MASTER'S THESIS

J.T. Udding

A Theory of Real Numbers and its Presentation in AUTOMATH

Volume 1

Supervisor : Prof. dr. N.G. de Bruijn

Advisor : Dr. L.S. van Benthem Jutting

February 1980

EINDHOVEN UNIVERSITY OF TECHNOLOGY
Department of Mathematics
P.O. Box 513, 5600 MB Eindhoven, The Netherlands

SUMMARY.

In this master's thesis a formal introduction of the reals is given. They will be introduced starting from binary strings.

A description of the method will be given on two different levels of precision. The first one is a very detailed description in the usual style of mathematical presentation. The other one is written in the mathematical language AUT-QE. This text has been verified by a computer, and turned out to be correct. The relation between the two texts will be discussed.

The main conclusion is that AUT-QE is adequate to represent this part of mathematics, in spite of the big gap between everyday mathematics and formalized mathematics.

0. INTRODUCTION.

In this section we give a brief description of some ways to introduce the real numbers and the reason why we chose for one of them. Also we give a short review of the AUTOMATH languages and the way in which we apply one of these languages to establish the introduction of the reals in AUTOMATH.

1. The introduction of reals.

A usual way to introduce the reals is to start from the positive integers with Peano's axioms, to construct the integers with addition and multiplication, next to construct the rationals with division too, and finally to define the reals using fundamental sequences, Dedekinds cuts or nests of rationals [1,10,13]. A slightly different approach is to postpone the introduction of the negative numbers until the positive reals have been introduced [14].

All these methods have in common that the reals are introduced by repeated use of definition by abstraction. This is quite troublesome, but it also means that the real numbers become quite complicated objects. Hardly anybody has those things in mind when actually working with reals.

A method to avoid this problem is to introduce the reals from the integers as binary strings, which gives us the reals immediately, and to define operations and relations that give the system all the desired properties. This was recently done by [15] and [16]. Both addition and multiplication were defined by means of their algorithms. For multiplication this is not very easy.

In [6] de Bruijn showed how to deal with the additive group structure of the reals. Actually he started with subtraction as the basic operation, without ever using addition or multiplication of the integers. Moreover he indicated how one might proceed with the infimum, multiplication and division.

In the first part of this volume we give a more or less exhaustive treatment of the introduction of the reals by this method.

2. The AUTOMATH languages.

The languages of the AUTOMATH family are formal languages in which we can express large part of everyday mathematics. They are based on natural deduction and interpretable as correct mathematics as long as our writing in these languages is syntactically correct. This implies that texts in these languages are written in such a precise fashion that verification can be carried out automatically.

The AUTOMATH project was initiated at the Technological University of Eindhoven by de Bruijn, who designed the fundamentals of AUTOMATH. The aim was to develop languages as described above, to make computer programs for automatical verification and to test the idea for practical use.

More information about the project and its motivation can be found in [4]. Thus far several mutually related languages have been developed. We mention here AUT-68, AUT-QE which is an extension of the previous one [8] and AUT-QE-SYNT [12] .They all have the same basic features, a description of which can be found in [5]. The reader who is not acquainted with AUTOMATH at all is referred to [2], [3] and [11].

A computer program for verification has been implemented by Zandleven [18]. It is provided with a conversational mode for on-line checking and correction of texts. Zandleven's verifier checks AUT-68 and AUT-QE.

Large scale practical use of AUTOMATH has been made by Jutting, who translated Landau's booklet "Grundlagen der Analysis" into AUT-QE [12], by Zucker [20], Kornaat and others.

3. The translation into AUTOMATH and the verification.

The mathematical text as presented in part I was translated into AUT-QE. The second part of this volume describes the process of translating. Difficulties which occurred during translation as well as their solutions are shown. In particular we discuss the way to avoid a boring distinction into cases at various places, and to reduce the amount of writing by choosing the primitive types very carefully.

The third and last part of this volume contains a report of the experiences with the language and with the verification of the text. Some suggestions are made for changing the language definition slightly and for adapting the verification strategy of the program in order to speed up the writing and verification of AUTOMATH texts.

In volume II and III the final AUT-QE text is reproduced as checked (and found correct) by the verification program. It is a straightforward translation of the text in part I, although the AUT-QE text is much more detailed, of course.

I. THE INTRODUCTION OF THE REALS.

The mathematics behind the AUTOMATH text.

In this part we give a definition of reals by means of binary strings and supply it with the necessary structure to prove all the essential properties about reals.

1. The integers.

The system Z of all integers will be the basis to start from. We only need very weak assumptions about its structure. It is a non-empty totally ordered set without maximal or mininal element, where every non-empty subset which is bounded below (above) has a minimum (maximum). This implies that every element $k \in Z$ has a unique successor $k+$ and a unique predecessor $k-$. In order to express the non-emptiness of Z we say that $0 \in Z$. We define $1 := 0+$ and $2 := 1+$. For the ordering we use the symbol $<$ (less).

In the present discussion, however, we shall use addition (+) and subtraction (-) in Z , but later these operations will be eliminated.

The symbol to express equality between two elements of Z will be =. For functions from Z to Z we use the same symbol to denote extensional equality: If $f,g \in Z^Z$ then $f = g \Leftrightarrow \forall_{k \in Z} [f(k) = g(k)]$.

2. The reals.

As stated before, the reals will be introduced as binary strings (elements of Σ as defined below). The system Z will only serve to label the positions in those strings. After having created enough structure in the reals, the set of labels will be ignored completely, and we do not bother to embed Z into the reals.

We define $\Sigma := \{0,1\}^Z$ and $\mathcal{O} \in \Sigma$ by $\mathcal{O} := \Upsilon_{k \in Z}\, 0$. ($\Upsilon$ is Freudenthal's way to write Church's λ . Example: $\Upsilon_{k \in Z}\,(k^2 + k)$ is the function on Z that maps, for each $k \in Z$, k into $(k^2 + k)$).

An element $f \in \Sigma$ is said to be weakly positive if

$$\exists_{k \in Z} \forall_{\ell \in Z, \ell \leq k} [f(\ell) = 0]$$

and positive if it is weakly positive and not equal to $\mathcal{O}$. We say that it is negative if

$$\exists_{k\in Z}\ \forall_{\ell\in Z,\ell<k}\ [f(\ell) = 1] .$$

(Note that by this definition $\curlyvee_{k\in Z} 1$ is called negative, whereas one might think that it represents zero. This does not matter : This $\curlyvee_{k\in Z} 1$ will be discarded presently).

The element f is said to be signed if f is negative or weakly positive. If f and g fall into the same one of these two categories, we shall say that f and g have the same sign. It will be obvious that f, if it is signed, is either negative, or equal to $\mathcal{O}$ or positive.

We now define $\mathcal{R}$ to be the set of all $f \in \Sigma$ with the following two properties:

a) $\forall_{k\in Z}\ \exists_{\ell\in Z,k\leq\ell}\ [f(\ell) = 0]$

(We shall refer to this as the unique representation property).

b) f is signed.

2.1. Subtraction.

Let $f,g \in \Sigma$. We shall define $f - g$. For this subtraction we need a carry function p. It is an element of Σ and defined as follows:

$$p := \curlyvee_{k\in Z}\ \underline{\text{if}}\ \exists_{\ell\in Z,k<\ell}\ [f(\ell) < g(\ell) \wedge \forall_{m\in Z,k<m<\ell}\ [f(m) \leq g(m)]]$$

$$\underline{\text{then}}\ 1\ \ \underline{\text{else}}\ 0.$$

The subtraction is defined by means of :

$$f - g := \curlyvee_{k\in Z} (f(k) - g(k) - p(k) + p(k-) + p(k-)).$$

Theorem 2.1.1 : If $f \in \Sigma$ then we have

$$f - \mathcal{O} = f \text{ and } f - f = \mathcal{O}.$$

Proof . It is easy to check that p is equal to $\mathcal{O}$ in both cases. The definition of subtraction now immediately yields the desired result.

□

Theorem 2.1.2 : Let $f,g \in \Sigma$ and $k \in \mathbb{Z}$ then the following holds:

a) if $f(k) < g(k)$ then $p(f,g)(k-) = 1$

b) if $g(k) < f(k)$ then $p(f,g)(k-) = 0$

c) if $f(k) = g(k)$ then $p(f,g)(k-) = p(f,g)(k)$

Proof: This follows immediately from the definition of p. □

Theorem 2.1.3 : If $f,g \in \Sigma$ then we have $f - g \in \Sigma$.

Proof : Let $f,g \in \Sigma$, $k \in \mathbb{Z}$.

We know that $p \in \Sigma$ so $p(f,g)(k-), p(f,g)(k) \in \{0,1\}$.

If $f(k) < g(k)$ then we have $p(f,g)(k-) = 1$ in consequence of 2.1.2.a. The definition of subtraction leads easily to $(f - g)(k) \in \{0,1\}$. The other cases i.e. $g(k) < f(k)$ and $f(k) = g(k)$ are covered by 2.1.2.b and c.

□

Theorem 2.1.4 : If $f,g \in R$ then $f - g$ satisfies the unique representation property.

Proof : Let $f,g \in R$.

Let k be an integer and suppose that

$$\forall_{\ell \in \mathbb{Z}, k \leq \ell} [(f - g)(\ell) = 1] . \qquad (*)$$

First we show the existence of an $\ell \in \mathbb{Z}, k \leq \ell$ with $p(f,g)(\ell) = 0$.

If $p(f,g)(k) = 0$ $\ell = k$ will do.

If $p(f,g)(k) = 1$ the definition of p supplies an ℓ with $k < \ell$ and $f(\ell) < g(\ell)$. Using (*) and the definition of subtraction we find $p(f,g)(\ell) = 0$ which shows the existence of such an ℓ in all cases.

On the other hand, if $\ell \in \mathbb{Z}$, $k \leq \ell$ and $p(f,g)(\ell) = 0$, we have $f(\ell+) = 1$ and $p(f,g)(\ell+) = 0$, since $(f - g)(\ell+) = 1$.

By induction we obtain the existence of an $\ell \in \mathbb{Z}$ such that $f(m) = 1$ for $m \in \mathbb{Z}, \ell \leq m$.

This is a contradiction : $f \in R$ whence it satisfies the unique representation property.

So (*) turns out to be false which implies that $f - g$ satisfies the unique representation property.

□

Theorem 2.1.5 : If $f,g \in R$ and $f - g = 0$ we have $f = g$.

Proof : Let $f,g \in R$ and assume $f - g = 0$.

Let $k \in Z$. Then $(f - g)(k) = 0$.

Suppose $f(k) < g(k)$. With 2.1.2.a and the definition of subtraction we find $p(f,g)(k) = 1$.

If $\ell \in Z$, $k \leq \ell$ and $p(f,g)(\ell) = 1$ we see that $g(\ell+) = p(f,g)(\ell+) = 1$, because $(f - g)(\ell+) = 0$. Induction again shows that

$$\forall_{\ell \in Z, k \leq \ell} [g(\ell) = 1]$$

which is false since $g \in R$.

So for all $\ell \in Z$ we have $g(\ell) \leq f(\ell)$. **(*)**

Now suppose $g(k) < f(k)$. Again we find $p(f,g)(k) = 1$.

But then we have $f(k+) = 0$ and $g(k+) = 1$, since $(f - g)(k+) = 0$.

So $f(k+) < g(k+)$. This, however, is in contradiction with (*). So the only remaining possibility $f(k) = g(k)$ holds for all $k \in Z$.

□

Theorem 2.1.6 : If $f,g \in R$ and f is weakly positive and g is negative then $f - g$ is positive.

Proof : Let f, $g \in R$ and assume that f is weakly positive and g is negative.

It will be clear that there exists a $k \in Z$ such that

$$\forall_{\ell \in Z, \ell \leq k} [f(\ell) < g(\ell)] .$$

Let $k \in Z$ be such an integer.

In consequence of 2.1.2.a we know that

$$\forall_{\ell \in Z, \ell \leq k} [p(f,g)(\ell-) = 1].$$

With the definition of subtraction it immediately follows that

$$\forall_{\ell \in Z, \ell < k} [(f - g)(\ell) = 0] .$$

which means that $f - g$ is weakly positive. By 2.1.5 it follows that $f - g \neq 0$, since $f \neq g$. Hence $f - g$ is positive.

