Constructing the Real Numbers using RODIN and EBRP's plugin

Jean-Raymond Abrial Dominique cansell

March 2023

The story

1. In 2012 JRA sent me the paper
2. During my next visit we didn't discuss about reals. I thought he did used Rodin
3. In 2021 he resent the paper and asked me to use Rodin and the plugin to manage the development
4. Job done during summer 2021 some errors are detected and corrected
5. I started JRA's development definitions, axioms and theorems step by step
6. For this talk I read carefully JRA's motivation

Reminder: Naturals, Integers and Rationals

Algebraic properties of the naturals, integers rationals

Axioms	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$
Addition is associative	$\surd$	$\surd$	$\surd$
Addition is commutative	$\surd$	$\surd$	$\surd$
Addition has an identity	$\surd$	$\surd$	$\surd$
Addition has an inverse		$\surd$	$\surd$
Multiplication is associative	$\surd$	$\surd$	$\surd$
Multiplication is commutative	$\surd$	$\surd$	$\surd$
Multiplication has an identity	$\surd$	$\surd$	$\surd$
Identities are different	$\surd$	$\surd$	$\surd$
Distributivity of multiplication	$\surd$	$\surd$	$\surd$
Multiplication has an inverse			$\surd$
Reflexivity of order	$\surd$	$\surd$	$\surd$
Antisymmetry of order	$\surd$	$\surd$	$\surd$
Transitivity of order	$\surd$	$\surd$	$\surd$
Totality of order	$\surd$	$\surd$	$\surd$
Addition and order	$\surd$	$\surd$	$\surd$
Multiplication and order	$\surd$	$\surd$	$\surd$

- Known from many centuries (Hippasus of Metapontum):

$$\sqrt{2} \text{ is not a rational}$$

- For this, Pythagoras sentenced Hippasus to death by drowning

- Some new numbers are needed: the Reals

- How to construct them ?

- What additional algebraic properties do they have?

Algebraic Axioms of the Reals

Axioms	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$
Addition is associative	$\surd$	$\surd$	$\surd$	$\surd$
Addition is commutative	$\surd$	$\surd$	$\surd$	$\surd$
Addition has an identity	$\surd$	$\surd$	$\surd$	$\surd$
Addition has an inverse		$\surd$	$\surd$	$\surd$
Multiplication is associative	$\surd$	$\surd$	$\surd$	$\surd$
Multiplication is commutative	$\surd$	$\surd$	$\surd$	$\surd$
Multiplication has an identity	$\surd$	$\surd$	$\surd$	$\surd$
Identities are different	$\surd$	$\surd$	$\surd$	$\surd$
Distributivity of multiplication	$\surd$	$\surd$	$\surd$	$\surd$
Multiplication has an inverse			$\surd$	$\surd$
Reflexivity of order	$\surd$	$\surd$	$\surd$	$\surd$
Antisymmetry of order	$\surd$	$\surd$	$\surd$	$\surd$
Transitivity of order	$\surd$	$\surd$	$\surd$	$\surd$
Totality of order	$\surd$	$\surd$	$\surd$	$\surd$
Addition and order	$\surd$	$\surd$	$\surd$	$\surd$
Multiplication and order	$\surd$	$\surd$	$\surd$	$\surd$
Completeness (more later)				$\surd$

Question

- Who remembers the Cauchy construction of the Real Numbers?

- Why I was interested?

- Browsing on Wikipedia

- Heavy frustrations in reading the referenced papers

Stephen Schanuel. Proposal without publication (early 80th)

Ross Street. An efficient construction of the real numbers. *Gazette Australian Math. Soc.* 12:57-58 (1985)

Ben Odgers and Nguyen Vo. Analysis of an efficient construction of the reals. *Vacation Scholar Project* (2002).
http:www.math,mq.edu/s̃treet/efficient.pdf

Norbert A'Campo. A natural construction for the real numbers. *arXiv:math.GN/0301015 v1* (2003)

Rob Arthan. The Eudoxus Real Numbers. *arXiv:math/04054454 v1* (2003)

Ross Street. Update on the efficient reals *Macquarie University* (2003)

James Douglas, et al. The Efficient Real Numbers *Macquarie University* (2004)

More on Frustrations (1)

- Proposed constructs are taken out of a hat

- You "see" them working but you do not "understand" why

- Lemmas follow each other without any explanations

- Many steps missing in proofs (when present)

- Backward references in papers are simply missing or erroneous

More on Frustrations (2)

