedge \ \mathsf{Q2} \ \wedge \ \mathsf{Q3} \, \}} \qquad \text{Definition 3}$$

In the referenced papers [1] to [6], all authors characterized the set **R** with property Q3[4] only. But they sometimes introduced properties Q1 and Q2 in some proofs. I found this a bit confusing as one does not

[4] Total functions from $\mathbb{Z}$ to $\mathbb{Z}$ obeying axiom Q3 are said to be *quasi-homomorphisms*.

know exactly when these properties are necessary. I prefer to suppose that Q1 and Q2 hold all the time: in fact, it does not change the final result.

As can be seen, Property Q3 is weaker than Property P3 where k was just 1. A constant such as k is called an *additivity constant* of function f. It is clearly not unique. It will be shown in section 4.13 that properties P3 will exist for some members of **R**. Note that Property Q3 can be equivalently formulated as Q3' as follows:

$$\mathsf{Q3}' : \qquad \text{finite}(\{m, n \cdot m \in \mathbb{N}_1 \wedge n \in \mathbb{N}_1 \mid f(m+n) - f(m) - f(n)\})$$

The advantage of this formulation is that it does not involve quantification and absolute value, only set finiteness.

We have also proved:

$$\mathsf{Q3}'' : \forall f \cdot f \in \mathbb{R} \Rightarrow \exists k \cdot k \in \mathbb{N} \wedge (\forall m, n \cdot m \in \mathbb{Z} \wedge n \in \mathbb{Z} \Rightarrow |f(m+n) - f(m) - f(n)| \leq k)$$

The avantage of this formulation is that we can use it when we define multiplication when we have $f(g(m+n)) - f(g(m)) - f(g(n))$ because we don't have the sign of $g(m+n)$, $g(m)$ and $g(n)$.

4.3 Defining an Equivalence Relation on the set $\mathbb{Z} \to \mathbb{Z}$

In section 2.5 we saw that the function approx could be approximated by another function provided the differences between values of these two functions are bounded. This gives us a clue to define an equivalence relation (induced by the predicate $=$) on the set $\mathbb{Z} \to \mathbb{Z}$: two functions f and g in $\mathbb{Z} \to \mathbb{Z}$ are said to be *equivalent* when the difference $f(n) - g(n)$ is bounded whatever n in $\mathbb{Z}$.

$$f = g \;\widehat{=}\; \exists k \cdot k \in \mathbb{N} \wedge (\forall n \cdot n \in \mathbb{N} \Rightarrow |f(n) - g(n)| \leq k) \qquad \text{Definition 4}$$

Notice that we reduced the variation of the quantified variable n to $\mathbb{N}$ since it can be extended to 0 or to negative values thanks to Properties Q1 and Q2. As we have done for Property Q3, we can also simplify Definition 4 in the same way:

$$f = g \;\widehat{=}\; \text{finite}(\{n \cdot n \in \mathbb{N} \mid f(n) - g(n)\}) \qquad \text{Definition 4'}$$

It is easy to prove that $=$ induces an equivalence relation[5]:

$$f = f \qquad f = g \Rightarrow g = f \qquad f = g \wedge g = h \Rightarrow f = h$$

When two functions f and g are equivalent, it means that they both represent the *same real number*. As a consequence, we identify the set of Reals with the quotient set $\mathbf{R}/=$.

4.4 Three Useful Lemmas

It is easy to prove that if a function $f1$ is a member of **R** and if a function $f2$ is equivalent to $f1$ and enjoys properties Q1 and Q2, then $f2$ also enjoys property Q3, hence it is also a member of **R**:

$$f1 \in \mathbf{R} \wedge f2 \in \{ f \mid f \in \mathbb{Z} \to \mathbb{Z} \wedge \mathsf{Q1} \wedge \mathsf{Q2} \} \wedge f1 = f2 \Rightarrow f2 \in \mathbf{R}$$

[5] The proof of the third property (transitivity of $=$) relies on the following *triangle property* of absolute values: $|a+b| \leq |a| + |b|$. Appendix 1 contains a reminder of absolute value properties.

More precisely, we have the following Lemma[6] to be used in the construction:

$$
\begin{array}{l}
f1 \in \mathbf{R} \\
f2 \in \{\, f \mid f \in \mathbb{Z} \to \mathbb{Z} \ \wedge\ \mathsf{Q1} \ \wedge\ \mathsf{Q2} \,\} \\
\exists k \cdot k \in \mathbb{N} \ \wedge\ (\forall n \cdot n \in \mathbb{N}_1 \ \Rightarrow\ |f1(n) - f2(n)| \leq k\,) \\
\Rightarrow \\
f2 \in \mathbf{R}
\end{array}
\qquad \text{Lemma 1}
$$

Notice that in the statement of Lemma 1, in the definition of $=$ used in f1$=$ f2, the quantified variable n has been reduced to $\mathbb{N}_1$ (the positive Natural Numbers): this is because it can be extended to $\mathbb{Z}$ thanks to properties Q1 and Q2 enjoyed by both $f1$ and $f2$.

We prove now another useful lemma that will be used in several parts of the construction. Given a fonction f of **R** with additivity constant k we have:

$$
\begin{array}{l}
\forall\, m, n \cdot m \in \mathbb{Z} \ \wedge\ n \in \mathbb{Z} \ \Rightarrow\ |f(m * n) - m * f(n)| \leq |m| * k \\
\\
\text{where } f \text{ is a member of } \mathbf{R} \text{ with additivity constant } k
\end{array}
\qquad \text{Lemma 2}
$$

Proof of Lemma 2. The lemma is first proved by induction on m for $m > 0$ and later extended to $m \in \mathbb{Z}$. For $m = 1$, the base step, we have the obvious:

$$|f(n) - f(n)| \leq k$$

The induction step assumes:

$$|f(m * n) - m * f(n)| \leq |m| * k$$

But we have:

$$|f(m * n + n) - f(m * n) - f(n)| \leq k$$

Thus

$$|f(m * n + n) - m * f(n) - f(n)| \leq |m| * k + k$$

that is

$$|f((m + 1) * n) - (m + 1) * f(n)| \leq (|m + 1|) * k$$

Thus we have:

$$\forall\, m, n \cdot m \in \mathbb{N}_1 \ \wedge\ n \in \mathbb{Z} \ \Rightarrow\ |f(m * n) - m * f(n)| \leq |m| * k$$

We now extend this result to $m = 0$ and then to $m < 0$. In the first case, we have the obvious:

$$|f(0) - 0| \leq 0 \qquad \text{remember: } f(0) = 0$$

When m is negative, we have:

$$
\begin{aligned}
|f(m * n) - m * f(n)| \leq |m| * k \ &\Leftrightarrow\ |-f(-m * n) + (-m) * f(n)| \leq (|-m|) * k \\
&\Leftrightarrow\ |f((-m) * n) - (-m) * f(n)| \leq |-m| * k
\end{aligned}
$$

Thus we have indeed

$$\forall\, m, n \cdot m \in \mathbb{Z} \ \wedge\ n \in \mathbb{Z} \ \Rightarrow\ |f(m * n) - m * f(n)| \leq |m| * k \qquad \blacksquare$$

[6] This lemma is boxed and named because it is used later in the paper.

Our third lemma deals with one member f of $\mathbf{R}$. We slightly modify it to a function g where we replace the value of f by β or $-\beta$ for all n where $f(n)$ is equal to α or $-\alpha$ respectively, where α is supposed to be different from 0. The lemma says that g is equivalent to f. More formally:

$$\begin{array}{l} \alpha \in \mathbb{Z} \setminus \{0\} \\ \beta \in \mathbb{Z} \\ f \in \mathbf{R} \\ g \in \mathbb{Z} \to \mathbb{Z} \\ \forall n \cdot n \in \mathbb{Z} \;\Rightarrow\; g(n) = \begin{cases} f(n) & \text{if } f(n) \neq \alpha \;\vee\; f(n) \neq -\alpha \\ \beta & \text{if } f(n) = \alpha \\ -\beta & \text{if } f(n) = -\alpha \end{cases} \\ \Rightarrow \\ g = f \end{array}$$

Lemma 3

The proof is obvious according to Definition 4'. Notice that g enjoys Properties Q1 and Q2. As a consequence, g is also a member of $\mathbf{R}$ according to Lemma 1

4.5 Embedding the set $\mathbb{Z}$ of Integers within R

By analogy with what was said about $\mathsf{approx}(r)$ in section 2.4, an integer i is represented by the function $\mathbf{f}_i$ of $\mathbf{R}$ such that:

$$\mathbf{f}_i(n) \;\widehat{=}\; i * n$$

Definition 5

Note that we have:

$$\mathbf{f}_i(0) = 0 \qquad \mathbf{f}_i(n) = -\mathbf{f}_i(-n) \qquad \mathbf{f}_i(m+n) - \mathbf{f}_i(m) - \mathbf{f}_i(n) = 0$$