□

Theorem 2.1.7 : If $f,g \in R$ and f is negative and g is weakly positive then $f - g$ is negative.

Proof : Let f, $g \in R$ and assume that f is negative and g is weakly positive.

As in theorem 2.1.6 the existence of $k \in Z$ such that

$$\forall_{\ell \in Z, \ell \leq k} [g(\ell) < f(\ell)]$$

will be obvious.

Let k be such an integer.

In consequence of theorem 2.1.2.b we now can prove that

$$\forall_{\ell \in Z, \ell \leq k} [p(f,g)(\ell) = 0] \text{ and so}$$

$$\forall_{\ell \in Z, \ell < k} [(f - g)(\ell) = 1] .$$

This proves that $f - g$ is negative.

||

Theorem 2.1.8 : Let $f, g \in R$. Assume that f and g have the same sign and that $f \neq g$.

Then there exists a (unique) $k \in Z$ with

$$f(k) \neq g(k) \text{ and } \forall_{\ell \in Z, \ell < k} [f(\ell) = g(\ell)] .$$

Moreover, if this k satisfies $f(k) < g(k)$ then $f - g$ is negative, otherwise $f - g$ is positive.

Proof : Let $f,g \in R$ and assume that f and g have the same sign and that $f \neq g$.

It follows that there exists an $\ell \in Z$ with

$$\forall_{m \in Z, m \leq \ell} [f(m) = g(m)] . \qquad (*)$$

Define $S := \{m \in Z \mid f(m) \neq g(m)\}$. Then S is not empty since $f \neq g$, and S is bounded below because of (*).

So there exists a(unique) $k \in Z$ with

$$f(k) \neq g(k) \text{ and } \forall_{\ell \in Z, \ell < k} [f(\ell) = g(\ell)] \qquad (**)$$

which proves the first part of the theorem.

Now assume that this k satisfies $f(k) < g(k)$. Then we see from the definition of p and from (**) that

$$\forall_{\ell \in Z, \ell < k} [p(f,g)(\ell) = 1] .$$

It follows from the definition of subtraction that $(f - g)(\ell) = 1$ for $\ell \in Z, \ell < k$, which means that $f - g$ is negative.
Assume on the contrary that $g(k) < f(k)$.
Then we have

$$\forall_{\ell \in Z, \ell < k} [p(f,g)(\ell) = 0]$$

because of $(**)$, whence $(f - g)(\ell) = 0$ for $\ell \in Z, \ell < k$.
Hence $f - g$ is weakly positive. By 2.1.5 we infer that $f - g$ is positive.

□

Theorem 2.1.9 : Let $f \in R$ and let f be positive. Then $0 - f$ is negative.

Proof : This is a consequence of the preceding theorem for if $f \in R$ and f is positive then f and 0 have the same sign, and $f \neq 0$ because f is positive.

□

Theorem 2.1.10 : If $f,g \in R$ then $f - g \in R$.

Proof : Let $f,g \in R$. By 2.1.4 it suffices to prove that $f - g$ is signed.
If $f = g$ this follows from 2.1.1.
If f and g have the same sign and if $f \neq g$ this follows from 2.1.8.
If f is weakly positive and g is negative this is a consequence of 2.1.6. If f is negative and g is weakly positive this follows from 2.1.7. Since those four cases cover the whole range of possibilities the theorem has been proved.

□

Theorem 2.1.11 : If $f,g,h \in R$ then $f - (g - h) = h - (g - f)$.

Proof : Let $f,g,h \in R$.
We put $p1 := p(g,h)$, $p2 := p(g,f)$, $s1 := g - h$, $s2 := g - f$, $t1 := f - s1$, $t2 := h - s2$, $q1 := p(f,s1)$, $q2 := p(h,s2)$, $r1 := p1 - q1$, $r2 := p2 - q2$, $u := r1 - r2$, $w := t2 - t1$.
By the definition of subtraction we have for all k

$$s1(k) = g(k) - h(k) - p1(k) + p1(k-) + p1(k-),$$
$$t1(k) = f(k) - s1(k) - q1(k) + q1(k-) + q1(k-),$$

whence

$$t1(k) = f(k) + h(k) - g(k) + r1(k) - r1(k-) - r1(k-).$$

In the same way we find

$$t2(k) = f(k) + h(k) - g(k) + r2(k) - r2(k-) - r2(k-).$$

Subtracting we get

$$u(k-) + u(k-) = u(k) + w(k). \qquad (*)$$

Since $|r1(\ell)| \leq 1$ and $|r2(\ell)| \leq 1$ we have $|u(\ell)| \leq 2$ for all $\ell \in Z$. (Here we use the abbreviation $|k| \leq 1$ for $k \leq 1 \wedge (0 - k) \leq 1$, and similarly for $|k| \leq 2$). By 2.1.10 it follows that $t2 \in R$ and $t1 \in R$, and so $w \in R$. Hence, if $k \in Z$, we have $w(k) \in \{0,1\}$. Now it is obvious that $|u(k-)| \neq 2$, since the lefthand and righthand side of (*) are equal. So we have

$$\forall_{k \in Z} \, [|u(k)| \leq 1].$$

Suppose that there exists a $k \in Z$ with $u(k) = 1$. Let k be such an integer. If $\ell \in Z$, $k \leq \ell$ and $u(\ell) = 1$ then it follows from (*) that $u(\ell+) = w(\ell+) = 1$. Now induction leads to

$$\forall_{\ell \in Z, k \leq \ell} \, [u(\ell) = 1].$$

Let $\ell \in Z$ and $(k+) \leq \ell$.
Then $u(\ell) = u(\ell-) = 1$, so $w(\ell) = 1$, and so $t2(\ell) = 1$. This is in contradiction with the fact that for t2 the unique representation property holds, since $t2 \in R$. The conclusion is that there is no such $k \in Z$ with $u(k) = 1$.
In exactly the same way we can prove that

$$\forall_{k \in Z} \, [u(k) \neq -1]$$

which yields that $\forall_{k \in Z} \, [u(k) = 0]$.
So we conclude that $w = t2 - t1 = 0$. By 2.1.5 we have now $t2 = t1$ which proves the theorem.

□

2.2. Addition.

We define the addition by means of the subtraction as follows.
If $f, g \in \mathcal{R}$ then

$$f + g := f - (\mathcal{O} - g).$$

Theorem 2.2.1 : $(\mathcal{R},+)$ is a commutative group with neutral element $\mathcal{O}$; if $f, g \in \mathcal{R}$ then $h = f - g$ is the solution of the equation $g + h = f$.

Proof : Let $f, g, h \in \mathcal{R}$.
References to the theorems, motivating equality, will be given immediately after the equality sign.

i) $\mathcal{O}$ is a neutral element:
$f + \mathcal{O} = f - (\mathcal{O} - \mathcal{O}) =$ (2.1.1) $f - \mathcal{O} =$ (2.1.1) f.

ii) addition is commutative:
$f + g = f - (\mathcal{O} - g) =$ (2.1.11) $g - (\mathcal{O} - f) = g + f$.

iii) addition is associative:
$f + (g + h) =$ (ii) $f + (h + g) = f - (\mathcal{O} - (h - (\mathcal{O} - g))) =$ (2.1.11)
$f - ((\mathcal{O} - g) - (h - \mathcal{O})) =$ (2.1.1) $f - ((\mathcal{O} - g) - h)$.
By interchanging the rôles of f and h we have also
$h + (g + f) = h - ((\mathcal{O} - g) - f)$. (**)
In consequence of 2.1.11 (*) and (**) are equal, whence
$f + (g + h) = h + (g + f) =$ (ii) $(f + g) + h$.

iv) $g + (f - g) = g - (\mathcal{O} - (f - g)) =$ (2.1.11) $g - (g - (f - \mathcal{O})) =$
(2.1.1) $g - (g - f) =$ (2.1.11) $f - (g - g) =$ (2.1.1) f.
By putting $f = \mathcal{O}$ we see that indeed every $g \in \mathcal{R}$ has an inverse.

□

From now on the familiar properties of addition and subtraction will be used without explicit reference to 2.2.1.

2.3. Order.

For $f, g \in \mathcal{R}$ we say that $f < g$ if $g - f$ is positive.

Theorem 2.3.1 : If $f \in \mathcal{R}$ we have

f is positive (negative) $\Leftrightarrow \mathcal{O} < f \; (f < \mathcal{O})$.

Proof : Let $f \in \mathcal{R}$.

If f is positive so is $f - \mathcal{O}$.

If f is negative 2.1.6 yields that $\mathcal{O} - f$ is positive.

If $\mathcal{O} < f$ then $f - \mathcal{O} = f$ is positive.

If $f < \mathcal{O}$ then $\mathcal{O} - f$ is positive. In consequence of 2.1.9 $\mathcal{O} - (\mathcal{O} - f) = f + \mathcal{O} = f$ is negative.

□

Theorem 2.3.2 : $(\mathcal{R}, <)$ is a completely ordered set.

Proof : Let $f, g, h \in \mathcal{R}$.

i) $<$ is anti-reflexive.

In consequence of 2.1.1 we know that $f - f = \mathcal{O}$, so $f - f$ is not positive, whence $\neg(f < f)$.

ii) $<$ is transitive.

Assume $f < g$ and $g < h$. So $g - f$ and $h - g$ are positive. In consequence of 2.1.9 $\mathcal{O} - (h - g)$ is negative, so $g - h$ is negative as a result of 2.1.11 and 2.1.1. Application of 2.1.6 yields $(g - f) - (g - h)$ is positive, whence $h - f$ is positive.

iii) Assume $\neg(f < g)$ and $\neg(g < f)$. So $g - f$ is not positive. $g - f$ cannot be negative either, for 2.1.6 would say $\mathcal{O} - (g - f)$ is positive, so $f - g$ would be positive. It remains that $g - f = \mathcal{O}$. From 2.1.5 it follows that $f = g$.

□

Theorem 2.3.3 : If $f, g, h \in \mathcal{R}$ and $f < g$ then

$$f + h < g + h .$$

Proof : Let $f, g, h \in \mathcal{R}$.

Then we have $(g + h) - (f + h) = g - f$ is positive .

□

At this point we introduce for future reference the set of the positive reals $\mathcal{R}^+$ and the weakly positive reals $\mathcal{R}_0^{\ +}$:

$$\mathcal{R}^+ = \{f \in \mathcal{R} \mid \mathcal{O} < f\} \text{ and } \mathcal{R}_0^{\ +} := \mathcal{R}^+ \cup \{\mathcal{O}\} .$$

2.4. The infimum.

In order to define the infimum we need the well-known entier function. Here, however, we want to be able to cut off the tail of a real at any point, so we define:

if $f \in \Sigma$ and $k \in Z$ then entier $:= \bigcup_{\ell \in Z}$ <u>if</u> $\ell < k$ <u>then</u> $f(\ell)$ <u>else</u> 0.

(Note that entier(f.0) is what is usually called the entier of f).
It will be clear, if $f \in R$ and $k \in Z$, that entier(f,k) has the same sign as f and that it has the unique representation property, whence entier(f,k) $\in R$.

<u>Theorem 2.4.1</u> : The entier is non-decreasing with respect to the integer argument.

<u>Proof</u> : Let $f \in R$ and $k \in Z$.
If f(k+) = 0 then entier(f,k) = entier(f,k+).
If f(k+) = 1 then entier(f,k)(k+) < entier(f,k+)(k+) and they have the same sign, so from 2.1.8 we conclude that entier(f,k) < entier(f,k+) .

□

<u>Theorem 2.4.2</u> : If $f,g \in R$, $k \in Z$ and if $f < g$ and f and g have the same sign then entier(f,k) $\le$ entier(g,k) .