- Some heavy misprints

- You try to understand until you figure out this is just a misprint

- Example of statements:

  there exists x such that a predicate on x and y hold, for all y

- It is not clear whether it means "$\exists x \cdot \forall y \ldots$" or "$\forall y \cdot \exists x \ldots$"

- Found in the paper by Ben Odgers and Nguyen Vo:

> *Notice that a real number α determines a function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = ip(\alpha n)$, where "ip" means "integer part". Then $f(n)/n \to \alpha$ as $n \to \infty$. From this motivation we attempt to construct the real number system directly from the set of integers.*

- This is the only motivation found in the referenced articles

Floor ($\lfloor x \rfloor$), Ceiling ($\lceil x \rceil$), and Integer Part ($\lfloor x \rceil$)

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

$$\lceil x \rceil \;\widehat{=}\; \min\left(\{n \mid n \in \mathbb{Z} \;\wedge\; n \ge x\}\right)$$

$$\lfloor x \rceil \;\widehat{=}\; \begin{cases} \lfloor x \rfloor & \text{if } x \ge 0 \\ \lceil x \rceil & \text{if } x \le 0 \end{cases}$$

Examples:

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

$$\lfloor 0.2 \rfloor = 0 \quad \lceil 0.2 \rceil = 1 \quad \lfloor -0.2 \rfloor = -1 \quad \lceil -0.2 \rceil = \;\; 0 \quad \lfloor 0.2 \rceil = 0 \quad \lfloor -0.2 \rceil = \;\; 0$$

Some properties of the integer part function:

$$-1 < x - \lfloor x \rceil < 1 \qquad -1 \le \lfloor x + y \rceil - \lfloor x \rceil - \lfloor y \rceil \le 1$$

$$x < 0 \Rightarrow \lfloor x \rceil \le 0 \qquad x > 0 \Rightarrow \lfloor x \rceil \ge 0$$

The approx Function (the Function f of the Quotation)

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

$$\textbf{approx}(r)(n) \;\widehat{=}\; \lfloor n * r \rfloor$$

Example:

$$\begin{aligned}\textbf{approx}(\sqrt{2})(n) &= \lfloor n * \sqrt{2} \rfloor \qquad \text{(for } n > 0\text{)} \\ &= \max(\{\, k \mid k \in \mathbb{Z} \;\wedge\; k \leq n * \sqrt{2} \,\}) \\ &= \max(\{\, k \mid k \in \mathbb{N} \;\wedge\; k^2 \leq 2 * n^2 \,\})\end{aligned}$$

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

Properties of the Function approx

P1 : $\forall r \cdot r \in \mathbb{R} \Rightarrow \mathbf{approx}(r)(0) = 0$

P2 : $\forall r, n \cdot r \in \mathbb{R} \land n < 0 \Rightarrow \mathbf{approx}(r)(n) = -\mathbf{approx}(r)(-n)$

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

P4 : $\forall r, n \cdot \; r \in \mathbb{R} \land r > 0 \land n \in \mathbb{N} \Rightarrow \mathbf{approx}(r)(n) \leq \mathbf{approx}(r)(n+1)$

P5 : $\lim_{n \to \infty} \frac{\mathbf{approx}(r)(n)}{n} = r$

Approximation of the function approx by a Function f

The difference between the two is bounded

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

Equivalent conditions:

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

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

Values of approx for Integers and Rationals

For an integer i, we have:

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

Given a rational $\frac{p}{q}$ where p and q are integers (with $q \neq 0$), we have:

$$\textbf{approx}(\tfrac{p}{q})(n) = \begin{cases} \max(\{k \mid k \in \mathbb{N} \ \wedge \ k * q \leq p * n\}) & \text{if} \quad p * q * n \geq 0 \\ \min(\{k \mid k \in \mathbb{Z} \ \wedge \ k * q \geq p * n\}) & \text{if} \quad p * q * n \leq 0 \end{cases}$$

Approximation of the Arithmetic Operations

$\textbf{approx}(r + s)(n)$	$\textbf{approx}(r)(n) + \textbf{approx}(s)(n)$
$\textbf{approx}(-r)(n)$	$-\textbf{approx}(r)(n)$
$\textbf{approx}(r * s)(n)$	$\textbf{approx}(r)(\textbf{approx}(s)(n))$
$\textbf{approx}(\frac{1}{r})(n)$	$\max(\{\, k \mid k \in \mathbb{N} \ \wedge\ \textbf{approx}(r)(k) \leq n\})$

Example: Approximation of the Product of two Reals

Supposing $r * s * n > 0$, we have:

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

We also have:

$$\textbf{approx}(r)(\textbf{approx}(s)(n)) \leq \textbf{approx}(r * s)(n) \qquad \text{applying two properties of floor } (\lfloor x \rfloor \leq x \quad \text{and} \quad x \leq y \Rightarrow \lfloor x \rfloor \leq \lfloor y \rfloor)$$

From these, we deduce the following:

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

That is:

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

Axiom of the Reals (1)

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: $x * (y + z) = (x * y) + (x * z)$

Axioms of the Reals (2)

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

This axiom characterizes the Reals

Every non empty set of reals A with an upper bound m has a LUB u

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

What we Have Done so Far

- We supposed that the set of Reals $\mathbb{R}$ was given to us

- We defined the function **approx**

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

- The image of $\mathbb{R}$ under the function **approx** is a included in $\mathbb{Z} \to \mathbb{Z}$:

$$\textbf{approx}[\mathbb{R}] \;\subseteq\; \mathbb{Z} \to \mathbb{Z}$$

-The idea for constructing the reals is to go the other way around

Approach for Constructing the Reals

- To start from a certain set **R** of functions from $\mathbb{Z}$ to itself:

$$\mathbf{R} \subseteq \mathbb{Z} \to \mathbb{Z}$$

- To characterize this set

- To define an equivalence relation on this set

- To define the arithmetic operations and the order relation

- To prove the 17 axioms of the reals as mere theorems

- What has been done on **approx** will help us as useful hints

Q1 : $f(0) = 0$

Q2 : $\forall n \cdot n < 0 \;\Rightarrow\; f(n) = -f(-n)$

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

- k is said to be an additivity constant for f

$$\mathbf{R} \;\widehat{=}\; \{\, f \mid f \in \mathbb{Z} \to \mathbb{Z} \;\land\; \mathbf{Q1} \;\land\; \mathbf{Q2} \;\land\; \mathbf{Q3} \,\}$$

- We use the following properties of **approx** as hints

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

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

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

Equivalence Relation on the Set R

- Again, we use what has been done on approximating **approx** as a hint

- The difference between f and g in **R** is bounded

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

- It induces an equivalence relation

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

- The Reals will thus be modelled as the quotient set $\mathrm{R}/\equiv$

Embedding $\mathbb{Z}$ in R

According to what we said about **approx**(r), an integer i is represented by the following function f_i:

$$f_i(n) = i * n$$

The integer 0 is represented by a function **0** of **R** with:

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

Any bounded function f is "equal" to **0** since $f(n) - \mathbf{0}(n) = f(n)$:

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

The integer 1 is represented by a function **1** of **R** with:

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

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

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

We have then:

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

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

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

This suggests the following:

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

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

We can prove

$$\textbf{POS}(f) \;\Rightarrow\; \neg\, \textbf{NEG}(f)$$

POS(f),**NEG**(f), and $f \;\mathbf{=}\; \mathbf{0}$ are incompatible

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

This suggests the following using Rodin: **POS** , **NEG** are sets.

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

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

We can prove

$$\begin{array}{l} \textbf{POS} \cap \textbf{NEG} = \\ \textbf{POS} \cap \{f \mid f = \mathbf{0}\} = \varnothing \\ \textbf{NEG} \cap \{f \mid f = \mathbf{0}\} = \varnothing \end{array}$$

This suggests the following using Rodin: **POS** , **NEG** are sets.

$$\textbf{NEG} \ \widehat{=} \ \{\, f | f \in \mathrm{R} \wedge \forall a \cdot a \in \mathbb{Z} \Rightarrow (\exists n \cdot n \in \mathbb{N} \wedge f(n) < a)\}$$

$$\textbf{POS} \ \widehat{=} \ \{\, f | f \in \mathrm{R} \wedge \forall b \cdot b \in \mathbb{Z} \Rightarrow (\exists n \cdot n \in \mathbb{N} \wedge f(n) > b)\}$$

$$\textbf{ZERO} \ \widehat{=} \ \{f \mid f \in R \wedge f = \mathbf{0}\}$$

We can prove

$$\textbf{POS} \cup \textbf{NEG} \cup \textbf{ZERO} = R$$

It’s a partition

Definitions of Arithmetic Operations in R

- As suggested from **approx**, we propose:

$(f\mathbf{+}g)(n)$	$f(n)+g(n)$
$(\mathbf{-}f)(n)$	$-f(n)$
$(f{\star}g)(n)$	$f(g(n))$
inv$(f)(n)$ (where $f \in$ **POS**)	$\max(\{\, k \mid k \in \mathbb{N} \ \wedge \ f(k) \le n \,\})$

- One has to prove that the RHS are in **R**

- One has to prove the axioms as mere theorems

To prove that $f{\star}g \ \in \mathrm{R}$ we need to prove that a k such

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

exists but we cannot use $Q3$

because we don't have the sign of $g(m+n)$, $g(m)$ and $g(n)$.