Thus $\mathbf{f}_i$ is indeed a member of $\mathbf{R}$. The integer 0 is represented by $\mathbf{f}_0$, that is a function $\mathbf{0}$ of $\mathbf{R}$ where:

$$\mathbf{0}(n) \;\widehat{=}\; 0$$

Definition 6

Any bounded function f in $\mathbf{R}$ is thus also representing the integer 0 since $f(n) - \mathbf{0}(n) = f(n)$:

$$f = \mathbf{0} \;\Leftrightarrow\; \exists k \cdot k \in \mathbb{N} \;\wedge\; (\forall n \cdot n \in \mathbb{N} \;\Rightarrow\; |f(n)| \leq k)$$

Lemma 4

According to Definition 4', we also have the following:

$$f = \mathbf{0} \;\Leftrightarrow\; \text{finite}(\{n \cdot n \in \mathbb{N} \mid f(n)\})$$

Lemma 4'

The integer 1 is represented by $\mathbf{f}_1$, that is a function $\mathbf{1}$ of $\mathbf{R}$ where:

$$\mathbf{1}(n) \;\widehat{=}\; n$$

Definition 7

In section 4.12 we shall say more about this embedding of the set $\mathbb{Z}$ within $\mathbf{R}$.

4.6 Addition

Definition. By analogy with what was said about $\mathsf{approx}(r)$ in section 2.6, we define the following function:

$$\begin{array}{|l} \_\mathbf{+}\_ \in \mathbf{R} \times \mathbf{R} \to (\mathbb{Z} \to \mathbb{Z}) \\ (f \mathbf{+} g)(n) \;\widehat{=}\; f(n) + g(n) \end{array}$$

Definition 8

Addition defines an Element of R. Properties Q1, Q2, and Q3 are easy to prove for $f\mathbf{+}g$. As a consequence, we have:

$$\_\mathbf{+}\_ \in \mathbf{R} \times \mathbf{R} \to \mathbf{R}$$

Independance. The definition of addition does not depend on the choice of equivalent functions. More precisely, it is easy to prove the following:

$$f1 \mathbf{=} f2 \;\wedge\; g1 \mathbf{=} g2 \;\Rightarrow\; f1\mathbf{+}g1 \mathbf{=} f2\mathbf{+}g2$$

Proving Addition Axioms as mere Theorems. **Axiom 1** (associativity of addition), **Axiom 2** (commutativity of addition) result from similar properties of integers. **Axiom 3** (addition has an identity) is trivial:

$$(f\mathbf{+0})(n) \;=\; f(n) + \mathbf{0}(n) \;=\; f(n) + 0 \;=\; f(n) \qquad \text{that is} \qquad f\mathbf{+0} \mathbf{=} f$$

Note that if f and g have additivity constants k and l respectively, then $f\mathbf{+}g$ has additivity constant $k + l$.

4.7 Additive Inverse

Definition. By analogy with what was said about $\mathsf{approx}(r)$ in section 2.7, we define the following function:

$$\begin{array}{|l} \mathbf{-}\_ \in \mathbf{R} \to (\mathbb{Z} \to \mathbb{Z}) \\ (\mathbf{-}f)(n) \;\widehat{=}\; -f(n) \end{array}$$

Definition 9

Additive Inverse defines an Element of R. Properties Q1, Q2, and Q3 are easy to prove for $\mathbf{-}f$. As a consequence, we have:

$$\mathbf{-}\_ \in \mathbf{R} \to \mathbf{R}$$

Independance. The definition of the additive inverse does not depend on the choice of equivalent functions. More precisely, it is easy to prove the following:

$$f1 \mathbf{=} f2 \;\Rightarrow\; \mathbf{-}f1 \mathbf{=} \mathbf{-}f2$$

Proving one More Addition Axiom as a mere Theorem. Axiom 4 (addition has an inverse) is trivial:

$$(f \mathbf{+} (\mathbf{-}f))(n) \;=\; f(n) + (\mathbf{-}f)(n) \;=\; f(n) + (-f(n)) \;=\; 0 \;=\; \mathbf{0}(n) \qquad \text{that is} \qquad f \mathbf{+} (\mathbf{-}f) \;\mathbf{=}\; \mathbf{0}$$

Defining Subtraction. As is usual, we can define a binary operation **-** (subtraction):

$$\_\mathbf{-}\_ \;\in\; \mathbf{R} \times \mathbf{R} \to \mathbf{R}$$

$$(f \mathbf{-} g)(n) \;=\; (f \mathbf{+} (\mathbf{-}g))(n)$$

Note that if f and g have additivity constants k and l respectively, then $f \mathbf{-} g$ has additivity constant $k + l$. We also notice the following:

$$f \mathbf{-} g \;\mathbf{=}\; \mathbf{0} \;\Leftrightarrow\; f \;\mathbf{=}\; g$$

4.8 Multiplication

Definition. By analogy with what was said about $\mathsf{approx}(r)$ in section 2.8, we define the following function:

$$\_\mathbf{*}\_ \;\in\; \mathbf{R} \times \mathbf{R} \to (\mathbb{Z} \to \mathbb{Z})$$

$$(f \mathbf{*} g)(m) \;\widehat{=}\; (f \circ g)(m) \;=\; f(g(m))$$

Definition 10

Proof of Property Q3 for Multiplication. Properties Q1 and Q2 are easy to prove. It remains for us to prove Property Q3. We suppose that two members f and g of **R** have respective additivity constants k and l. In order to prove that property Q3 holds for $f \circ g$, we have to prove that the quantity:

$$f(g(m+n)) - f(g(m)) - f(g(n))$$

is bounded for any m and n in $\mathbb{N}_1$.

We have $\quad -f(g(m)) - f(g(n)) = -f(g(n) + g(m)) + a$

where $\quad a = f(g(n) + g(m)) - f(g(m)) - f(g(n)) \qquad$ thus $\qquad a \in -k \,..\, k$

We have $\quad g(m+n) = b + g(n) + g(m)$

where $\quad b = g(n+m) - g(n) - g(m) \qquad$ thus $\qquad b \in -l \,..\, l$

Thus $\quad f(g(m+n)) - f(g(m)) - f(g(n)) = f(b + g(n) + g(m)) - f(g(n) + g(m)) + a$

We have $\quad f(b + g(n) + g(m)) = c + f(g(n) + g(m)) + f(b)$

where $\quad c = f(b + g(n) + g(m)) - f(b) - f(g(n) + g(m)) \qquad$ thus $\qquad c \in -k \,..\, k$

Thus $\quad f(g(m+n)) - f(g(m)) - f(g(n)) = c + f(g(n) + g(m)) + f(b) - f(g(n) + g(m)) + a$

That is $\quad f(g(m+n)) - f(g(m)) - f(g(n)) = c + f(b) + a$

but we have $\quad b \in -l \,..\, l \qquad$ thus $\qquad f(b) \in \min(f[-l \,..\, l]) \,..\, \max(f[-l \,..\, l])$

Note that $\min(f[-l \,..\, l]$ and $\max(f[-l \,..\, l])$ are well defined (finite and non-empty). We have then:

$$f(g(m+n)) - f(g(m)) - f(g(n)) \in -2 * k + \min(f[-l \,..\, l]) \,..\, 2 * k + \max(f[-l \,..\, l])$$

The quantity $f(g(m+n)) - f(g(m)) - f(g(n))$ is indeed bounded. ■

As a consequence, we have:

$$\_\mathbin{\ast}\_ \;\in\; \mathbf{R} \times \mathbf{R} \to \mathbf{R}$$

Independance. The definition of multiplication does not depend on the choice of equivalent functions. More precisely, we have to prove the following:

$$f1 = f2 \;\wedge\; g1 = g2 \;\;\Rightarrow\;\; f1 \ast g1 = f2 \ast g2$$

Given $f1 = f2 \;\wedge\; g1 = g2$ we have:

$$f1 \ast g1 = f1 \ast g2 = g2 \ast f1 = g2 \ast f2 = f2 \ast g2$$

Proving Multiplication Axioms as mere Theorems. Axiom 5 (associativity of multiplication) is a consequence of the associativity of composition. **Axiom 6** (commutativity of multiplication) is proved below after **Axiom 9**. **Axiom 7** (multiplication has an identity) is trivial:

$$(f \ast \mathbf{1})(n) = f(\mathbf{1}(n)) = f(n) \qquad \text{that is} \qquad f \ast \mathbf{1} = f$$

Axiom 8 (additive and multiplicative identities are different) is also trivial. This is because $\mathbf{1}(n) - \mathbf{0}(n)$ cannot be bounded since:

$$\mathbf{1}(n) - \mathbf{0}(n) = n \qquad \text{that is} \qquad \neg\,(\mathbf{1} = \mathbf{0})$$