<u>Proof</u> : Let $f,g \in R$, $k \in Z$. Assume that $f < g$ and that f and g have the same sign. Let m be the integer from 2.1.8 with

$$f(m) \ne g(m) \text{ and } \forall_{\ell \in Z,\, \ell < m} [f(\ell) = g(\ell)] \,. \qquad (*)$$

Since $f < g$ we also have $f(m) < g(m)$.
If $k < m$ we see from the definition of entier and (*) that entier(f,k) = entier(g,k).
If $m \le k$ then we see that entier(f,k)(m) < entier(g,k)(m).
Hence we have entier(f,k) $\le$ entier(g,k).

□

We need a similar entier function on subsets of reals. So it is quite natural to define:

If $S \subset R$ and $k \in Z$ then set-entier $:= \{$entier(f, k) $\mid f \in S\}$.

which again is a subset of reals.

Theorem 2.4.3 : If $S \subset R$, $k \in Z$, $g \in R$ and if g is a smallest element of set-entier(S,k) then g is a lower bound of set-entier(S,k+).

Proof : Let $S \subset R$, $k \in Z$, $g \in R$ and assume that g is a smallest element of set-entier(S,k).

So if $f \in S$ then $g \leq$ entier(f,k) , and because of 2.4.1 and 2.3.2 we also know that then $g \leq$ entier(f,k+).

Hence g is a lower bound of set entier(S,k+).

[]

Assume from now on that S is a non-empty subset of R bounded below by 0.

Theorem 2.4.4 : If $k \in Z$, $g \in R$ and if g is a smallest element of set-entier(S,k+) then entier(g,k) is a smallest element of set-entier(S,k).

Proof : Let $k \in Z$, $g \in R$ and assume that g is a smallest element of set-entier(S,k+).

Then there exists a $g1 \in S$ with g = entier(g1,k+).

Let $g1 \in S$ be such an element. It will be clear that entier(g,k) = entier(g1,k), whence entier(g,k) $\in$ set-entier(S,k).

Let $f \in S$. Then we know $g \leq$ entier(f,k+). With 2.4.2 we see that entier(g,k) $\leq$ entier(entier(f,k+),k) = entier(f,k), whence entier(g,k) is a lower bound of set-entier(S,k).

Hence entier(g,k) is a smallest element of set-entier(S,k).

[]

Theorem 2.4.5 : There exists an $\ell \in Z$ with

$$\forall_{m \in Z, m \leq \ell} \, [0 \text{ is the smallest element of set-entier}(S,m)] \, .$$

Proof : Take $f \in S$ (note that S is non-empty). Since S is bounded below by 0, we have $0 \leq f$ so f is weakly positive by 2.3.1. Hence there exists an $\ell \in Z$ with

$$\forall_{m \in Z, m \leq \ell} \, [f(m) = 0] \, .$$

Let ℓ be such an integer and let $m \in Z$, $m \leq \ell$. Then obviously entier(f,m) = 0. So $0 \in$ set-entier(S,m). Moreover all elements in set-entier(S,m) are weakly positive, so 0 is the smallest element of set-entier(S,m).

[]

Theorem 2.4.6 : If $m \in Z$ then set-entier(S,m) has a smallest element.

Proof : Let $m \in Z$ and assume that set-entier(S,m) has a smallest element g, say. We shall prove that set-entier(S,m+) has a smallest element. We distinguish two cases : either

$$\forall_{g1 \in S}\ [g = \text{entier}(g1,m) \Rightarrow g1(m+) = 1] \quad (*) \qquad \text{or}$$

$$\exists_{g1 \in S}\ [g = \text{entier}(g1,m) \wedge g1(m+) = 0] \ .$$

The latter case is the easier, because if g1 is such an element then g = entier(g1,m+) $\in$ set-entier(S,m+) and from 2.4.3 we infer that g is a lower bound of set-entier(S,m+).
Now assume that (*) holds. Let $g1 \in S$ be such that g = entier(g1,m).
We prove that entier(g1,m+) is the smallest element of set-entier(S,m+).
Suppose the contrary i.e.:
Let $f \in S$ be such that entier(f,m+) < entier(g1,m+) . (**)
f and g1 are weakly positive and not equal so 2.1.8 supplies an $\ell \in Z$ with

$$f(\ell) < g1(\ell) \quad \text{and} \quad \forall_{k<\ell}\ [f(k) = g1(k)] \ .$$

It will be obvious in consequence of (*) and (**) that $\ell < m$. Hence entier(f,m) < entier(g1,m) = g which is a contradiction since g is supposed to be the smallest element of set-entier(S,m).
We now have proved that set-entier(S,m+) has a smallest element, provided that set-entier(S,m) has one. By induction, using 2.4.5, it follows that set-entier(S,m) has a smallest element for $m \in Z$.

Because of the uniqueness of smallest elements we are now able to define:
If $k \in Z$ then
smel(k) := the smallest element of set-entier(S,k).

We define (by means of some kind of diagonal process):

$$\text{pos-inf} := \Upsilon_{k \in Z}\ \text{smel}(k)(k) \ .$$

Since smel(k) $\in R$ for $k \in Z$ we see immediately that pos-inf $\in \Sigma$, and from 2.4.5 we have that pos-inf is weakly positive, and therefore signed.

Theorem 2.4.7 : If $k \in Z$ then entier(pos-inf,k) = smel(k).

Proof : From 2.4.5 again we have the existence of an $\ell \in Z$ with

$$\forall_{k \in Z, k < \ell}[\text{entier(pos-inf,k)} = 0 = \text{smel(k)}] .$$

Let $k \in Z$ and assume that entier(pos-inf,k) = smel(k). We prove that entier(pos-inf,k+) = smel(k+) . Let $\ell \in Z$.
If $\ell \leq k$ then entier(pos-inf,k+)(ℓ) = entier(pos-inf,k)(ℓ)
= smel(k)(ℓ) = (2.4.4) entier(smel(k+),k)(ℓ) = smel(k+)(ℓ).
If (k+) $< \ell$ then entier(pos-inf,k+)(ℓ) = 0 = smel(k+)(ℓ) .
If ℓ = k+ the equality follows from the definition of pos-inf.
Induction yields the desired result.

$\square$

Theorem 2.4.8 : pos-inf $\in \bar{R}$.

Proof : It suffices to prove the unique representation property. Let $k \in Z$ and suppose that

$$\forall_{\ell \in Z, k \leq \ell}[\text{pos-inf}(\ell) = 1] . \qquad (*)$$

Since entier(pos-inf,k) = smel(k) by 2.4.7, there exists an $f \in S$ with

entier(pos-inf,k) = entier(f,k) .

Let f be such an element of S. Let $\ell \in Z$ be the smallest element greater than k with f(ℓ) = 0. This ℓ exists since f has the unique representation property.
Hence if $m \in Z$, $m < \ell$ then pos-inf(m) = f(m) and pos-inf(ℓ) = 1 $\neq$ 0 = f(ℓ). So with 2.1.8 we see that entier(f,ℓ) < entier(pos-inf,ℓ) = smel(ℓ). This contradicts the fact that smel(ℓ) is the smallest element of set-entier(S,ℓ). So (*) cannot hold which means that pos-inf has the unique representation property.

Theorem 2.4.9 : If $f \in S$ then pos-inf $\leq f$.

Proof: Let $f \in S$ and suppose $f <$ pos-inf. Let $k \in \mathbb{Z}$ be such that $f(k) <$ pos-inf(k) and $\forall_{m \in \mathbb{Z}, m<k}$ [$f(m) =$ pos-inf(m)] .

That this k exists we see from 2.1.8, since f and pos-inf are both weakly positive and not equal. But then we also have entier(f,k) < entier(pos-inf,k) = (2.4.7) smel(k). However, smel(k) is the smallest element of set-entier(S,k). Hence pos-inf $\leq$ f.

[]

Theorem 2.4.10 : If $f \in \mathbb{R}$ and pos-inf $< f$ then there exists a $g \in S$ with $g < f$.

Proof: Let $f \in \mathbb{R}$ and assume pos-inf $< f$. pos-inf is weakly positive, so with 2.3.1 and 2.3.2 we see that f is also weakly positive. Moreover pos-inf $\neq$ f, whence 2.1.8 supplies some $k \in \mathbb{Z}$ with

$$\text{pos-inf}(k) < f(k) \text{ and } \forall_{m \in \mathbb{Z}, m<k} [\text{pos-inf}(m) = f(m)] . \quad (*)$$

From 2.4.7 we derive that entier(pos-inf,k) = smel(k). Since smel(k) $\in$ set-entier(S,k) there exists a $g \in S$ with smel(k) = entier(g,k). Let g be such an element of S. Then we have entier(pos-inf,k) = entier(g,k), which with (*) yields $g < f$. So there exists a $g \in S$ with $g < f$.

[]

Thus far we assumed S to be bounded below by 0. For such an S we have defined an infimum and have proved all its essential properties. We now take the weaker assumption that S is bounded below.

Theorem 2.4.11 : If $S \subset \mathbb{R}$ is non-empty and bounded below then there exists a $g \in \mathbb{R}$ with

i) $\forall_{f \in S} [g \leq f]$ and (ii) $\forall_{f \in \mathbb{R}, g<f} \exists_{h \in S} [h < f]$.

Proof : Let $S \subset R$ be non-empty and bounded below. Let $f0 \in R$ be a lower bound of S. We define $A := \{f - f0 \mid f \in S\}$.

Now A is a non-empty subset of R, bounded below by 0, so pos-inf(A) exists. We put g := pos-inf(A) + f0 and prove that g satisfies both properties.

i) Let $f \in S$. So $f - f0 \in A$, and from 2.4.9 we know that pos-inf(A) $\leq$ $f - f0$.

With 2.3.3 we now derive that g = pos-inf(A) + f0 $\leq$ f.

ii) Let $f \in R$ and assume $g < f$.

Then we know from 2.3.3 that $g - f0 < f - f0$.

Hence pos-inf(A) $<$ $f - f0$.

Now 2.4.10 supplies an $h \in A$ with $h < f - f0$.

It follows that $h + f0$ is satisfactory since $h + f0 \in S$ and $h + f0 < f$.

□

Since there exists at most one element in R with the properties of 2.4.11 we define:

If $S \subset R$ is non-empty and bounded below then inf := the element in R with the properties of 2.4.11.

2.5. The set of integers as a subset of the reals.

The system of integers $Z^* \subset R$ is defined as:

$$Z^* := \text{set-entier}(R,0) \ .$$

Of course $0 \in Z^*$, and if we define

$$1 := \Upsilon_{k \in Z}\ \underline{\text{if}}\ k = 0\ \underline{\text{then}}\ 1\ \underline{\text{else}}\ 0$$

then 1 is an element of Z^* too, and 1 is positive.
Furthermore Z^* is closed with respect to subtraction and addition. This is easily seen from the definitions.

<u>Theorem 2.5.1</u> : If $f \in \mathcal{R}$ then $\exists_{g \in Z^*} [f < g]$.

<u>Proof</u> : Let $f \in \mathcal{R}$.
We put $h := \curlyvee_{k \in Z}$ <u>if</u> $k \leq 0$ <u>then</u> 1 <u>else</u> $f(k)$.
h has the unique representation property, since $f \in \mathcal{R}$. Moreover h is negative. Hence $h \in \mathcal{R}$.
From the definition of $p(f,h)$ it is easily derived that $p(f,h)(\ell) = 0$ for $\ell \in Z$, $0 < \ell$. The definition of subtraction now yields that $(f - h)(\ell) = 0$ for $\ell \in Z$, $0 < \ell$. Hence $f - h \in Z^*$.
h is negative, which leads with 2.3.1 and 2.3.3 to $f < f - h$.
So there exists some $g \in Z^*$ with $f < g$.

||

In the same way we can prove that if $f \in \mathcal{R}$

$$\exists_{g \in Z^*} [g < f] \ .$$

<u>Theorem 2.5.2</u> : There is no integer between $\mathit{0}$ and $\mathit{1}$.