Using $Q3$ we can prove:

$$\exists k \cdot \forall m, n \cdot \begin{array}{l} m \in \mathbb{Z} \ \wedge \ n \in \mathbb{Z} \\ \Rightarrow \\ |f(m+n) - f(m) - f(n)| \leq k \end{array}$$

- As suggested from **approx**, we propose:

$(f\,\textbf{+}\,g)(n)$	$f(n) + g(n)$
$(\textbf{-}f)(n)$	$-f(n)$
$(f \star g)(n)$	$f(g(n))$
inv$(f)(n)$ (where $f \in$ **POS**)	$\max(\{\, k \mid k \in \mathbb{N} \;\wedge\; f(k) \leq n \,\})$

- One has to prove that the RHS are in **R**

- One has to prove the axioms as mere theorems

- As suggested from **approx**, we propose:

$(f\mathbf{+}g)(n)$	$f(n) + g(n)$
$(\mathbf{-}f)(n)$	$-f(n)$
$(f{\star}g)(n)$	$f(g(n))$
inv$(f)(n)$ (where $f \in$ **POS**)	$\max($ $\{k \mid k \in \mathbb{N} \wedge (\forall x \cdot x \in 0..k \Rightarrow f(x) \leq n)$

- $\{k \mid k \in \mathbb{N} \ \wedge \ f(k) \leq n\}$ is not bounded!

- $\{k \mid k \in \mathbb{N} \ \wedge \ (\forall x \cdot x \in 0..k \ \Rightarrow \ f(x) \leq n)\}$ is bounded

- Equivalence conservation

If f = f' and g = g' then

f+g = f'+g'

f*g = f'*g'

-g = -g'

inv(f) = **inv**(f')

+ : commutative, associative, **0** neutral.

$\star$: associative

$\star$: commutative by equivalence $f \star g$ **=** $g \star f$

$\star$: distributivity over **+** by equivalence $f \star (g \mathbf{+} h)$ **=** $(f \star g) \mathbf{+} (f \star h)$

$\star$: **1** neutral by equivalence $f \star \mathbf{inv}(f)$ **= 1**

$$f \leq g \;\hat{=}\; f\mathbf{+}(\mathbf{-}g) \in \textbf{NEGZ} \;\hat{=}\; g\mathbf{+}(\mathbf{-}f) \in \textbf{POSZ}$$

$$\textbf{NEGZ} \;\hat{=}\; \textbf{NEG} \cup \textbf{ZERO} \quad \textbf{POSZ} \;\hat{=}\; \textbf{POS} \cup \textbf{ZERO}$$

Axiom 11 (reflexivity), :$f\mathbf{+}(\mathbf{-}f) \in$ **ZERO**

Axiom 12 (antisymmetry) only by equivalence

$f \leq g \wedge g \leq f \Rightarrow f = g$

Axiom 13 (transitivity), and **Axiom 14** (totality) of relation induced by $\leq$ hold trivially.

About the Proofs: Some Useful Lemmas

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

where f has additivity constant k

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

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

- The additivity constant can always be reduced to 1 (see later)

$$g \mathbin{\textbf{<}} f \Rightarrow \forall n \cdot n \in \mathbb{N} \Rightarrow g(n) - f(n) \leq 2$$

where f and g have additivity constant 1

$$g \mathbin{\textbf{<}} f \Leftrightarrow \exists n \cdot f(n) - g(n) > 2$$

where f and g have additivity constant 1

Given a non-empty subset S of **R** (with only additivity constant 1) and a member M of **R** (additivity constant 1) such that:

$$\forall f \cdot f \in S \;\Rightarrow\; f \mathbf{<} M$$

We have thus (according to previous lemma):

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

We define **sup** as follows:

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

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

Note that $\mathbf{sup}(S)$ is well-defined

We prove that $\mathbf{sup}(S)$ is:

1. a member of **R**
2. a least upper bound of S

$$\mathbf{sup}(\boldsymbol{S}) \;\in\; \mathrm{R}$$

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

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

additivity constant is less than $\mathbf{3}$ but we can reduce this constant to $\mathbf{1}$

Reduce additivity constant to 1

- Reminder

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

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

Can we do this with **R** and **Z**?