Axiom 9 (distributivity of multiplication over addition) is trivial:

$$(f \ast (g + h))(n) \;=\; f((g + h)(n)) \;=\; f(g(n) + h(n))$$

Property Q3 applied to f allows us to conclude:

$$f \ast (g + h) \;=\; f \ast g + f \ast h$$

Proof of Axiom 6 (commutativity of multiplication). Here is what we have to prove:

$$f \ast g \;=\; g \ast f \qquad \text{that is} \qquad \exists\, k \cdot k \in \mathbb{N} \;\wedge\; (\forall n \cdot n \in \mathbb{N}_1 \;\Rightarrow\; |f(g(n)) - g(f(n))| \leq k\,)$$

This proof is not difficult, just a bit long. It relies on some local lemmas that we prove after using them. Here is the first local lemma that is proved below:

$$\begin{array}{l} \forall\, f, g \cdot \;\; f \in \mathbf{R} \;\wedge\; g \in \mathbf{R} \\ \qquad \Rightarrow \\ \qquad \exists k \cdot k \in \mathbb{N} \;\wedge\; (\forall\, n \cdot n \in \mathbb{N}_1 \;\Rightarrow\; |n * f(g(n)) - g(n) * f(n)| \leq (|n| + 1) * k\,) \end{array}$$

From this lemma, we can assume the following for f and g in $\mathbf{R}$ and $n > 0$:

$$|n * f(g(n)) - g(n) * f(n)| \leq (n+1) * k1$$

$$|n * g(f(n)) - f(n) * g(n)| \leq (n+1) * k2$$

From this, we deduce:

$$|n * f(g(n)) - n * g(f(n))| \leq (n+1) * (k1 + k2)$$

But, as n is positive, we have:

$$|n * f(g(n)) - n * g(f(n))| \leq 2 * n * (k1 + k2)$$

yielding:

$$|f(g(n)) - g(f(n))| \leq 2 * (k1 + k2)$$

Thus:

$$\exists\, k \cdot k \in \mathbb{N} \ \wedge\ (\,\forall n \cdot n > 0 \ \Rightarrow\ |f(g(n)) - g(f(n))| \leq k\,)$$

Proof of first local lemma. Here is our our first local lemma:

$$\begin{array}{l}\forall\, f, g \cdot\ f \in \mathbf{R} \ \wedge\ g \in \mathbf{R} \\ \quad\Rightarrow \\ \quad \exists k \cdot k \in \mathbb{N} \ \wedge\ (\,\forall\, n \cdot n \in \mathbb{N}_1 \ \Rightarrow\ |n * f(g(n)) - g(n) * f(n)| \leq (|n| + 1) * k\,)\end{array}$$

It relies itself on the following second local lemma that is proved later:

$$\forall\, f \cdot f \in \mathbf{R} \ \Rightarrow\ (\exists k \cdot \forall\, m, n \cdot m \in \mathbb{Z} \ \wedge\ n \in \mathbb{Z} \ \Rightarrow\ |n * f(m) - m * f(n)| \leq (|m| + |n|) * k)$$

From this lemma, we can assume the following for f and g in $\mathbf{R}$ and n in $\mathbb{Z}$ (instantiating m with $g(n)$):

$$|n * f(g(n)) - g(n) * f(n)| \leq (|g(n)| + |n|) * k1$$

We can also assume the following (instantiating this time f with g, m with n, and n with 1)

$$|g(n) - n * g(1)| \leq (|n| + 1) * k2 \qquad \text{thus} \qquad |g(n)| \leq |n| * |g(1)| + (|n| + 1) * k2$$

yielding:

$$|n * f(g(n)) - g(n) * f(n)| \leq (|n| * |g(1)| + (|n| + 1) * k2 + |n|) * k1$$

that is:

$$|n * f(g(n)) - g(n) * f(n)| \leq (|n| * (|g(1)| + k2 + 1) + k2) * k1$$

yielding:

$$|n * f(g(n)) - g(n) * f(n)| \leq (|n| + 1) * (|g(1)| + k2 + 1) * k1$$

Thus

$$\forall\, f, g \cdot f \in \mathbf{R} \ \wedge\ g \in \mathbf{R} \ \Rightarrow\ (\exists k \cdot \forall\, n \cdot n \in \mathbb{Z} \ \Rightarrow\ |n * f(g(n)) - g(n) * f(n)| \leq (|n| + 1) * k) \quad \blacksquare$$

Proof of second local lemma. Here is our second local lemma:

$$\forall\, f \cdot f \in \mathbf{R} \ \Rightarrow\ (\exists k \cdot \forall\, m, n \cdot m \in \mathbb{Z} \ \wedge\ n \in \mathbb{Z} \ \Rightarrow\ |n * f(m) - m * f(n)| \leq (|m| + |n|) * k)$$

It relies on Lemma 2 proved in section 4.4 where f is in $\mathbf{R}$ with additivity constant k:

$$\forall\, m, n \cdot m \in \mathbb{Z} \ \wedge\ n \in \mathbb{Z} \ \Rightarrow\ |f(m * n) - m * f(n)| \leq |m| * k$$

From Lemma 2 we can deduce:

$$|f(m * n) - m * f(n)| \leq |m| * k$$

$$|f(n * m) - n * f(m)| \leq |n| * k$$

From this we deduce:

$$|n * f(m) - m * f(n)| \leq (|m| + |n|) * k \qquad \blacksquare$$

4.9 "Positive" and "Negative" Members of R

Definition. In section 4.5, we said that a function f in **R** is equivalent to **0** when it is bounded. This can be re-written formally as follows:

$$f = \mathbf{0} \Leftrightarrow \exists a, b \cdot a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge (\forall n \cdot n \in \mathbb{N} \Rightarrow f(n) \in a \mathinner{..} b)$$

$$\Leftrightarrow \exists a, b \cdot a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge (\forall n \cdot n \in \mathbb{N} \Rightarrow f(n) \geq a \wedge f(n) \leq b)$$

We have then:

$$\neg f = \mathbf{0} \Leftrightarrow \neg \exists a, b \cdot a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge (\forall n \cdot n \in \mathbb{N} \Rightarrow f(n) \geq a \wedge f(n) \leq b)$$

$$\Leftrightarrow \forall a, b \cdot a \in \mathbb{Z} \wedge b \in \mathbb{Z} \Rightarrow (\exists n \cdot n \in \mathbb{N} \wedge (f(n) < a \vee f(n) > b))$$

$$\Leftrightarrow (\forall a \cdot a \in \mathbb{Z} \Rightarrow (\exists n \cdot n \in \mathbb{N} \wedge f(n) < a)) \vee (\forall b \cdot b \in \mathbb{Z} \Rightarrow (\exists n \cdot n \in \mathbb{N} \wedge f(n) > b))$$

This suggests defining two predicates[7] **NEG**(f) and **POS**(f) as follows:

$$\mathbf{NEG}(f) \mathrel{\widehat{=}} \forall a \cdot a \in \mathbb{Z} \Rightarrow (\exists n \cdot n \in \mathbb{N} \wedge f(n) < a)$$

$$\mathbf{POS}(f) \mathrel{\widehat{=}} \forall b \cdot b \in \mathbb{Z} \Rightarrow (\exists n \cdot n \in \mathbb{N} \wedge f(n) > b)$$

Definition 11

Independance. The definitions of these predicates do not depend on the choice of equivalent functions. For instance, it is easy to prove the following:

$$\mathbf{POS}(f) \wedge f = g \Rightarrow \mathbf{POS}(g)$$

Some Properties. Of course, we would like these two predicates to be incompatible, that is:

$$\mathbf{POS}(f) \Rightarrow \neg \mathbf{NEG}(f)$$

We have then to prove the following:

$$(\forall b \cdot b \in \mathbb{Z} \Rightarrow (\exists n \cdot n \in \mathbb{N} \wedge f(n) > b)) \Rightarrow (\exists a \cdot a \in \mathbb{Z} \wedge (\forall n \cdot n \in \mathbb{N} \wedge f(n) \geq a))$$

This is an immediate consequence of the following lemma where f is a member of **R** with additivity constant k:

$$(\exists n \cdot n \in \mathbb{N} \wedge f(n) > k) \Rightarrow (\forall n \cdot n \in \mathbb{N} \Rightarrow f(n) \geq -k)$$

where f has additivity constant k

Lemma 5

[7] In Rodin we used sets **NEG** and **POS**, $\{f | f \in R \wedge f = \mathbf{0}\}$ which are a partition of R