<u>Proof</u> : Let $f \in \mathcal{R}$ and assume that $\mathit{0} < f < \mathit{1}$.
Then f and $\mathit{1}$ are both positive by 2.3.1. Moreover they are not equal, so there exists a $k \in Z$ with

$$f(k) < \mathit{1}(k) \text{ and } \forall_{\ell \in Z;\, \ell < k} [f(\ell) = \mathit{1}(\ell)]$$

in consequence of 2.1.8. This k can only have the value 0. So $f(\ell) = 0$ for $\ell \in Z$, $\ell \leq 0$.
Since $f \neq \mathit{0}$ there must be an $\ell \in Z$ with $0 < \ell$ and $f(\ell) = 1$, so $f \notin Z^*$.

||

We also need a notation for the positive elements of Z^* :

$$Z^{*+} := \{f \in Z^* \mid \mathit{0} < f\} \ .$$

2.6. <u>The set Q^*.</u>

For the introduction of multiplication we need a countable set which [illegible] in $\mathcal{R}$, for which we take

$$Q^* := \{f \in \mathcal{R} \mid \exists_{k \in Z} [f \in \text{set-entier}(\mathcal{R},k)]\} \ .$$

Obviously:

- $Z^{*} \subset Q2$.
- Q2 is closed with respect to subtraction and addition.

Theorem 2.6.1 : Q2 is dense in R.

Proof : Let $f, g \in R$, $g < f$. So $f - g$ and 0 have the same sign and they are not equal. Again 2.1.8 gives us a $k \in Z$ with

$$(f - g)(k) = 1 \text{ and } \forall_{m \in Z, m<k} \left[(f - g)(m) = 0 \right] . \quad (*)$$

We define

$$h := \Upsilon_{\ell \in Z} \;\underline{\text{if}}\; \ell \le k \;\underline{\text{then}}\; 0 \;\underline{\text{else}}\; \underline{\text{if}}\; \ell = k+ \;\underline{\text{then}}\; 1 \;\underline{\text{else}}\; f(\ell) .$$

This h is positive and it has the unique representation property since $f \in R$, so $h \in R$. In the same way as in 2.5.1 we derive

$$\forall_{\ell \in Z, (k+) < \ell} \left[(f - h)(\ell) = 0 \right] .$$

So $f - h \in Q2$.

h is positive, so $f - h < f$. From 2.1.8, (*) and the definition of h it follows that $h < f - g$. Using 2.3.3 we get $g < f - h$.

Hence there exists an element in Q2 between g and f.

[]

Another set that we need is:

$$Q2^{+} := \{ f \in Q2 \mid 0 < f \} .$$

$Q2^{+}$ is closed with respect to addition, and $1 \in Q2^{+}$.

Furthermore we define operations for "multiplication with" and "division by" 2 i.e.:

If $f \in \Sigma$ then

$$\text{half}(f) := \Upsilon_{k \in Z} \; f(k-) .$$

$$\text{twice}(f) := \Upsilon_{k \in Z} \; f(k+) .$$

The following assertions are obvious consequences of these definitions.

- If $f \in \mathcal{R}$ then half(f) and twice(f) $\in \mathcal{R}$.
- If $f \in Q2$ then half(f) and twice(f) $\in Q2$.
- If $f \in \mathcal{R}$ then half(f) and twice(f) have the same sign as f.
- If $f \in Q2^+$ then half(f) and twice(f) $\in Q2^+$.
- If $f \in \mathcal{R}$ and $\mathcal{O} < f$ then half(f) < f and f < twice(f) (both to be proved with 2.1.8).
- half and twice are inverse operations .
- If $f,g \in \mathcal{R}$ and f < g then half(f) < half(g) .

<u>Theorem 2.6.2</u> : If $f,g \in \mathcal{R}$ then half(f + g) = half(f) + half(g).

<u>Proof</u> : Let $f,g \in \mathcal{R}, k \in \mathcal{Z}$.

First we prove that p(f,g)(k-) = p(half(f),half(g))(k).

Assume that p(f,g)(k-) = 1, so

$$\exists_{\ell \in \mathcal{Z},(k-)<\ell}\left[f(\ell) < g(\ell) \wedge \forall_{m \in \mathcal{Z},(k-)<m<\ell}[f(m) \le g(m)]\right]. \quad (*)$$

Let ℓ be such an integer. Then $(k-) < \ell$ so $k < (\ell+)$.

Since $f(\ell) < g(\ell)$ we also have half(f)(ℓ+) < half(g)(ℓ+).

If $m \in \mathcal{Z}$, $k < m < (\ell+)$ then (*) and the definition of half yield half(f)(m) < half(g)(m).

So

$$\exists_{\ell 1 \in \mathcal{Z},k<\ell 1}\left[\text{half}(f)(\ell 1) < \text{half}(g)(\ell 1) \wedge \forall_{m \in \mathcal{Z},k<m<\ell 1}[\text{half}(f)(m) \le \text{half}(g)(m)]\right]$$

that is $\ell 1 = \ell+$.

So we see that also p(half(f), half(g))(k) = 1. Hence

$$p(f,g)(k-) = 1 \Rightarrow p(\text{half}(f),\text{half}(g))(k) = 1 . \quad (**)$$

Now assume that p(half(f),half(g))(k) = 1 .

Then we have:

$$\exists_{\ell \in \mathcal{Z},k<\ell}\left[\text{half}(f)(\ell) < \text{half}(g)(\ell) \wedge \forall_{m \in \mathcal{Z},k<m<\ell}[\text{half}(\ell)(m) \le \text{half}(g)(m)]\right] .$$

Let ℓ be such an integer. Then $k < \ell$ so $(k-) < (\ell-)$. Since $\mathrm{half}(f)(\ell) <$ $\mathrm{half}(g)(\ell)$ we also have $f(\ell-) < g(\ell-)$. If $m \in \mathbb{Z}$ $(k-) < m < (\ell-)$ then we have $f(m) = g(m)$. So $\ell-$ is an integer satisfying all properties of $(*)$. Hence we find $p(f,g)(k-) = 1$.
With $(**)$ this leads to

$$p(f,g)(k-) = 1 \Leftrightarrow p(\mathrm{half}(f), \mathrm{half}(g))(k) = 1 \ ,$$

whence we find

$$p(f,g)(k-) = p(\mathrm{half}(f), \mathrm{half}(g))(k) \ .$$

Remembering the definition of $(f - g)(k-)$ and $(\mathrm{half}(f) - \mathrm{half}(g))(k)$, we see that

$$(f - g)(k-) = (\mathrm{half}(f) - \mathrm{half}(g))(k) \ .$$

This holds for all $k \in \mathbb{Z}$, so we have proved:

$$\mathrm{half}(f - g) = \mathrm{half}(f) - \mathrm{half}(g) \ .$$

It follows that:

$$\mathrm{half}(f + g) = \mathrm{half}(f - (\mathcal{O} - g)) = \mathrm{half}(f) - \mathrm{half}(\mathcal{O} - g) =$$
$$= \mathrm{half}(f) - (\mathcal{O} - \mathrm{half}(g)) = \mathrm{half}(f) + \mathrm{half}(g) \ .$$

□

<u>Theorem 2.6.[illegible]</u> : If $S \subset \mathbb{Q}2^+$, if $\mathcal{I} \in S$ and if $f \in S$ implies $f + \mathcal{I}$ and $\mathrm{half}(f) \in S$ then we have $S = \mathbb{Q}2^+$.

<u>Proof</u> : Let $S \subset \mathbb{Q}2^+$ satisfy the desired properties. First we prove that $\mathbb{Z}^{*+} \subset S$.
Suppose the contrary i.e. suppose that $T := \{f \in \mathbb{Z}^{*+} \mid f \notin S\} \neq \emptyset$.
T is obviously bounded below by $\mathcal{O}$ and T is non-empty so, by 2.4.6, T has a smallest element f, say.
Since $f \in \mathbb{Z}^{*+}$ we have $\mathcal{O} < f$. But then, in consequence of 2.5.2 and the fact that $\mathcal{I} \in S$, we also have $\mathcal{I} < f$.
$\mathbb{Z}^{*}$ is closed with respect to subtraction and $f - \mathcal{I}$ is positive, so $f - \mathcal{I} \in \mathbb{Z}^{*+}$ and $f - \mathcal{I} \notin T$, since f was the smallest element of T.
So $f - \mathcal{I} \in S$ but this implies that $(f - \mathcal{I}) + \mathcal{I} = f \in S$, so $f \notin T$.
This is a contradiction, so T is empty and $\mathbb{Z}^{*+} \subset S$. Let $k \in \mathbb{Z}$ and assume that $\text{set-entier}(\mathbb{R}^+,k) \subset S$. We shall prove that $\text{set-entier}(\mathbb{R}^+,k+) \subset S$.

Let $f \in$ set-entier(R^+,k+). Then twice(f) $\in$ set-entier(R^+,k) so twice(f) $\in$ S. But this implies that f = half(twice(f)) $\in$ S.
So set-entier(R^+,k+) $\subset$ S.
By induction, noting that Z^{*+} = set-entier(R^+,0), we see that $Q2^+ \subset$ S. Hence S = $Q2^+$.

□

Lemma 2.6.4 : If S $\subset$ Q2, if $0 \in$ S and if f $\in$ S implies f-$1 \in$ S and half(f) $\in$ S then we have $\{g \in Q2^+ \mid 0 - g \in S\} = Q2^+$.

Proof : Let S $\subset$ Q2 satisfy the desired properties.
We put T := $\{g \in Q2^+ \mid 0 - g \in S\}$ and prove T = $Q2^+$ with 2.6.3.
It is obvious that $0 - 1 \in$ S. So $1 \in$ T. Let g $\in$ T. So $0 - g \in$ S.
Then we know $0 - (g + 1) = (0 - g) - 1 \in$ S, so $g + 1 \in$ T.
And 0 - half(g) = half(0 - g) $\in$ S, so half(g) $\in$ T.
Hence with 2.6.3 we derive T = $Q2^+$.

□

Theorem 2.6.4 : If S $\subset$ Q2, if $0 \in$ S and if f $\in$ S implies f + 1, f - 1 and half(f) $\in$ S then we have S = Q2.

Proof : Let S $\subset$ Q2 have the desired properties. It will be clear that $1 = 0 + 1 \in$ S so with 2.6.3 we derive $Q2^+ \subset$ S.
It remains to prove: if f $\in$ Q2, f < 0 then f $\in$ S.
Let f $\in$ Q2 and assume that f < 0. So 0 - f $\in Q2^+$, since Q2 is closed with respect to subtraction and 0 - f is positive. With lemma 2.6.4 we have $0 - (0 - f) \in$ S so f + 0 = f $\in$ S.
Hence Q2 $\subset$ S and so S = Q2.

□

Application of 2.6.3 (2.6.4) will be called induction in $Q2^+$(Q2).

Theorem 2.6.5 : half(1) + half(1) = 1.

Proof : With the definition of p it is easy to derive that:
- if k $\in$ Z, k $\neq$ 0 then p(1,half(1))(k) = 0.
- p(1,half(1))(0) = 1.

Remembering the definition of subtraction we see that (1 - half(1))(k) = 1 holds only if (k-) = 0.
Hence 1 - half(1) = half(1) and therefore

half(1) + half(1) = 1.

□

At this point Z has served its purpose and from now on we will ignore it completely. Actually we are able to prove that Z^* has the properties which were postulated for Z, but we do not need this for our purposes.

Theorem 2.6.6 : If $f \in Q2$ then $\mathrm{half}(f) + \mathrm{half}(f) = f$.

Proof : We prove this by induction in Q2.

By 2.6.5 we see immediately that the theorem holds for $f = 1$.

Assume it holds for $f \in Q2$. Then we have

- $\mathrm{half}(f + 1) + \mathrm{half}(f + 1) =$ (2.6.2) $\mathrm{half}(f) + \mathrm{half}(f) + \mathrm{half}(1) + \mathrm{half}(1) = f + 1$.
- $\mathrm{half}(f - 1) + \mathrm{half}(f - 1) = \mathrm{half}(f) + \mathrm{half}(f) - (\mathrm{half}(1) + \mathrm{half}(1)) = f - 1$.
- $\mathrm{half}(\mathrm{half}(f)) + \mathrm{half}(\mathrm{half}(f)) = \mathrm{half}(\mathrm{half}(f) + \mathrm{half}(f)) = \mathrm{half}(f)$.