Reduce additivity constant to 1

- Yes

$$\textbf{APPROX} \in \mathrm{R} \rightarrow (\mathrm{Z} \rightarrow \mathrm{Z}) \quad \textbf{APPROX}(f)(\mathrm{f}_n) \ \hat{=}\ \llbracket f{\star}\mathrm{f}_n \rrbracket$$

We have defined $maxR$ using the plugin and we prove that

$$\textbf{- 1} \leq \textbf{APPROX}(f)(\mathrm{f}_m \textbf{+} \mathrm{f}_n) \textbf{ - APPROX}(f)(\mathrm{f}_m) \textbf{ - APPROX}(f)(\mathrm{f}_n) \leq \textbf{1}$$

constants: $\boldsymbol{b}$, $\boldsymbol{Z}$, $\boldsymbol{leq}$, $\boldsymbol{maxR}$

Axioms:

$$\boldsymbol{b} \in \boldsymbol{Z} \rightarrowtail\!\!\!\!\!\twoheadrightarrow \mathbb{Z}$$

$$\{\boldsymbol{x} \mapsto \boldsymbol{y} | \boldsymbol{x} \in \boldsymbol{Z} \wedge \boldsymbol{y} \in \boldsymbol{Z} \wedge \boldsymbol{b}(\boldsymbol{x}) \leq \boldsymbol{b}(\boldsymbol{y})\} \subseteq \boldsymbol{leq}$$

$$(\boldsymbol{Z} \lhd \boldsymbol{leq} \rhd \boldsymbol{Z}) \cap (\boldsymbol{Z} \lhd \boldsymbol{leq} \rhd \boldsymbol{Z})^{-1} \subseteq \boldsymbol{id}$$

Definition

$$\begin{aligned}\boldsymbol{maxR} = (\boldsymbol{\lambda s} \cdot \boldsymbol{s} \in \mathbb{P}1(\boldsymbol{Z}) \wedge \\ &(\exists \boldsymbol{M} \cdot \boldsymbol{M} \in \boldsymbol{Z} \wedge (\forall \boldsymbol{x} \cdot \boldsymbol{x} \in \boldsymbol{s} \Rightarrow \boldsymbol{x} \mapsto \boldsymbol{M} \in \boldsymbol{leq}) \\ &| \ \boldsymbol{b}^{-1}(\boldsymbol{max}(\boldsymbol{b}[\boldsymbol{s}])))\end{aligned}$$

Theorems

$$\boldsymbol{maxR} \in \mathrm{dom}(\boldsymbol{maxR}) \rightarrow \boldsymbol{Z}$$

$$\forall \boldsymbol{s} \cdot \boldsymbol{s} \in \mathrm{dom}(\boldsymbol{maxR}) \Rightarrow \boldsymbol{maxR}(\boldsymbol{s}) \in \boldsymbol{s}$$

$$\forall \boldsymbol{s} \cdot \boldsymbol{s} \in \mathrm{dom}(\boldsymbol{maxR}) \Rightarrow (\forall \boldsymbol{f} \cdot \boldsymbol{f} \in \boldsymbol{s} \Rightarrow \boldsymbol{f} \mapsto \boldsymbol{maxR}(\boldsymbol{s}) \in \boldsymbol{leq})$$

Reduce additivity constant to 1

- Reminder: a bijection

$$\boldsymbol{b} \in \mathbf{Z} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathbb{Z} \quad \boldsymbol{b}(\mathrm{f}_{\boldsymbol{i}}) \;\hat{=}\; \mathrm{f}_{\boldsymbol{i}}(1) \quad (= \boldsymbol{i})$$

then we define the function **approx** as follows:

$$\textbf{approx} \in \mathrm{R} \rightarrow (\mathbb{Z} \rightarrow \mathbb{Z}) \quad \textbf{approx}(f)(n) \;\hat{=}\; b(\textbf{APPROX}(f)(\mathrm{f}_n))$$

$$-1 \leq \textbf{approx}(f)(m+n) - \textbf{approx}(f)(m) - \textbf{approx}(f)(n) \leq 1$$

Equivalence of **approx**(f) and f

Conclusion

- $\boldsymbol{Real} = \mathbf{approx}[\boldsymbol{R}]/$ **=**

- All 17 axioms on reals are proved

- Nothing is complicated in this construction (simple concepts)

- However, some of the proofs are a bit hairy (done with Rodin)

- If interested by the proofs, have a look at the paper:

"Constructing the Reals (an Exercise in Mathematical Methodology)"

- The implementation of Reals in Rodin will NOT be done in this way

- We'll use an axiomatic approach using the 17 (without type $\mathbb{Z} \leftrightarrow \mathbb{Z}$)