Proof of Lemma 5. The proof of this lemma is by contradiction (here I follow [6]). We assume both:

$$\exists\, n \cdot n \in \mathbb{N} \ \wedge\ f(n) > k \qquad \text{and} \qquad \exists\, n \cdot n \in \mathbb{N} \ \wedge\ f(n) < -k$$

and we shall derive a contradiction. Let a and b be the following:

$$a \ \widehat{=}\ \min(\{\, x \mid x \in \mathbb{N} \ \wedge\ f(x) > k \,\}) \qquad b \ \widehat{=}\ \min(\{\, x \mid x \in \mathbb{N} \ \wedge\ f(x) < -k \,\})$$

The two hypotheses ensure that a and b are well-defined. Note that a and b are both positive and distinct (since $k \in \mathbb{N}$). The proof proceeds by cases. Suppose $a > b$, then $a - b < a$, hence $f(a-b) \leq k$. We also have $f(a) > k$ and $f(b) < -k$, thus:

$$f(a) - f(a-b) - f(b) > k - k + k = k$$

contradicting:

$$f(a - b + b) - f(a - b) - f(b) \leq k$$

Suppose now $b > a$, then $b - a < b$, hence $f(b-a) \geq -k$. We also have $f(a) > k$ and $f(b) < -k$, thus:

$$f(b) - f(b-a) - f(a) < -k + k - k = -k$$

contradicting:

$$f(b - a + a) - f(b - a) - f(a) \geq -k$$

Thus our second hypothesis, $\exists\, n \cdot n \in \mathbb{N}_1 \ \wedge\ f(n) < -k$, is false, yielding:

$$\forall\, n \cdot n \in \mathbb{N} \Rightarrow f(n) \geq -k$$

■

As a side product, we have the following lemma for all members f of **R** with additivity constant k:

$\mathbf{POS}(f) \ \Rightarrow\ \forall n \cdot n \in \mathbb{N} \ \Rightarrow\ f(n) \geq -k$	where f has additivity constant k
$\mathbf{NEG}(f) \ \Rightarrow\ \forall n \cdot n \in \mathbb{N} \ \Rightarrow\ f(n) \leq k$	where f has additivity constant k

Lemma 6

In conclusion, we have three incompatible predicates $f = \mathbf{0}$, $\mathbf{NEG}(f)$, and $\mathbf{POS}(f)$ with:

$$\mathbf{NEG}(f) \ \vee\ f = \mathbf{0} \ \vee\ \mathbf{POS}(f)$$

The following is easy to prove:

$$\mathbf{NEG}(f) \ \Leftrightarrow\ \mathbf{POS}(\text{-}f)$$

We define the predicates $\mathbf{NEGZ}(f)$ and $\mathbf{POSZ}(f)$ as follows:

$$\mathbf{NEGZ}(f) \ \widehat{=}\ \neg\mathbf{POS}(f) \ \Leftrightarrow\ \exists\, b \cdot b \in \mathbb{Z} \ \wedge\ (\forall\, n \cdot n \in \mathbb{N} \ \Rightarrow\ f(n) \leq b)$$

$$\mathbf{POSZ}(f) \ \widehat{=}\ \neg\mathbf{NEG}(f) \ \Leftrightarrow\ \exists\, a \cdot a \in \mathbb{Z} \ \wedge\ (\forall\, n \cdot n \in \mathbb{N} \ \Rightarrow\ f(n) \geq a)$$

We have thus

$$\mathbf{NEGZ}(f) \ \Leftrightarrow\ \mathbf{NEG}(f) \ \vee\ f = \mathbf{0} \qquad \mathbf{POSZ}(f) \ \Leftrightarrow\ \mathbf{POS}(f) \ \vee\ f = \mathbf{0}$$

We define the set **R1** of "positive" members of **R** as follows:

$$\mathbf{R1} \ \widehat{=}\ \{\, f \mid f \in \mathbf{R} \ \wedge\ \mathbf{POS}(f) \}$$

Our next lemma establishes a relationship between a "positive" member f of **R** and its additivity constant k. This lemma will be used in section 4.11.

$\mathbf{POS}(f) \ \Leftrightarrow\ \exists\, n \cdot n \in \mathbb{N} \ \wedge\ f(n) > k$	where f has additivity constant k

Lemma 7

Proof of Lemma 7. Given a member f of **R** with additivity constant k, we already have the following according to the definition of the predicate **POS**(f) at the beginning of section 4.9:

$$\mathbf{POS}(f) \;\Rightarrow\; \exists n \cdot n \in \mathbb{N} \;\wedge\; f(n) > k$$

Let us now prove the reverse implication. According to Lemma 5 of previous section we have:

$$(\exists n \cdot n \in \mathbb{N} \;\wedge\; f(n) > k) \;\Rightarrow\; (\forall n \cdot n \in \mathbb{N} \;\Rightarrow\; f(n) \geq -k)$$

thus (definition of **POSZ**(f) at the end of previous section):

$$(\exists n \cdot n \in \mathbb{N} \;\wedge\; f(n) > k) \;\Rightarrow\; \mathbf{POSZ}(f)$$

that is:

$$(\exists n \cdot n \in \mathbb{N} \;\wedge\; f(n) > k) \;\Rightarrow\; \mathbf{POS}(f) \;\vee\; f = \mathbf{0}$$

However, f is not bounded (thus f is not equivalent to **0**) according to the following:

$$\forall n \cdot n \in \mathbb{N} \;\wedge\; f(n) > k \;\Rightarrow\; (\forall m \cdot m > 0 \;\Rightarrow\; f(m * n) \geq m)$$

For proving this, we assume $f(n) > k$ (that is, $f(n) \geq k + 1$) and we use Lemma 2 of section 4.4, yielding:

$$-m * k \leq f(m * n) - m * f(n)$$

that is

$$f(m * n) \geq m * f(n) - m * k$$

But $f(n) \geq k + 1$, so we have

$$f(m * n) \geq m * (k + 1) - m * k = m$$

As a consequence, we have indeed:

$$(\exists n \cdot n \in \mathbb{N} \;\wedge\; f(n) > k) \;\Rightarrow\; \mathbf{POS}(f)$$ ■

4.10 Multiplicative Inverse for members of R1 ("Positive" Members of R)

Definition. By analogy with what was said about $\mathsf{approx}(r)$ in section 2.9, we define the following function:

$$\mathbf{inv} \;\subseteq\; \mathbf{R1} \to (\mathbb{Z} \to \mathbb{Z})$$

$$\mathbf{inv}(f)(n) \;\widehat{=}\; \begin{cases} \max(\{\, k \mid k \in \mathbb{N} \;\wedge\; (\forall x \cdot x \in 0 \,..\, k \;\Rightarrow\; f(x) \leq n) \,\}) & \text{if} \quad n > 0 \\ 0 & \text{if} \quad n = 0 \\ -\mathbf{inv}(f)(-n) & \text{if} \quad n < 0 \end{cases}$$

Definition 12

In a first attempt the definition was: $\max(\{\, k \mid k \in \mathbb{N} \;\wedge\; f(k) \leq n \,\})$ but using Rodin we need to prove that $\{\, k \mid k \in \mathbb{N} \;\wedge\; f(k) \leq n \,\}$ is bounded. It's not true.

According to the definition of **POS** in section 4.9, we have:

$$\forall n \cdot n \in \mathbb{Z} \;\Rightarrow\; \exists k \cdot k \in \mathbb{N} \;\wedge\; f(k) > n$$

Hence the set $\{\, k \mid k \in \mathbb{N} \ \wedge\ f(k) \leq n \,\}$ has an upper bound. Moreover, this set is not empty (it contains 0). As a consequence, $\mathbf{inv}(f)(n)$ is well-defined. As the definiton of $\mathbf{inv}(f)$ is not very "natural", here is an example of the inverse of the number 3:

$$\mathbf{inv}(\mathbf{f}_3)(n) = \max\left(\{\, k \mid k \in \mathbb{N} \ \wedge\ (\forall x \cdot x \in 0 \,..\, k \ \Rightarrow\ 3 * x \leq n) \,\}\right) \qquad \text{for } n \in \mathbb{N}$$

That is, for $q \in \mathbb{N}$

$$\mathbf{inv}(\mathbf{f}_3)(3 * q) = q \qquad \mathbf{inv}(\mathbf{f}_3)(3 * q + 1) = q \qquad \mathbf{inv}(\mathbf{f}_3)(3 * q + 2) = q$$

and similarly for negative values. This yields

$$|\mathbf{f}_3(\mathbf{inv}(\mathbf{f}_3)(n)) - \mathbf{1}(n)| \leq 2$$

Thus

$$(f_3)_{*}\mathbf{inv}(\mathbf{f}_3) = \mathbf{1}$$

Here are some values of $\mathbf{inv}(\mathbf{f}_3)(n)$ and $\mathbf{f}_3(\mathbf{inv}(\mathbf{f}_3)(n))$ for $n \in -9 \,..\, 9$:

$\mathbf{1}(n) = n$	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
$\mathbf{inv}(\mathbf{f}_3)(n)$	-3	-2	-2	-2	-1	-1	-1	0	0	0	0	0	1	1	1	2	2	2	3
$f_3(\mathbf{inv}(\mathbf{f}_3)(n))$	-9	-6	-6	-6	-3	-3	-3	0	0	0	0	0	3	3	3	6	6	6	9
$\lvert f_3(\mathbf{inv}(\mathbf{f}_3)(n)) - \mathbf{1}(n)\rvert$	0	2	1	0	2	1	0	2	1	0	1	2	0	1	2	0	1	2	0

Proof of Property Q3 for Multiplicative Inverse. Properties Q1 and Q2 are obvious from the definition of $\mathbf{inv}(f)$. It remains for us to prove Property Q3. Here is what we have to prove:

$$\text{finite}(\{m, n \cdot m \in \mathbb{N} \ \wedge\ n \in \mathbb{N} \mid \mathbf{inv}(f)(m + n) - \mathbf{inv}(f)(m) - \mathbf{inv}(f)(n)\}$$

This relies on the following two local lemmas that hold for a member f of **R1**:

$$\text{finite}(\{m, n \cdot m \in \mathbb{N} \ \wedge\ n \in \mathbb{N} \mid f(\mathbf{inv}(f)(m + n) - \mathbf{inv}(f)(m) - \mathbf{inv}(f)(n))\}$$

$$\forall Q \cdot Q \subseteq \mathbb{Z} \ \wedge\ \text{finite}(f[Q]) \ \Rightarrow\ \text{finite}(Q)$$

From these lemmas, we deduce

$$\text{finite}(\{m, n \cdot m \in \mathbb{N} \ \wedge\ n \in \mathbb{N} \mid \mathbf{inv}(f)(m + n) - \mathbf{inv}(f)(m) - \mathbf{inv}(f)(n)\}$$

In other words, property Q3 holds and we have indeed:

$$\mathbf{inv} \ \in\ \mathbf{R1} \to \mathbf{R}$$

■

Proof of First Local Lemma. Here is our first local lemma (in the proof, I follow [4]):

$$\text{finite}(\{m, n \cdot m \in \mathbb{N} \ \wedge \ n \in \mathbb{N} \mid f(\textbf{inv}(f)(m+n) - \textbf{inv}(f)(m) - \textbf{inv}(f)(n))\}$$

From the definition of $\textbf{inv}(f)(n)$, we deduce the following for all $m \in \mathbb{N}$ and $n \in \mathbb{N}$:

$$f(\textbf{inv}(f)(m+n)) \leq m+n \qquad f(\textbf{inv}(f)(m+n)+1) > m+n$$

$$m < f(\textbf{inv}(f)(m)+1) \qquad m \geq f(\textbf{inv}(f)(m))$$

$$n < f(\textbf{inv}(f)(n)+1) \qquad n \geq f(\textbf{inv}(f)(n))$$

That is

$$f(\textbf{inv}(f)(m+n)) < f(\textbf{inv}(f)(m)+1) + f(\textbf{inv}(f)(n)+1)$$

$$f(\textbf{inv}(f)(m+n)+1) > f(\textbf{inv}(f)(m)) + f(\textbf{inv}(f)(n))$$

According to property Q3, we have the following for all x in $\mathbb{Z}$: $f(x+1) \leq k + f(x) + f(1)$, hence we have:

$$f(\textbf{inv}(f)(m+n)) < 2*k + 2*f(1) + f(\textbf{inv}(f)(m)) + f(\textbf{inv}(f)(n))$$

$$k + f(1) + f(\textbf{inv}(f)(m+n)) > f(\textbf{inv}(f)(m)) + f(\textbf{inv}(f)(n))$$

Hence:

$$-k - f(1) < f(\textbf{inv}(f)(m+n)) - f(\textbf{inv}(f)(m)) - f(\textbf{inv}(f)(n)) < 2*k + 2*f(1)$$

With the help of property Q3, it is easy to prove the following:

$$f(\textbf{inv}(f)(m+n) - \textbf{inv}(f)(m) - \textbf{inv}(f)(n)) - 2*k \leq f(\textbf{inv}(f)(m+n)) - f(\textbf{inv}(f)(m)) - f(\textbf{inv}(f)(n))$$

$$f(\textbf{inv}(f)(m+n)) - f(\textbf{inv}(f)(m)) - f(\textbf{inv}(f)(n)) \leq f(\textbf{inv}(f)(m+n) - \textbf{inv}(f)(m) - \textbf{inv}(f)(n)) + 2*k$$

Thus we have indeed:

$$-3*k - f(1) < f(\textbf{inv}(f)(m+n) - \textbf{inv}(f)(m) - \textbf{inv}(f)(n)) < 4*k + 2*f(1)$$

That is

$$\text{finite}(\{m, n \cdot m \in \mathbb{N} \ \wedge \ n \in \mathbb{N} \mid f(\textbf{inv}(f)(m+n) - \textbf{inv}(f)(m) - \textbf{inv}(f)(n))\}$$ ■

Proof of Second Local Lemma. Here is our our second local lemma:

$$\forall Q \cdot Q \subseteq \mathbb{Z} \ \wedge \ \text{finite}(f[Q]) \ \Rightarrow \ \text{finite}(Q)$$

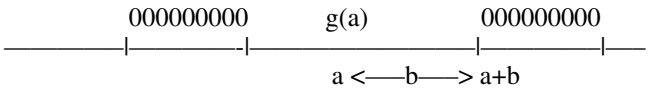
We can suppose that Q is not empty. The proof is by contradiction, hence we assume

$$\textbf{POS}(f) \qquad \text{finite}(f[Q]) \qquad \text{infinite}(Q)$$

and we shall derive a contradiction.We replace the function f by a function g identical to f except that all elements in the finite set $f[Q]$ are replaced by 0 in $g[Q]$. According to Lemma 3 of section 4.4, we have $g = f$, $g[Q] = \{0\}$ and $\textbf{POS}(g)$. We suppose that g has additivity constant equal to k. If after a certain value p we have

$$\forall n \cdot n > p \ \Rightarrow \ g(n) = 0$$

then according to Lemma 4 of section 4.5, we have g=**0** contradicting $\textbf{POS}(g)$. Thus the infinite set Q is made of an infinite number of finite sets as shown in the following figure:



In between two finite subsets of Q we have some finite sets P with points x where $g(x) \neq 0$. In such a set, let a be such that $g(a)$ is the maximum of $g[P]$. The point a is supposed to be at a distance b from the beginning of the next subset of Q. We have then:

$$|g(a+b) - g(a) - g(b)| \leq k$$

that is

$$g(a) + g(b) \leq k$$

But, according to Lemma 6 of section 4.9, we have

$$-k \leq g(b)$$

Thus

$$g(a) \leq 2 * k$$

But, according to Definition 11 of section 4.9, we can find such an a where $g(a) > 2*k$, thus contradicting $g(a) \leq 2 * k$

■

Independance. The definition of inverse does not depend on the choice of an equivalent function. More precisely, we have to prove the following:

$$f = g \;\Rightarrow\; \mathbf{inv}(f) = \mathbf{inv}(g)$$

The proof goes as follows:

$$g * \mathbf{inv}(f) = f * \mathbf{inv}(f) = g * \mathbf{inv}(g) \qquad \text{thus} \qquad \mathbf{inv}(g) * g * \mathbf{inv}(f) = \mathbf{inv}(g) * g * \mathbf{inv}(g)$$

thus

$$\mathbf{1} * \mathbf{inv}(f) = \mathbf{1} * \mathbf{inv}(g) \qquad \text{that is} \qquad \mathbf{inv}(f) = \mathbf{inv}(g)$$

Proving one More Multiplication Axiom as a mere Theorem. Axiom 10 (multiplication has an inverse) is easy to prove. This is a direct consequence of Q3 for f and the following that results from the definition of **inv**:

$$f(\mathbf{inv}(f)(n)) \leq n \qquad f(\mathbf{inv}(f)(n) + 1) > n$$

As a consequence, we have:

$$\exists k \cdot \forall n \cdot |f(\mathbf{inv}(f)(n)) - \mathbf{1}(n)| \leq k \qquad \text{that is} \qquad f * \mathbf{inv}(f) = \mathbf{1}$$

4.11 Order

Definition. We define the following predicate $\leq$:

$$f \leq g \;\widehat{=}\; \mathbf{NEGZ}(f - g) \qquad \text{Definition 13}$$

Likewise, we define the following predicates $\mathbf{\geq}$, $\mathbf{<}$, and $\mathbf{>}$ as follows:

$$\begin{array}{l} f \mathbf{\geq} g \;\widehat{=}\; \mathbf{POSZ}(f \mathbf{-} g) \\ f \mathbf{<} g \;\widehat{=}\; \mathbf{NEG}(f \mathbf{-} g) \\ f \mathbf{>} g \;\widehat{=}\; \mathbf{POS}(f \mathbf{-} g) \end{array}$$

Definition 14

We have:

$$\mathbf{NEGZ}(f) \Leftrightarrow f \mathbf{\leq 0} \qquad \mathbf{POSZ}(f) \Leftrightarrow f \mathbf{\geq 0} \qquad \mathbf{NEG}(f) \Leftrightarrow f \mathbf{< 0} \qquad \mathbf{POS}(f) \Leftrightarrow f \mathbf{> 0}$$

Proving Order Axioms as mere Theorems. Axiom 11 (reflexivity), **Axiom 13** (transitivity), and **Axiom 14** (totality) of relation $\mathbf{\leq}$ hold trivially for the predicate $\mathbf{\leq}$. As a consequence, the relation associated with the predicate $\mathbf{\leq}$ is almost a total order relation. **Axiom 12** (antisymmetry) of relation $\mathbf{\leq}$ holds only by equivalence: $x \leq y \;\wedge\; y \leq x \;\Rightarrow\; x \mathbf{=} y$. The quotient relation $\mathbf{\leq}\,/\mathbf{=}$ is indeed a total order.