With 2.6.4 the theorem follows.

□

Theorem 2.6.7 : If $f,g,h \in R$ and if $f + g < h$ then

$$\exists_{f1 \in Q2}\, \exists_{g1 \in Q2}\, [(f < f1) \wedge (g < g1) \wedge ((f1 + g1) < h)] .$$

Proof : Let $f,g,h \in R$ and assume $f + g < h$.

Since Q2 is dense in R (2.6.1) there exists an $h1 \in Q2$ with $0 < h1$ and $h1 < (h - (f + g))$, for $h - (f + g)$ is real and positive.

Let h1 be such an element of R.

Then we have $0 < \mathrm{half}(h1)$, and 2.3.3 leads to $f < f + \mathrm{half}(h1)$ and $g < g + \mathrm{half}(h1)$.

Applying 2.6.1 twice, we get f1 and g1 in Q2 with $f < f1 < f + \mathrm{half}(h1)$ and $g < g1 < g + \mathrm{half}(h1)$.

Now 2.3.3 leads easily to $f1 + g1 < f + g + \mathrm{half}(h1) + \mathrm{half}(h1)$.

Since $h1 \in Q2$ this leads with 2.6.6 to

$$f1 + g1 < f + g + h1 < f + g + (h - (f + g)) = h.$$

□

2.7. Multiplication in Q2.

Let us consider homomorphisms M of Q2 i.e. mappings of Q2 into itself that satisfy $M(f + g) = M(f) + M(g)$ for $f,g \in Q2$.
It will be obvious, if M is a homomorphism of Q2 and $f,g \in Q2$, that

- $M(f - g) = M(f) - M(g)$.
- $M(0) = 0$.

Theorem 2.7.1 : If M is a homomorphism of Q2 and $f \in Q2$ then

$$M(half(f)) = half(M(f)).$$

Proof : Let M be a homomorphism of Q2 and let $f \in Q2$.
As a result of 2.6.6 we see

$$M(f) = M(half(f) + half(f)) = M(half(f)) + M(half(f)).$$

So

$$half(M(f)) = half(M(half(f)) + M(half(f))) =$$
$$half(M(half(f))) + half(M(half(f)))$$

in consequence of 2.6.2.
Again by 2.6.6, since $M(half(f)) \in Q2$ we have

$$half(M(f)) = M(half(f)).$$

||

We define the trivial homomorphism Z as:

$$Z := \text{Y}_{f \in Q2}\ 0 .$$

If M is a homomorphism of Q2 then we define:

$$M^{+} := \text{Y}_{f \in Q2}\ (M(f) + f) ,$$

$$M^{-} := \text{Y}_{f \in Q2}\ (M(f) - f) \qquad \text{and}$$

$$M^{h} := \text{Y}_{f \in Q2}\ half(M(f)) .$$

It is easy to check that M^{+}, M^{-} and M^{h} are homomorphisms too.

Theorem 2.7.2 : If $f \in Q2$ then there exists exactly one homomorphism M of $Q2$ with $M(1) = f$.

Proof : The first part of this proof deals with the existence, the second part with the uniqueness of such homomorphisms.

(i) The proof goes by induction in Q2.
Z is a homomorphism with $Z(1) = 0$ so the existence of a homomorphism M with $M(1) = 0$ has been proved.
Assume that we have for some $f \in Q2$ a homomorphism M of $Q2$ with $M(1) = f$.
Then M^+, M^-, M^h are homomorphisms with the desired properties for $f + 1$, $f - 1$ and half(f) respectively.
By induction we now have for all $f \in Q2$ the existence of a homomorphism M of $Q2$ with $M(1) = f$

(ii) The uniqueness.
Let $f \in Q2$ and assume that M_1 and M_2 are homomorphisms of $Q2$ with $M_1(1) = M_2(1) = f$. Again by induction we prove $M_1 = M_2$.
Since M_1 and M_2 are homomorphisms we have $M_1(0) = M_2(0) = 0$.
Leg $g \in Q2$ and assume $M_1(g) = M_2(g)$.
Then we also have the equality of M_1 and M_2 for $g + 1$, $g - 1$ and half(g) since $M_1(1) = M_2(1)$.
By induction it easily follows that $M_1 = M_2$.

□

Now we are able to define for $f \in Q2$:

$$M_f := \text{the homomorphism of } Q2 \text{ with } M_f(1) = f \, .$$

Multiplication in Q2 is the binary operation, that attaches to every pair $f,g \in Q2$ the value $M_f(g)$. Its right distributivity follows from the fact that M_f is a homomorphism, the left distributivity then follows by 2.7.3.

Theorem 2.7.3 (commutativity) : If $f,g \in Q2$ then $M_f(g) = M_g(f)$.

Proof : We prove this by induction in Q2 with respect to g. Let $f \in Q2$.
We have $M_f(0) = 0$ since M_f is a homomorphism. $M_0 = Z$ because of 2.7.2 (ii), whence $M_f(0) = M_0(f)$. Let $g \in Q2$ and assume that $M_f(g) = M_g(f)$. Hence:

- $M_f(g + 1) = M_f(g) + M_f(1) = M_g(f) + f = M_g^+(f)$.

  We have $M_g^+(1) = g + 1$, and M_g^+ is a **homomorphism** of Q2, so 2.7.2 (ii) leads to $M_g^+ = M_{g+1}$.

  Hence $M_f(g + 1) = M_{g+1}(f)$.

- $M_f(g - 1) = M_f(g) - M_f(1) = M_g(f) - f = M_g^-(f)$.

  As in the previous case we have $M_g^- = M_{g-1}$, so $M_f(g - 1) = M_{g-1}(f)$.

- $M_f(\text{half}(g)) = (2.7.1)\ \text{half}(M_f(g)) = \text{half}(M_g(f)) = M_g^h(f)$.

  Again applying the uniqueness of this kind of homomorphisms we find $M_g^h(f) = M_{\text{half}(g)}(f)$.

  So $M_f(\text{half}(g)) = M_{\text{half}(g)}(f)$.

Now induction shows that (for all $f,g \in$ Q2)

$$M_f(g) = M_g(f) \ .$$

□

Theorem 2.7.4 (associativity) : If $f,g,h \in$ Q2 then

$$M_{M_f(g)}(h) = M_f(M_g(h)) \ .$$

Proof : We prove this by induction in Q2 with respect to f. Let $g,h \in$ Q2. $M_0(g) = M_0(h) = M_0(M_g(h)) = 0$ as we have seen in the proof of 2.7.3. So for $f = 0$ the theorem holds. Let $f \in$ Q2 and assume that $M_{M_f(g)}(h) = M_f(M_g(h))$.

Then we derive with 2.7.3 all the time:

- $M_{f+1}(g) = M_f(g) + g$. So

  $$M_{M_{f+1}(g)}(h) = M_{M_f(g)+g}(h) = M_{M_f(g)}(h) + M_g(h) \ .$$

  The induction assumption now yields:

  $$M_{M_{f+1}(g)}(h) = M_f(M_g(h)) + M_g(h) =$$

  $$M_f(M_g(h)) + M_1(M_g(h)) =$$

  $$M_{f+1}(M_g(h)) \ .$$

- $M_{f-1}(g) = M_f(g) - g$. So in the same way as before we get:

$$M_{M_{f-1}(g)}(h) = M_{M_f(g)}(h) - M_g(h) =$$

$$M_f(M_g(h)) - M_1(M_g(h)) =$$

$$M_{f-1}(M_g(h)) \ .$$

- $M_{half(f)}(g) = half(M_f(g))$ with 2.7.1. So we get

$$M_{M_{half(f)}(g)}(h) = M_{half(M_f(g))}(h) = (2.7.1)$$

$$half(M_{M_f(g)}(h)) = half(M_f(M_g(h))) = (2.7.1)$$

$$M_{half(f)}(M_g(h)) \ .$$

Hence by induction we proved for all $f,g,h \in Q2$ that

$$M_{M_f(g)}(h) = M_f(M_g(h)) \ .$$

[]

<u>Theorem 2.7.5</u> (monotonicity) : If $f,g \in Q2$, $h \in Q2^+$ and if $f < g$ then

$$M_h(f) < M_h(g) \ .$$

<u>Proof</u> : The proof goes by induction in $Q2^+$ with respect to h. Let $f,g \in Q2$. Since $M_1(f) = f < g = M_1(g)$ we see that the theorem holds for $h = 1$. Now assume the theorem holds for $h \in Q2^+$. Then, using the commutativity of 2.7.3 all the time:

- $M_{h+1}(f) = M_h(f) + f < M_h(g) + g = M_{h+1}(g)$.

- $M_{half(h)}(f) = (2.7.1)\ half(M_h(f)) < half(M_h(g)) = (2.7.1)\ M_{half(h)}(g)$.

This completes the induction proof.

[]

A consequence of this theorem is that $M_f(g) \in Q2^+$ for $f,g \in Q2^+$.

Theorem 2.7.6 (continuity): If $f \in Q2^+$ then we have for all $\varepsilon \in Q2^+$:

$$\exists_{g \in Q2^+} [M_f(g) \leq \varepsilon].$$

Proof : We shall prove a stronger theorem that is easier to prove:
If $f \in Q2^+$ then we have for all $\varepsilon \in Q2^+$

$$\exists_{g \in Q2^+, g \leq \varepsilon} [M_f(g) \leq \varepsilon]. \qquad (*)$$

The proof goes by induction in $Q2^+$ with respect to f. If $\varepsilon \in Q2^+$ we have $\varepsilon \leq \varepsilon$ and $M_1(\varepsilon) = \varepsilon \leq \varepsilon$.
Hence for $f = 1$ the theorem holds.
Now assume the theorem is true for some $f \in Q2^+$. So for all $\varepsilon \in Q2^+$ (*) holds.

- Let $\varepsilon \in Q2^+$, then $\mathrm{half}(\varepsilon) \in Q2^+$. Let $g \in Q2^+$ be such that $g \leq \mathrm{half}(\varepsilon)$ and $M_f(g) \leq \mathrm{half}(\varepsilon)$. (This g exists as follows from (*) applied to $\mathrm{half}(\varepsilon)$). But then we have

$$M_{f+1}(g) = M_f(g) + g \leq \mathrm{half}(\varepsilon) + \mathrm{half}(\varepsilon) = \varepsilon$$

and since $\mathrm{half}(\varepsilon) < \varepsilon$, we now have proved that for $\varepsilon \in Q2^+$ (*) holds for $f + 1$.

- Let again $\varepsilon \in Q2^+$.
Let $g \in Q2^+$ be such that $g \leq \varepsilon$ and $M_f(g) \leq \varepsilon$. Now

$$M_{\mathrm{half}(f)}(g) = \mathrm{half}(M_f(g)) \leq \mathrm{half}(\varepsilon) < \varepsilon$$

since $0 < \varepsilon$.
So $g \in Q2^+$ satisfying (*) for f, also satisfies (*) for half(f).

Now by induction it immediately follows that (*) will hold for all $f \in Q2^+$ and $\varepsilon \in Q2^+$.

□

2.8. Multiplication in $\mathcal{R}_0^+$.

We have defined multiplication in Q2 and proved all its basic properties. We shall extend it now to the set of weakly positive reals.
For that purpose we define a multiplication set for all $f,g \in \mathcal{R}_0^+$:

If $f,g \in \mathcal{R}_0^+$ then
$$\text{mult-set} := \{M_{f1}(g1) \mid f1,g1 \in Q2^+,\ f < f1,\ g < g1\} .$$

It is easy to check that:

- If $f,g \in \mathcal{R}_0^+$ then mult-set(f,g) = mult-set(g,f) since the multiplication in Q2 is commutative by 2.7.3.
- If $f,g \in \mathcal{R}_0^+$ then mult-set(f,g) is bounded below by $\mathcal{O}$ since multiplication of two positive elements in Q2 yields a positive result.
- If $f,g \in \mathcal{R}_0^+$ then mult-set(f,g) is non-empty since Q2 is unbounded by 2.5.1.