Proof of Axiom 15 (addition is compatible with order) This requires to prove the following:

$$f \mathbf{\leq} g \;\Rightarrow\; f \mathbf{+} h \mathbf{\leq} g \mathbf{+} h$$

This results in proving the following trivial statement:

$$\begin{array}{l} \exists b \cdot \forall n \cdot n \in \mathbb{N} \;\Rightarrow\; f(n) - g(n) \leq b \\ \Rightarrow \\ \exists b \cdot \forall n \cdot n \in \mathbb{N} \;\Rightarrow\; (f(n) + h(n)) - (g(n) + h(n)) \leq b \end{array}$$

■

Proof of Axiom 16 (multiplication is compatible with order). This requires to prove the following:

$$f \mathbf{\leq} g \;\wedge\; h \mathbf{\geq 0} \;\Rightarrow\; f \mathbf{*} h \mathbf{\leq} g \mathbf{*} h$$

We have:

$$h \mathbf{\geq 0} \;\Leftrightarrow\; \exists a \cdot \forall n \cdot n \in \mathbb{N} \;\Rightarrow\; h(n) \geq a$$

It is easy to find a function r in $\mathbf{R}$ such that:

$$r \mathbf{=} h \;\wedge\; \forall n \cdot n \in \mathbb{N} \;\Rightarrow\; r(n) \geq 0$$

We can then replace h by r and then prove:

$$f \mathbf{\leq} g \;\wedge\; r \mathbf{\geq 0} \;\Rightarrow\; f \mathbf{*} r \mathbf{\leq} g \mathbf{*} r$$

This is trivial since we clearly have:

$$\begin{array}{l} \exists b \cdot \forall n \cdot n \in \mathbb{N} \;\Rightarrow\; f(n) - g(n) \leq b \\ \forall n \cdot n \in \mathbb{N} \;\Rightarrow\; r(n) \geq 0 \\ \Rightarrow \\ \exists b \cdot \forall n \cdot n \in \mathbb{N} \;\Rightarrow\; f(r(n)) - g(r(n)) \leq b \end{array}$$

■

Given two members f and g of $\mathbf{R}$ with additivity constants k and l respectively, then $f \text{-} g$ has additivity constant $k + l$. We can thus generalize Lemma 6 and Lemma 7 of section 4.9 as follows:

$$f \succ g \;\Rightarrow\; \forall n \cdot n \in \mathbb{N} \;\Rightarrow\; g(n) - f(n) \leq k + l$$

where f and g have additivity constants k and l respectively

Lemma 8

$$f \succ g \;\Leftrightarrow\; \exists n \cdot n \in \mathbb{N} \;\wedge\; f(n) - g(n) > k + l$$

where f and g have additivity constants k and l respectively

Lemma 9

4.12 More on the Embedding of the Set $\mathbb{Z}$ of Integers in R

In section 4.5, we defined (Definition 5) the functions $\mathbf{f}_i$ (with $\mathbf{f}_i \in \mathbf{R}$ and where i is an integer) with $\mathbf{f}_i(n) = i * n$. Such functions form a subset $\mathbf{Z}$ of $\mathbf{R}$, that is:

$$\mathbf{Z} \;\widehat{=}\; \{i \cdot i \in \mathbb{Z} \mid \mathbf{f}_i\}$$

Definition 15

It is trivial to prove that the two sets $\mathbf{Z}$[8] and $\mathbb{Z}$ are isomorphic, namely that there is a bijection b between the two. Here is this bijection:

$$b \in \mathbf{Z} \rightarrowtail\!\!\!\!\!\rightarrow \mathbb{Z}$$

$$b(\mathbf{f}_i) \;\widehat{=}\; \mathbf{f}_i(1)$$

Definition 16

Thus $b(\mathbf{f}_i) = i$ and $b^{-1}(i) = \mathbf{f}_i$. Operations (addition, additive inverse, multiplications, order) done on $\mathbf{Z}$ corresponds to similar operations in $\mathbb{Z}$. For instance, we have the following (for $i \in \mathbb{Z}$ and $j \in \mathbb{Z}$):

$$\mathbf{f}_{i+j} = \mathbf{f}_i \text{+} \mathbf{f}_j \qquad \mathbf{f}_{-i} = \text{-}\mathbf{f}_i \qquad \mathbf{f}_{i*j} = (\mathbf{f}_i) \circledast (\mathbf{f}_j) \qquad i \leq j \;\Leftrightarrow\; \mathbf{f}_i \preceq \mathbf{f}_j$$

Proof of $i \leq j \;\Leftrightarrow\; \mathbf{f}_i \preceq \mathbf{f}_j$. According to Definition 13 of section 4.11, We have:

$$\mathbf{f}_i \preceq \mathbf{f}_j \;\Leftrightarrow\; \mathbf{POSZ}(\mathbf{f}_j \text{-} \mathbf{f}_i) \;\Leftrightarrow\; \neg\, \mathbf{NEG}(\mathbf{f}_j \text{-} \mathbf{f}_i)$$

Thus, according to Definition 11 of section 4.9:

$$\mathbf{f}_i \preceq \mathbf{f}_j \;\Leftrightarrow\; \neg \forall a \cdot a \in \mathbb{Z} \;\Rightarrow\; \exists n \cdot n \in \mathbb{N} \;\wedge\; (\mathbf{f}_j \text{-} \mathbf{f}_i)(n) < a$$

$$\exists a \cdot a \in \mathbb{Z} \;\wedge\; (\forall n \cdot n \in \mathbb{N} \;\Rightarrow\; n * (j - i) \geq a)$$

As a consequence, we have (take $a = 0$):

$$i \leq j \;\Rightarrow \mathbf{f}_i \preceq \mathbf{f}_j$$

[8] Note that there are members of $\mathbf{R}$ that are not in $\mathbf{Z}$ but that are also corresponding to integers.

The other implication ($\mathbf{f}_i \mathbin{\mathbf{\leq}} \mathbf{f}_j \;\Rightarrow\; i \leq j$) goes as follows. We assume

$$\forall n \cdot n \in \mathbb{N} \;\Rightarrow\; n * (j - i) \geq a$$

and we have to prove $j - i \geq 0$. If $a \geq 0$, we are done. We assume $a < 0$. The proof is by contradiction. We assume $i - j > 0$. We have then the following, which is clearly not true for n sufficiently large:

$$\forall n \cdot n \in \mathbb{N} \;\Rightarrow\; -a \geq n * (i - j)$$ ■

Operators such as $\lfloor\_\rfloor$, $\lceil\_\rceil$, $\lfloor\_\rceil$, min, max, etc can be transferred from $\mathbb{Z}$ to **Z**. Also results obtained within $\mathbb{Z}$ can be transferred to similar results within **Z**. Among these results are all the ones presented in section 2.1 and in Appendix 1.

4.13 Reducing the Additivity Constant to 1

Given a member f of **R** with additivity constant k, we are going to exhibit an equivalent member of **R** with additivity constant 1. This property is fundamental in the next section (completeness). In section 2.2, we defined (Definition 2) a function approx as follows:

$$\mathsf{approx} \in \mathbb{R} \to (\mathbb{Z} \to \mathbb{Z})$$

Given a real r and an integer n, we had:

$$\mathsf{approx}(r)(n) \;\widehat{=}\; \lfloor r * n \rceil$$

We can now transfer the function approx into a function **approx** defined on **Z**. For this, we first define the following function **APPROX**:

$$\boxed{\begin{array}{l}\mathbf{APPROX} \in \mathbf{R} \to (\mathbf{Z} \to \mathbf{Z}) \\ \mathbf{APPROX}(f)(\mathbf{f}_n) \;\widehat{=}\; [\![f \mathbin{\ast} \mathbf{f}_n]\!]\end{array}}$$ Definition 17

where $[\![\_]\!]$ denotes the transfer to **Z** of the function $\lfloor\_\rceil$ defined for $\mathbb{Z}$ (Definition 1 of section 2.1). Then we define the function **approx** as follows:

$$\boxed{\begin{array}{l}\mathbf{approx} \in \mathbf{R} \to (\mathbb{Z} \to \mathbb{Z}) \\ \mathbf{approx}(f)(n) \;\widehat{=}\; b(\mathbf{APPROX}(f)(\mathbf{f}_n))\end{array}}$$ Definition 18

where b denotes the bijection between **Z** and $\mathbb{Z}$ (Definition 16 of section 4.12).

Proof that approx(f) has additivity constant 1. In section 2.3 we proved that the function approx had an additivity constant equal to 1. Therefore it can be proved that **APPROX** has an "additivity constant" of **1**, that is:

$$\mathbf{-1 \mathbin{\leq} APPROX}(f)(\mathbf{f}_m \mathbf{+} \mathbf{f}_n) \mathbf{-} \mathbf{APPROX}(f)(\mathbf{f}_m) \mathbf{-} \mathbf{APPROX}(f)(\mathbf{f}_n) \mathbin{\mathbf{\leq}} \mathbf{1}$$

As a consequence, and according to what has been done in section 4.12, we have

$$-1 \leq \mathbf{approx}(f)(m + n) \;-\; \mathbf{approx}(f)(m) \;-\; \mathbf{approx}(f)(n) \leq 1$$ ■

It remains now for us to prove that **approx**(f) is equivalent to f. If we succeed in doing so, then it means that with each function f (with additivity constant k) we can associate an equivalent function **approx**(f) with additivity constant 1.

Proof of the Equivalence of approx(f) and f. We first prove that we can find an integer constant l such that:

$$\mathbf{-f}_l \leq \mathbf{APPROX}(f)(\mathbf{f}_n) \mathbf{-} \mathbf{f}_{f(n)} \leq \mathbf{f}_l$$

that is (according to the definition of $\leq$ in section 4.11):

$$(\mathbf{-f}_l)(m) \mathbf{-} (\lfloor f_* \mathbf{f}_n \rceil \mathbf{-} \mathbf{f}_{f(n)})(m) \leq b \qquad (\lfloor f_* \mathbf{f}_n \rceil \mathbf{-} \mathbf{f}_{f(n)})(m) \mathbf{-} \mathbf{f}_l(m) \leq c$$

where b and c are two integer constants to be discovered. But we have:

$$\mathbf{-} \lfloor f_* \mathbf{f}_n \rceil \leq \mathbf{1} \mathbf{-} f_* \mathbf{f}_n \qquad \lfloor f_* \mathbf{f}_n \rceil \leq f_* \mathbf{f}_n \mathbf{+1}$$

then it is sufficient to prove the following (since $\mathbf{f}_{f(n)}$ and $\mathbf{f}_l$ are members of $\mathbf{Z}$):

$$-m * l + m - (f_* \mathbf{f}_n)(m) - m * f(n) \leq b \qquad (f_* \mathbf{f}_n)(m) + m - m * f(n) - m * l \leq c$$

Now (5) is equivalent to the following (according to the definition of $*$ in section 4.8):

$$-m * l + m - f(\mathbf{f}_n(m)) + m * f(n) \leq b \qquad f(\mathbf{f}_n(m)) + m - m * f(n) - m * l \leq c$$

that is

$$-m * l + m - f(m * n) + m * f(n) \leq b \qquad f(m * n) + m - m * f(n) - m * l \leq c$$

But, according to Lemma 2 of section 4.4, we have:

$$-m * k \leq f(m * n) - m * f(n) \leq m * k$$

As a consequence, we can choose l to be $k + 1$ and b and c to be 0 and we have:

$$\mathbf{-f}_{k+1} \leq \mathbf{APPROX}(f)(\mathbf{f}_n) \mathbf{-} \mathbf{f}_{f(n)} \leq \mathbf{f}_{k+1}$$

Thus according to what has been done in section 4.12, we have:

$$-(k+1) \leq \mathbf{approx}(f)(n) - f(n) \leq k + 1$$ ■

We can now specialize Lemma 8 and Lemma 9 of section 4.11 when f and g are both members of $\mathbf{R}$ with additivity constant 1, yielding the following Lemma 10 and Lemma 11:

$f > g \Rightarrow \forall n \cdot n \in \mathbb{N} \Rightarrow g(n) - f(n) \leq 2$
where f and g have additivity constant 1

Lemma 10

$f > g \Leftrightarrow \exists n \cdot f(n) - g(n) > 2$ where f and g have additivity constant 1

Lemma 11

These lemmas will be used in the next section where we present completeness.

4.14 Supremum

Definition. We are given a non-empty set S of mutually non-equivalent members of $\mathbf{R}$. That is, either $f \lessdot g$ or $g \lessdot f$ for any two distinct members f and g of S. We suppose that the set S is made of members of $\mathbf{R}$ *all with additivity constants* 1. Moreover, we suppose that this set is bounded above by a member M of $\mathbf{R}$:

$$\forall\, f \cdot f \in S \;\Rightarrow\; M \gtrdot f$$

$f \lessdot g$ or $g \lessdot f$ is too restrictive to conclude. We have added the case $g = f$ where we can prove $\forall x, \cdot\, x > 0 \;\Rightarrow\; |g(x) - f(x)| \leq 2$

Proof: we have $f \text{-} g = \mathbf{0}$ because $f = g$

by contradiction $\exists x \cdot x > 0 \;\wedge\; |g(x) - f(x)| > 2$ then we can proved $\mathbf{POS}(f \text{-} g)$ or $\mathbf{NEG}(f \text{-} g)$ but it's $\mathbf{0}$

We have thus the following according to Lemma 10 of section 4.13:

$$\forall\, f \cdot f \in S \;\Rightarrow\; (\forall\, n \cdot n \in \mathbb{N} \;\Rightarrow\; f(n) \leq M(n) + 2) \tag{1}$$

We then define the Supremum as a function $\mathbf{sup}$ as follows:

$$\mathbf{sup} \in \mathbb{P}(\mathbf{R}) \setminus \{\varnothing\} \to (\mathbb{Z} \to \mathbb{Z})$$

$$\mathbf{sup}(S)(n) \;\widehat{=}\; \begin{cases} \max(\{f \cdot f \in S \mid f(n)\}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -\mathbf{sup}(S)(-n) & \text{if } n < 0 \end{cases}$$

Definition 19

Note that the non-emptiness of S and the above condition (1) guarantee the well-definedness of $\mathbf{sup}(S)(n)$.

Proof of Property Q3 for Supremum. As Properties Q1 and Q2 are obvious from the definition, we have just to prove property Q3. Here I follow the approach of [6]. First, we notice that each value $\mathbf{sup}(S)(n)$ comes from a certain member f_n of S, formally:

$$\forall\, n \cdot n > 0 \;\Rightarrow\; (\exists\, f_n \cdot f_n \in S \;\wedge\; \mathbf{sup}(S)(n) = f_n(n) \;\wedge\; (\forall\, f \cdot f \in S \;\Rightarrow\; f(n) \leq f_n(n)))$$

We prove now the following:

$$\exists\, a, b \cdot \forall\, m, n \cdot \mathbf{sup}(S)(m+n) - \mathbf{sup}(S)(m) - \mathbf{sup}(S)(n) \in a \mathinner{..} b$$

Since $f_{m+n}(m) \leq f_m(m)$ and $f_{m+n}(n) \leq f_n(n)$, we have:

$$\begin{aligned} \mathbf{sup}(S)(m+n) - \mathbf{sup}(S)(m) - \mathbf{sup}(S)(n) &= f_{m+n}(m+n) - f_m(m) - f_n(n) \\ &\leq f_{m+n}(m+n) - f_{m+n}(m) - f_{m+n}(n) \\ &\leq 1 \end{aligned}$$

The proof now proceeds by cases. First suppose $f_m \gtrdot f_n$, thus $\forall\, x \cdot f_m(x) - f_n(x) \geq -2$ according to Lemma 10 of section 4.13, hence:

$$\begin{aligned} \mathbf{sup}(S)(m+n) - \mathbf{sup}(S)(m) - \mathbf{sup}(S)(n) &= f_{m+n}(m+n) - f_m(m) - f_n(n) \\ &\geq (f_m(m+n) - f_m(m) - f_m(n)) + (f_m(n) - f_n(n)) \\ &\geq -1 - 2 \\ &= -3 \end{aligned}$$

The other case, $f_n \succ f_m$, yields the same result. Thus Q3 holds and $\mathbf{sup}(S)$ is a member of $\mathbf{R}$ since we have:

$$\mathbf{sup}(S)(m+n) - \mathbf{sup}(S)(m) - \mathbf{sup}(S)(n) \in -3\,..\,1$$

The last case, $f_n = f_m$, yields the same result. Thus Q3 holds and $\mathbf{sup}(S)$ is a member of $\mathbf{R}$ since we have:

$$\mathbf{sup}(S)(m+n) - \mathbf{sup}(S)(m) - \mathbf{sup}(S)(n) \in -3\,..\,1$$ ■

As proved $\mathbf{sup}(S)$ doesn't have an additivity constant 1 (it's 3) but $\mathbf{APPROX}(\mathbf{sup}(S))$ yes.