This enables us to define multiplication in $\mathcal{R}_0^+$ as:

If $f,g \in \mathcal{R}_0^+$ then
$$f \times g := \inf(\text{mult-set}(f,g)).$$

Again we have some direct results:

- If $f,g \in \mathcal{R}_0^+$ then $f \times g = g \times f$ since mult-set(f,g) = mult-set(g,f) .
- If $f,g \in \mathcal{R}_0^+$ then $\mathcal{O} \leq f \times g$ since an infimum of a set cannot be less than a lower bound of that set.

Theorem 2.8.1 : If $f,g \in \mathcal{R}_0^+$ and if $f1,g1 \in Q2^+$, $f < f1$ and $g < g1$ then we have

$$f \times g \leq M_{f1}(g1) .$$

Proof : Let $f,g \in \mathcal{R}_0^+$ and $f1,g1 \in Q2^+$.
Assume that $f < f1$ and $g < g1$. So $M_{f1}(g1) \in$ mult-set(f,g).
It follows immediately from the definition of multiplication that

$$f \times g \leq M_{f1}(g1) .$$

Since $Q2$ is dense in $\mathbb{R}$ we know the existence of a $g2 \in Q2$ with $g < g2 < g1$.

Let $g2$ be such an element.

Then we know that $M_{f1}(g2) \in$ mult-set(f,g).

On the other hand we have from 2.7.5, since $f1 \in Q2^+$, that

$$M_{f1}(g2) < M_{f1}(g1) .$$

So $M_{f1}(g1)$ cannot be the infimum of mult-set(f,g).

Hence we conclude: $f \times g < M_{f1}(g1)$.

□

Theorem 2.8.2 : If $f,g,h \in \mathbb{R}_0^+$ and $f \le g$ then we have $f \times h \le g \times h$.

Proof : Let $f,g,h \in \mathbb{R}_0^+$ and assume $f \le g$.

Let $g1$ and $h1 \in Q2^+$ and assume $g < g1$ and $h < h1$. Now we also have $f < g1$.

Hence $M_{g1}(h1) \in$ mult-set(f,h), so mult-set$(g,h) \subset$ mult-set(f,h).

This implies that $f \times h = \inf($mult-set$(f,h)) \le \inf($mult-set$(g,h)) = g \times h$ which proves the theorem.

□

Theorem 2.8.3 : Multiplication in $\mathbb{R}_0^+$ is distributive.

Proof : Let $f,g,h \in \mathbb{R}_0^+$. First we prove that $f \times h + g \times h < (f + g) \times h$ cannot hold and afterwards that $f \times h + g \times h \le (f + g) \times h$.

Suppose that $f \times h + g \times h < (f + g) \times h$.

Then 2.6.7 supplies $fh1, gh1 \in Q2^+$ with $f \times h < fh1$, $g \times h < gh1$ and $fh1 + gh1 < (f + g) \times h$.

Since $f \times h$ was defined as the infimum of mult-set(f,h), there exist $f1$ and $h1 \in Q2^+$ with $f < f1$, $h < h1$, and $M_{f1}(h1) < fh1$.

Let $f1$ and $h1 \in Q2^+$ be such that

$$f < f1,\ h < h1 \text{ and } M_{f1}(h1) < fh1 . \qquad (*)$$

In the same way we assume $g1$ and $h2 \in Q2^+$ to be such that

$$g < g1,\ h < h2 \text{ and } M_{g1}(h2) < gh1 . \qquad (**)$$

We define h0 to be the minimum of h1 and h2, so from (*) and (**) we derive with 2.7.5:

$$h < h0,\ M_{f1}(h0) < fh1 \text{ and } M_{g1}(h0) < gh1 .$$

Since multiplication in Q2 is distributive we also have from this

$$M_{f1+g1}(h0) < fh1 + gh1 < (f + g) \times h .$$

So we have found an element in mult-set(f + g,h) (that is $M_{f1+g1}(h0)$, since f + g < f1 + g1 and h < h0), which is less than the infimum of that set. This is a contradiction so we must conclude that

$$(f + g) \times h \leq f \times h + g \times h . \tag{1}$$

Let on the other hand fg and h1 $\in Q2^+$ be such that f + g < fg and h < h1.
Application of 2.6.7 once more supplies f1 and g1 $\in Q2^+$ with

$$f < f1,\ g < g1 \text{ and } f1 + g1 < fg .$$

But then we have by the commutativity, distributivity and monotonicity of multiplication in Q2 that

$$f \times h + g \times h \leq M_{f1}(h1) + M_{g1}(h1) = M_{f1+g1}(h1) < M_{fg}(h1)$$

So f × h + g × h is a lower bound of mult-set(f+g,h). Hence we derive
$f \times h + g \times h \leq (f + g) \times h$. (2)

Combination of (1) and (2) yields the desired result.

□

Theorem 2.8.4 : Multiplication in R_0^+ is associative.

Proof : Let f,g,h $\in R_0^+$. Let f1 and gh $\in Q2^+$ be such that f < f1 and g × h < gh. Since g × h is the infimum of mult-set(g,h), there exist g1 and h1 $\in Q2^+$ with

$$g < g1,\ h < h1 \text{ and } M_{g1}(h1) < gh . \tag{*}$$

Let g1 and h1 be such elements in $Q2^+$. Since $f < f1$ and $g < g1$, we know that $M_{f1}(g1) \in$ mult-set(f,g), so $f \times g < M_{f1}(g1)$ by [illegible].1. Moreover $h < h1$ so (note that $0 \leq f \times g$)

$$M_{M_{f1}(g1)}(h1) \in \text{mult-set}(f \times g, h) .$$

Hence $(f \times g) \times h \leq M_{M_{f1}(g1)}(h1)$.

Since multiplication in $Q2^+$ is associative we get

$$(f \times g) \times h \leq M_{f1}(M_{g1}(h1)) .$$

Now it is an easy consequence of (*) and 2.7.5 that

$$(f \times g) \times h < M_{f1}(gh) .$$

This implies that $(f \times g) \times h$ is a lower bound of mult-set$(f, g \times h)$. Hence we find $(f \times g) \times h \leq f \times (g \times h)$. When we interchange the rôles of f and h we see that $(h \times g) \times f \leq h \times (g \times f)$. So $f \times (g \times h) = (h \times g) \times f \leq h \times (g \times f) = (f \times g) \times h$. Hence $(f \times g) \times h = f \times (g \times h)$.

□

Theorem 2.8.5 : $\mathit{1}$ is the unit element of multiplication in R_0^+.

Proof : Let $f \in R_0^+$. Let $f1, g1 \in Q2^+$ be such that $f < f1$ and $\mathit{1} < g1$. In consequence of 2.7.5 we see that $f < M_{f1}(g1)$ since $M_{f1}(\mathit{1}) = f1$. So f is a lower bound of mult-set$(f,\mathit{1})$, whence

$$f \leq f \times \mathit{1} . \qquad (*)$$

Now assume that $g \in R_0^+$ and that $f < g$. Since Q2 is dense in R there exist f1 and $f2 \in Q2^+$ with $f < f1 < f2 < g$. Let f1 and f2 be such elements in $Q2^+$. We define $\delta := f2 - f1 \in Q2^+$. From 2.7.6 we know the existence of $\varepsilon \in Q2^+$ with $M_{f1}(\varepsilon) \leq \delta$. Let $\varepsilon \in Q2^+$ have this property. Then we know $\mathit{1} < \mathit{1} + \varepsilon$, so $M_{f1}(\mathit{1} + \varepsilon) \in$ mult-set$(f,\mathit{1})$. On the other hand we have:

$$M_{f1}(\mathit{1} + \varepsilon) = M_{f1}(\mathit{1}) + M_{f1}(\varepsilon) \leq f1 + \delta = f2 < g .$$

So $g \in R_0^+$ with $f < g$ cannot be the infimum of mult-set$(f,\mathit{1})$. Hence

$$f \times \mathit{1} \leq f . \qquad (**)$$

Combination of (*) and (**) proves the theorem.

□

Theorem 2.8.6 : If $f \in R_0^{+}$ we have

$$\forall_{\varepsilon \in R^{+}} \exists_{g \in R^{+}} [f \times g < \varepsilon] .$$

Proof : Let $f \in R_0^{+}$ and $\varepsilon \in R^{+}$. So $0 < \varepsilon$. Since Q2 is dense in R there exists a $\delta \in Q2$ with $0 < \delta < \varepsilon$.

Let δ be such an element of Q2. So $\delta \in Q2^{+}$.

Let $f1 \in Q2^{+}$ and assume $f < f1$. (The existence of such an f1 has been shown in 2.5.1).

From 2.7.6, the continuity of multiplication in Q2, we get an $\varepsilon f \in Q2^{+}$ with $M_{f1}(\varepsilon f) < \delta$.

Since $0 < \text{half}(\varepsilon f) < \varepsilon f$ we see that $M_{f1}(\varepsilon f) \in$ mult-set(f,half(εf)).

So $f \times \text{half}(\varepsilon f) \leq M_{f1}(\varepsilon f) \leq \delta < \varepsilon$.

Moreover we have that $\text{half}(\varepsilon f) \in R^{+}$. Hence there exists some $g \in R^{+}$ with $f \times g < \varepsilon$.

□

In order to show that multiplication in R^{+} has an inverse operation we define for $f \in R^{+}$ a so-called inverse set:

If $f \in R^{+}$ then

inv-set $:= \{g \in R^{+} \mid 1 < g \times f\}$.

Some immediate consequences are:

- If $f \in R^{+}$ then inv-set(f) is a subset of R^{+}.
- If $f \in R^{+}$ then inv-set(f) is bounded below.

Theorem 2.8.7 : If $f \in R^{+}$ then inv-set(f) is non-empty.

Proof : Let $f \in R^{+}$. Suppose that inv-set(f) is empty. We define $A_{\varepsilon} := \{g \in R^{+} \mid \varepsilon < g \times f\}$ and shall prove that A_{ε} is empty for $\varepsilon \in Q2^{+}$ by induction. For $\varepsilon = 1$ this holds. Let $\varepsilon \in Q2^{+}$ and assume that A_{ε} is empty. Let $g \in R^{+}$ and suppose that $\varepsilon + 1 < g \times f$. Then $\varepsilon < \varepsilon + 1 \leq g \times f$ and that would imply that A_{ε} is not empty. Hence no such g exists and $A_{\varepsilon+1}$ is empty. Let $g \in R^{+}$ and suppose that $\text{half}(\varepsilon) < g \times f$. From 2.6.6 we know that $\text{half}(\varepsilon) + \text{half}(\varepsilon) = \varepsilon$.

So $\varepsilon < g \times f + g \times f = (g + g) \times f$. And this again is impossible since A_ε is empty. So $A_{half(\varepsilon)}$ is empty. By induction we conclude that A_ε is empty for $\varepsilon \in Q2^+$. In particular $1 \notin A_\varepsilon$, whence $f \leq \varepsilon$ for $\varepsilon \in Q2^+$. This contradicts the existence of $\varepsilon \in Q2^+$ with $0 < \varepsilon < f$. It follows that inv-set(f) is non-empty

□

So now we know that the infimum of the inverse set exists.

Theorem 2.8.8 : If $f \in R^+$ then there exists some $g \in R^+$ with $g \times f = 1$.

Proof : Let $f \in R^+$ and let us put $g := \inf \{\text{inv-set}(f)\}$.

We prove that $g \times f = 1$.

It will be clear that $g \in R_0^+$. Let $f1$ and $g1 \in Q2^+$ be such that $f < f1$ and $g < g1$. From the properties of the infimum we have the existence of a $g2 \in$ inv-set(f) with $g2 < g1$. Let $g2$ be such an element of inv-set(f). Hence we have

$$1 < g2 \times f \ .$$

We also know that $M_{g1}(f1) \in$ mult-set(g2,f) since $f1, g1 \in Q2^+$, $f < f1$ and $g2 < g1$, whence we derive

$$g2 \times f \leq M_{g1}(f1) \ .$$

So $1 < M_{g1}(f1)$, which implies that 1 is a lower bound of mult-set(g,f). Hence we have

$$1 \leq g \times f \ .$$

Now suppose that $1 < g \times f$. We put $\delta := g \times f - 1$. Then we know $\delta \in R^+$. Now 2.8.6 shows the existence of an $h \in R^+$ with $f \times h < \delta$. In consequence of 2.8.2 we may assume such an h to satisfy $h < g$. Let h be such an element of R^+. Then we know $1 + f \times h < 1 + \delta = g \times f$. And since $h < g$ so $g - h \in R_0^+$ we get

$$1 < g \times f - h \times f = (g - h) \times f.$$

So $g - h \in$ inv-set(f) and $g - h < g$ where g was supposed to be the infimum of inv-set(f). This is a contradiction, hence $g \times f = 1$.