Proof of the Completeness Axiom. Finally, we prove **Axiom 17** (completeness). Here I follow the approach of [3]. We first prove that $\mathbf{sup}(S)$ is an *upper bound* of S. For any f in S, we have:

$$\forall\, n \cdot n \in \mathbb{N} \;\Rightarrow\; f(n) \leq \mathbf{sup}(S)(n)$$

that is

$$\forall\, n \cdot n \in \mathbb{N} \;\Rightarrow\; f(n) - \mathbf{sup}(S)(n) \leq 0$$

that is

$$\exists\, b \cdot \forall\, n \cdot n \in \mathbb{N} \;\Rightarrow\; f(n) - \mathbf{sup}(S)(n) \leq b$$

that is, according to the definition of $\preceq$ in section 4.11:

$$\forall\, f \cdot f \in S \;\Rightarrow\; f \preceq \mathbf{sup}(S)$$

Thus $\mathbf{sup}(S)$ is indeed an upper bound of S. It remains now for us to prove that $\mathbf{sup}(S)$ is a *least* upper bound. The proof is by contradiction. Suppose we have another upper bound t of S such that $\mathbf{sup}(S) \succ t$. Then, according to Lemma 11 of section 4.13, that is:

$$f \succ g \;\Leftrightarrow\; \exists\, n \cdot f(n) - g(n) > 2$$

there exists a positive natural number n such that $\mathbf{sup}(S)(n) - t(n) > 2$. Let $\mathbf{sup}(S)(n) = f_n(n)$, we have then $f_n(n) - t(n) > 2$, thus $f_n \succ t$, again according to Lemma 11 of section 4.13. But since f_n is a member of S, we have thus $f_n \preceq t$ (as t is an upper bound of S). This contradicts $f_n \succ t$. Thus $\mathbf{sup}(S)$ is indeed a least upper bound of S:

$$\forall\, t \cdot t \in \mathbf{R} \;\wedge\; (\forall\, f \cdot f \in S \;\Rightarrow\; f \preceq t) \;\Rightarrow\; \mathbf{sup}(S) \preceq t$$ ■

5 Conclusion

In this paper, I presented a systematic construction of the Real Numbers as introduced by various authors some years ago. I said in the introduction that this construction did not require complicated mathematical concepts. This is true. But also true is the fact that this construction is not so simple. Some developments required some attention: commutativity of multiplication (section 4.8), construction of the multiplicative inverse (section 4.10), proof of the supremum (section 4.14).

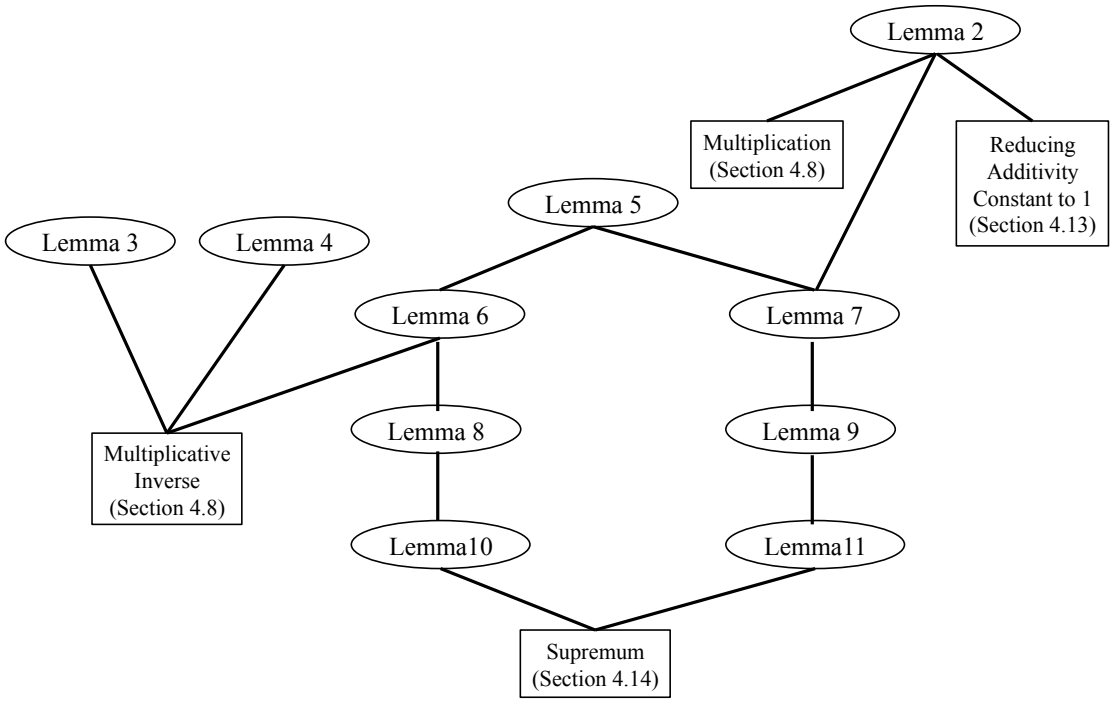
The reduction of additivity constant to 1 done in section 4.13 is completely different from that proposed in [3]. I was very impressed by this proposal but could not understand really where it comes from. My proposal is to "transfer" the function approx into $\mathbf{R}$. It seems more natural (to me). I also simplified the proof for the operator **inv** (see the proof of the second local lemma in section 4.10).

I payed lots of attention to carefully structure the construction so that the reader could follow the development without (I hope) the trouble I had when reading the referenced papers. I insisted a lot on the preliminary investigations giving some clues to the proposed constructions. It resulted in systematic

definitions of the operators that are sometimes slightly different from those of the referenced papers (for **inv** in particular).

The construction necessitates to prove somme lemmas used in different situations. In this case it is always very important to ensure that these lemmas do not introduce some circularities. Next is a diagram showing the relationship between these lemmas and the places where they are used.

Real numbers are the set of equivalence classes of the set $\mathbf{APPROX}[\mathbf{R}]$. Real numbers are $\mathbf{APPROX}[\mathbf{R}]/\ \mathbf{=}$



Acknowledgments: I would like to thank very much Wen Su. She did some very careful readings of various drafts of this paper and gave me very useful advices. I would like also to thank Rob Arthan for interesting comments on an earlier draft of this paper.

References

1. Ross Street. An efficient construction of the real numbers. *Gazette Australian Math. Soc.* 12:57-58 (1985)
2. Ben Odgers and Nguyen Vo. Analysis of an efficient construction of the reals. *Vacation Scholar Project* (2002). See http:www.math,mq.edu/s̃treet/efficient.pdf
3. Norbert A'Campo. A natural construction for the real numbers. *arXiv:math. GN/0301015 v1* (2003)
4. Rob Arthan. The Eudoxus Real Numbers. *arXiv:math/04054454 v1* (2003)
5. Ross Street. Update on the efficient reals *Macquarie University* (2003)
6. James Douglas, et al. The Efficient Real Numbers *Macquarie University* (2004)
7. http://www.event-b.org/platform.html

Appendix 1: Some Useful Properties of Absolute Values of Integers

Next are presented some properties of the absolute value of integers. These properties have been used in the paper without being mentioned explicitly. The absolute value is a total function from integers to

natural numbers:

$$|\_| \in \mathbb{Z} \to \mathbb{N}$$

In the properties to follow, m and n are supposed to be integers and k a natural number:

$$|n| = \max(\{ -n, n \}) \qquad n \geq 0 \;\Rightarrow\; |n| = n \qquad n \leq 0 \;\Rightarrow\; |n| = -n$$

$$|m + n| \leq |m| + |n| \qquad |-n| = |n| \qquad |m| - |n| \leq |m - n| \qquad |m * n| = |m| * |n|$$

$$|n| \leq k \;\Leftrightarrow\; n \in -k \mathinner{..} k \qquad (\exists\, k \cdot k \in \mathbb{N} \;\wedge\; |n| \leq k) \;\Leftrightarrow\; (\exists\, a, b \cdot a \in \mathbb{Z} \;\wedge\; b \in \mathbb{Z} \;\wedge\; n \in a \mathinner{..} b)$$