□

2.9. Multiplication in $\mathcal{R}$.

At last we define multiplication in $\mathcal{R}$ and prove all necessary properties to show that $\mathcal{R}$ with this multiplication, order and addition is an ordered field.

For $f,g \in \mathcal{R}$ we define:

$$
\begin{aligned}
f \star g := \underline{\text{if}}\ 0 \leqslant f\ \underline{\text{then}}\ \underline{\text{if}}\ 0 \leqslant g\ &\underline{\text{then}}\ f \times g \\
&\underline{\text{else}}\ 0 - f \times (0 - g) \\
\underline{\text{else}}\ \underline{\text{if}}\ 0 \leq g\ &\underline{\text{then}}\ 0 - (0 - f) \times g \\
&\underline{\text{else}}\ (0 - f) \times (0 - g)\ .
\end{aligned}
$$

It is obvious, that in this definition the arguments of the multiplication in $\mathcal{R}_0^+$ are always elements of $\mathcal{R}_0^+$. Furthermore we see immediately, for $f,g \in \mathcal{R}$, that $f \star g \in \mathcal{R}$, that $0 \leq f \star g$, if $0 \leq f$ and $0 \leq g$, and that $f \star g = 0$, if $f = 0$ or $g = 0$.

<u>Theorem 2.9.1</u> : If $f,g \in \mathcal{R}$ then $f \star g = g \star f$.

<u>Proof</u> : Let $f,g \in \mathcal{R}$.

- If $f,g \in \mathcal{R}_0^+$ this commutativity follows immediately from the definition of $\star$ and the commutativity of $\times$.
- If $0 \leq f$ and $g < 0$ then
  $f \star g = 0 - f \times (0 - g) = 0 - (0 - g) \times f = g \star f$.
- If $f < 0$ and $0 \leq g$ then
  $f \star g = 0 - (0 - f) \times g = 0 - g \times (0 - f) = g \star f$.
- If $f < 0$ and $g < 0$ then
  $f \star g = (0 - f) \times (0 - g) = (0 - g) \times (0 - f) = g \star f$.

□

<u>Theorem 2.9.2</u> : If $f,g \in \mathcal{R}$ then $f \star g = 0 - f \star (0 - g)$.

<u>Proof</u> : Let $f,g \in \mathcal{R}$. The case $g = 0$ is obvious.

- Assume $0 \leq f$ and $0 < g$. Then $0 - g < 0$.
  So $f \star (0 - g) = 0 - f \times (0 - (0 - g)) = 0 - f \times (g + 0) = 0 - f \times g$.
  Hence $f \star g = f \times g = 0 - f \star (0 - g)$.

- Assume $0 \leq f$ and $g < 0$.
  Then $f \star g = 0 - f \times (0 - g) = 0 - f \star (0 - g)$ after the definition of $\star$, since $0 \leq 0 - g$.
- Assume $f < 0$ and $0 < g$.
  Now $f \star (0 - g) = (0 - f) \times (0 - (0 - g)) = (0 - f) \times g = 0 - f \star g$.
- Assume $f < 0$ and $g < 0$.
  Then $f \star g = (0 - f) \times (0 - g) = 0 - f \star (0 - g)$.

[]

Theorem 2.9.3 : Multiplication in R is associative.

Proof : Let $f,g,h \in R$. We shall prove $f \star (g \star h) = (f \star g) \star h$.

(i) If $0 \leq f$, $0 \leq g$ and $0 \leq h$ then we know $0 \leq f \star g$ and $0 \leq g \star h$, so
$f \star (g \star h) = f \times (g \star h) = f \times (g \times h) = (f \times g) \times h =$
$(f \star g) \times h = (f \star g) \star h$.
All other cases now reduce to this one by means of 2.9.1 and 2.9.2.

(ii) If $0 \leq f$, $0 \leq g$ and $h < 0$ we get
$f \star (g \star h) = 0 - f \star (0 - g \star h) = 0 - f \star (0 - (0 -$
$g \star (0 - h))) = 0 - f \star (g \star (0 - h))$.
By application of (i) we have:
$f \star (g \star h) = 0 - (f \star g) \star (0 - h) = (f \star g) \star h$.

(iii) If $0 \leq f$, $g < 0$ and $0 \leq h$ we get $f \star (g \star h) = f \star (h \star g)$.
By application of (ii) we have
$f \star (g \star h) = (f \star h) \star g = (h \star f) \star g$.
Now we use (ii) from the right to the left and get
$f \star (g \star h) = h \star (f \star g) = (f \star g) \star h$.

The rest of the cases can now be proved in a similar pure algebraic way without using multiplication in R_0^+.

[]

Theorem 2.9.4 : 1 is the unit element of the multiplication in R.

Proof : Let $f \in R$. We know that $0 \leq 1$.

- If $0 \leq f$ then $1 \star f = 1 \times f = f$ by 2.8.5.
- If $f < 0$ then $1 \star f =$ (2.9.2) $0 - 1 \star (0 - f)$ and this reduces to the previous case, since $0 \leq 0 - f$. Hence
  $1 \star f = 0 - (0 - f) = f$.

[]

Theorem 2.9.5 : If $f \in \mathcal{R}$ $f \neq 0$ then there exists some $g \in \mathcal{R}$ with $g * f = 1$.

Proof : Let $f \in \mathcal{R}$, $f \neq 0$.

- If $0 < f$ there exists some $g \in \mathcal{R}^+$ with $g \times f = 1$ in consequence of 2.8.8.
  For such a g also holds $g * f = g \times f = 1$.
- If $f < 0$ we know that $0 < 0 - f$. So there exists some $g \in \mathcal{R}^+$ with $g * (0 - f) = 1$.
  In consequence of 2.9.2 and 2.9.1 we get for such a g
  $$(0 - g) * f = 0 - (0 - g) * (0 - f) = 0 - (0 - f) * (0 - g)$$
  $$= (0 - f) * g = g * (0 - f) = 1.$$

□

Theorem 2.9.6 : Multiplication in $\mathcal{R}$ is distributive.

Proof : Let $f,g,h \in \mathcal{R}$. We shall prove $(f + g) * h = f * h + g * h$.

(i) If $0 \leq f$, $0 \leq g$, $0 \leq h$ we find, since $0 \leq f + g$,
$(f + g) * h = (f + g) \times h = f \times h + g \times h = f * h + g * h$
as a result of the distributivity of $\times$ in $\mathcal{R}_0^+$.

(ii) If $0 \leq f$, $0 \leq g$, $h < 0$ we use 2.9.2 and 2.9.1 and we see
$(f + g) * h = 0 - (f + g) * (0 - h) =$ (i) $0 - f * (0 - h) -$
$g * (0 - h) = f * h - g * (0 - h) = f * h + g * h.$

(iii) If $0 \leq f$, $g < 0$, $0 \leq h$ we distinguish two cases

a) $0 \leq f + g$:
Then we have
$f * h = (f + g + (0 - g)) * h.$
Since $0 \leq f + g$ and $0 \leq 0 - g$ we can apply (i), so
$f * h = (f + g) * h + (0 - g) * h$
From 2.9.2 and 2.9.1 we know now that
$(0 - g) * h = 0 - g * h$, so
$f * h = (f + g) * h - g * h$, whence
$(f + g) * h = f * h + g * h.$

b) $(f + g) < 0$.
Then we have
$f * h = ((0 - g) + (f + g)) * h$
Now we use (iii a), since $0 \leq 0 - g$, $f + g < 0$ and
$0 \leq f = (0 - g) + (f + g).$

So

$f * h = (0 - g) * h + (f + g) * h.$

With 2.9.1 and 2.9.2 this leads again to

$f * h = (f + g) * h - g * h$, so $(f + g) * h = f * h + g * h.$

As in the proof of 2.9.3 all further cases reduce to cases that have been proved already.

□

II. THE TRANSLATION INTO AUT-QE.

This part II is devoted to the translation of the text in part I into AUT-QE. Several problems arising during translation will be discussed.

1. Paragraphs and names.

For the AUTOMATH languages we have a paragraph system for the user's convenience [12,19]. Here we use it in two different ways.

Paragraphs of the first kind are used to introduce a chapter structure as usual in mathematical books. Whenever we begin a new chapter we open a new paragraph. Hence every new chapter in part I corresponds with a new paragraph in the AUT-QE text. Paragraphs of this kind are never closed.

Paragraphs of the second kind contain the proofs which are necessary to derive the theorems immediately following those paragraphs. They play the role of lemmas which are used only once. These paragraphs will be closed immediately. This enables us to use, in two different paragraphs of this kind, the same names for proofs or objects. We use, e.g., names like th1, th2, over and over again.

Names of constants in paragraphs of the first kind intend to express the contents of the theorem that they prove, or else they are just the usual names for mathematical constants like 0, integer, or operations like +, −, inf. We give a few more examples: AND-I expresses the introduction of $\wedge$. With propositions a and b and proofs that a and b hold, it proves $a \wedge b$. Another example is LESS-SO-SUCC-LESS-SUCC, a theorem about the successor function on the integers, expressing that $k < \ell$ implies $(k+) < (\ell+)$.

2. Logic in AUT-QE.

Since hardly any logic is implemented in the definition of AUTOMATH the book has to start with a chapter on logic. The system of logic used in this AUT-QE text is classical, and its implementation is contained in the logic used in [12].

3. Coding binary strings.

In order to introduce the reals as binary strings we need a way to represent those strings in AUT-QE. Since functions are primitive objects in AUTOMATH there seems to be no problem to define those strings as functions from Z to $\{0,1\}$. As we see from the definition of subtraction in 2.1 of part I, this forces us to provide the integers with subtraction and addition, at least between -3 and 3, or to prove a theorem like 2.1 11 by splitting into cases. This splitting has been carried out by Wieringa [17] and led to very long texts.

In this translation we have preferred to represent those strings by functions from Z to $\{id, sr\}$, where id is the identical function from Z to Z and sr the successor function on Z. Now id should be interpreted as 0 and sr as 1. Adding 1 can be interpreted as composition with sr. Since we cannot express subtraction in this way, we still need another function, viz. $s\ell$, the predecessor function. (sr and $s\ell$ are abbreviations for shift to the right and shift to the left, respectively). If we also have a map "dual", which maps sr to $s\ell$, $s\ell$ to sr and id to id then we can translate the definition of subtraction in part I as:

$$f - g := \curlyvee_{k \in Z} f(k) \circ \mathrm{dual}(g(k)) \circ \mathrm{dual}(p(k)) \circ (p(k-) \circ p(k-),$$

where $\circ$ means the composition of two functions from Z to Z defined in AUTOMATH as:

$$[f : Z \to Z][g : Z \to Z]$$

$$f \circ g := [k : Z] << k > g > f .$$

The advantages of this approach are:

- We do not need to define addition and subtraction in Z.
- When we develop a theory for those three functions it is immediately applicable to prove properties about "half" and "twice" as defined in 2.6 of part I.
- The most useful property, however, is that we need not bother about parentheses when composing functions.
  If $f,g,h : Z \to Z$ then

$$f \circ (g \circ h) \overset{D}{=} (f \circ g) \circ h,$$

where $\overset{D}{=}$ denotes the definitional equality of expressions in AUTOMATH [8].

We devote some attention to this definitional equality. Under the equality sign we indicate by what kind of reduction the equality is derived:

If f,g,h are functions from Z to Z then

$$f \circ (g \circ h) =_{\delta} [k : Z] << k > g \circ h > f =_{\delta}$$

$$[k : Z] << k > [\ell : Z] << \ell > h > g > f =_{\beta}$$

$$[k : Z] <<< k > h > g > f$$

and the same thing holds for $(f \circ g) \circ h$. These operations are carried out by the verifying machine and that reduces the amount of writing considerably.

Another consequence is that $f \circ id$ and $id \circ f$ are definitionally equal to f for $f : Z \to Z$.
This is also quite obvious. If we note that the definition of id is :
$id := [k : Z]k$ then we derive for $f : Z \to Z$:

$$f \circ id =_{\delta} [k : Z] << k > id > f =_{\delta} [k : Z] << k > [\ell : Z]\, \ell > f =_{\beta}$$

$$[k : Z] < k > f =_{\eta} f$$

and similarly for $id \circ f$.

We see here the necessity of η-reduction, which we had to use 54 times during verification. As a contrast, we mention that Jutting's Landau translation used it only twice and even there it could have been avoided.

4. <u>The type $\mathcal{R}$-extra.</u>

In part I we considered reals as maps from Z to $\{0,1\}$ with certain properties, and we called the set of those maps $\mathcal{R}$. When defining a new object, like the subtraction, we first gave its definition and proved afterwards that it had all required properties in order to be called real.

This procedure is quite natural. As van Daalen says [9], it is how we first met objects and their types in our early youth: first there were the table and the chair, and afterwards we learned that they belonged to our furniture. In AUTOMATH it is the other way round. Types must be introduced before the objects. Therefore we introduce R-extra, the type of all functions from Z to Z^Z (Note that id and sr have type Z^Z). We say that an element of $\mathcal{R}$-extra is real if (i) it is a string of id and sr, (ii) it is signed and (iii) it has the unique representation property.

Now it will be clear that most operations and functions acting on $\mathcal{R}$ are partial functions on R-extra i.e. they do not only depend on their usual arguments but also on the proofs that those arguments are [illegible] An example is the multiplication in $\mathcal{R}$.

5. Irrelevance of proofs.

As already mentioned in 4., names of proofs appear not only in proofs as references to what we proved before, but also in objects. In AUTOMATH objects and proofs are treated in the same way. In standard mathematics, however, references to proofs appear in the metalanguage only. It is impossible to discern in the language between different proofs of the same proposition.

We can simulate this in AUTOMATH by an axiom that there is book equality between two objects depending on two different arguments proving the same proposition (i.e. having the same type). Another possibility is to include this irrelevance of proofs in the language definition, taking the equality as definitional equality.

In our translation we have chosen for proving the irrelevance of proofs seperately at every place where it was needed. This was the case for the multiplication in Q2, $\mathcal{R}_0^+$ and $\mathcal{R}$, and for the infimum. The other operations like + and - could fortunately be defined on R-extra.

6. Sets in AUT-QE.

Sets in standard mathematics have a notation slighty different from the one in AUT-QE. In everyday mathematics we usually denote sets like the multiplication set in 2.8 of part I, given $f,g \in \mathcal{R}_0^+$, as:

$$\{M_{f1}(g1) \mid f1,g1 \in Q2^+,\ f < f1,\ g < g1\} .$$

When we want to take an arbitrary element from this set we usually think we only have to pick arbitrary elements f1,g1. This implies, however, the knowledge about the shape of certain names of the elements in this set, here $M_{f1}(g1)$. In formal systems like AUTOMATH we cannot talk about shapes of names, and the only way to implement what we mean, seems to be via book equality. The above set can be introduced like this:

$$\{h \in \mathcal{R} \mid \exists_{f1 \in Q2^+}\left[f < f1 \wedge \exists_{g1 \in Q2^+}[g < g1 \wedge h = M_{f1}(g1)]\right]\} .$$

This forces us, when taking an arbitrary element from this set, to introduce h in the first place and f1 and g1 afterwards. Tedious but inevitable.

6. Variables.

For the reader's convenience we tried to normalize the names of variables. That means that we used for integers the names k, ℓ, m, for functions from $\mathbb{Z} \to \mathbb{Z}$ the names f, g, h and for functions from $\mathbb{Z}$ to $\mathbb{Z}^{\mathbb{Z}}$ always ff, gg, hh.

7. Degree of precision.

In standard mathematical texts one usually starts with a high degree of precision in order to make the reader familiar with the subject. Little by little this fades away, as in 2.2 in part I where we said: "From now on ...". This is to keep the reader interested and aware of the mathematical structure. There is no need to tell time after time, given two propositions a and b and a proof of $a \wedge b$, that a holds. In the AUT-QE text, however, we did it 223 times ! Fortunately computers never get bored (they only break down sometimes).

8. Relation between part I and the AUT-QE text.

Sometimes a reader might think to be able to shorten a proof in part I. The reason for the longer proof is that this text is closely related to the AUT-QE text in which those shortenings are not always improvements. As an example we refer to the end of the proof of theorem 2.1.11 in part I, where we derive $w(\ell) = 1$ for $\ell \in \mathbb{Z}, (k+) \leq \ell$. Since w is the difference of two reals and therefore real itself, we have a contradiction already, and there seems no need to prove this contradiction by means of t2. In the AUT-QE text w is defined just slightly differently (because of the representation of reals in terms of id en sr), and it is easier to prove the contradiction by means of t2 than to prove that w is real.

Another matter is that we have to apologize for something, that is superfluous even in the AUT-QE text. We defined the multiplication in R_0^+ by means of $Q2^+$ and we did not really use the existence of Q2. Hence the definition of Q2 is unnecessary and theorems about Q2 can be replaced by theorems about $Q2^+$. The reason for introducing Q2 was that the original idea was to define the multiplication in R at once from Q2 by means of fundamental sequences, as was suggested in [6]. After a while, at a moment where Q2 and the multiplication in Q2 had been introduced in the AUT-QE text already, this seemed to lead to a lot of work. Actually it turned out that our intuitive ideas about strings are very difficult to capture in a formal system like AUTOMATH without a lot of writing. At that moment we changed our mind, and chose for the method as described in part I. A large number of lines depended on Q2 already (the multiplication in Q2 for example). It would have been a waste of time to replace Q2 by $Q2^+$ at that moment.

9. The amount of work involved in the translation.

The time needed to translate the mathematical text of part I into AUT-QE amounted to about 1050 hours. This was purely for translation and not for developing the mathematics (this mathematics included the problem of avoiding addition and subtraction in Z). The number of lines finally produced in the AUT-QE text amounts to 6312.

III. EXPERIENCES.

In this part we relate some experiences with the actual verification as well as with the whole process of translating such a voluminous part of mathematics into such a precise language.

1. Verification.

The verification of the AUT-QE text was executed on the Burroughs 7700 computer of the Technological University of Eindhoven. The whole book was checked in a final run on Jan. 10, 1980.

1.1. A shortcoming in the strategy of the verification program.

Although the verification program was quite able to check the AUT-QE text, it was sometimes necessary to control the verification in on-line runs, since the program did not always follow an adequate strategy.

In order to establish definitional equality between two expressions the verification system sometimes has to make a choice how to proceed. Suppose, for example, that definitional equality has to be established between f(a,b) and f(c,d). The program has to choose between reduction and decomposition. Reduction means in this case reducing one of the two expressions by application of the definition of f and then trying to establish definitional equality to the other one. Decomposition means trying to establish $a \stackrel{D}{=} c$ and $b \stackrel{D}{=} d$. Experience learns that almost always decomposition is preferable. Hence the program will first try decomposition in such a case and, if this fails, reduction afterwards.

In some cases, however, this is very poor: Sometimes reduction is the only way to establish definitional equality, whereas decomposition leads to an immense amount of work, until finally the verification system returns to this so-called decision point to take the right decision i.e. to choose for reduction.

With our style of writing, those cases often occurred. As an example, we quote from part II the definitional equality of id $\circ$ (sℓ $\circ$ sr) and sℓ $\circ$ (id $\circ$ sr). Choosing for decomposition the program tries to establish definitional equality between id en sℓ. Since sℓ has a rather complicated definition it takes a lot of work before the program returns to this point, reduces and takes the wrong decision again. In some cases it turned out to be impossible to verify one single line without human intervention (in off-line runs the program stops after three minutes verification time for one line).

In on-line runs, however, the program will ask for help if intermediate results are obtained which strongly suggest a negative answer to the question of definitional equality. When the program tries, as in the example above, to establish id $\overset{D}{=}$ sℓ, it gets this idea, since the names id and sℓ are not equal. Although it still could be that id and sℓ reduce to the same expression, the program will ask at this point how to proceed. Now the user can lead the program to the decision point where it took the wrong decision, and restart the verification from there. The loss for the computer is now only a matter of seconds, but the human user wastes quite some time !

1.2. A possible solution.

A possible solution to the problem as sketched above is to enable the user to forbid decomposition on certain defined constants, as $\circ$ above. This is, however, unattractive since even for $\circ$ decomposition is almost always faster than reduction. Only with sℓ, id and sr these problems occur in our text. A better solution seems to be to enable the user to forbid δ-reduction on certain constants in certain lines. In the case of sℓ, id and sr we could, after having proved all necessary properties, forbid δ-reduction on these functions. The program would still take the wrong decision in the example above, but it would discover very fast that it was the wrong one indeed, and return in order to take the right one.

1.3. Some statistics.

The verification of the whole book took 4 hours (real time). Of this time 42 minutes were spent on verification (so not including the time needed for coding). In a table we list a number of data of the last run concerning verification time, number of performed reductions and the number of decision points.

	logic	integers	chapter 2.1	chapter 2.2	chapter 2.3	chapter 2.4	chapter 2.5	chapter 2.6	chapter 2.7	chapter 2.8	chapter 2.9	complete text
verification time	71.0	622.0	524.9	23.6	74.1	212.9	48.9	188.6	174.0	283.6	303.6	2527.2
β-reduction	335	5636	4708	-	635	939	227	739	1461	672	[illegible]	15435
δ-reduction	542	26680	22065	143	3226	2250	574	2213	2283	1245	896	[illegible]
η-reduction	-	37	17	-	-	-	-	-	-	-	-	51
nr. of lines	397	731	889	54	94	638	155	628	443	876	407	[illegible]
nr. of decisions	2685	47416	52841	2038	5647	17716	4130	17002	15689	22447	33542	221143

In comparison with the translation of Landau's "Grundlagen" by Jutting [12], after all an introduction of the reals too, we see that the present introduction is about twice as fast as Landau's.

2. The language AUT-QE.

As in previous experiences the language AUT-QE turned out to be adequate for writing mathematics. At various points, however, improvements might be desirable and possible.

2.1. Parentheses.

A lot of mistakes were made with writing parentheses in the AUT-QE text. On the one hand they are necessary for the parameter list of a constant, on the other we need them in arithmetic expressions like $a + (b + c)$ or $a \wedge (b \wedge c)$. In particular for expressions where those parentheses are redundant it is a pity to have to use them. As an example, we quote the expression $f \circ (g \circ h)$, which is definitionally equal to $(f \circ g) \circ h$ as we have seen in part II.

A way to economize on parentheses could be to agree that expressions with fix symbols are read from the left to the right. For example, $a + b \times c$ should be interpreted as $(a + b) \times c$. Another solution, nicer but more difficult to implement, is to enable an author of AUTOMATH texts to give some fix symbols a higher priority than others. This is everyday practice in standard mathematics, cf. the priority rule "multiplication before addition".

2.2. AUT-QE-SYNT.

A very annoying feature of AUT-QE is, that it is often necessary to write down expressions that might have been computed by the verification program itself. For example AND-I (and introduction) depends, as shown in part II, on four parameters: propositions a and b and proofs p and q that a and b hold. One might say, when applying AND-I, that the propositions a and b can be calculated (up to definitional equality) from p and q (the categories of p and q will do). This seems only a small improvement, but in practice there a and b are often long and complicated expressions whereas p and q are short and simple.

AUT-QE-SYNT |12| is an extension of AUT-QE in which it is possible to suppress those redundant parameters. This language contains some pre-defined constants like CAT to compute the category of an expression or DOM to compute the domain of a function. Moreover this language contains a basic symbol 'synt'. Variables of type 'synt' are to be interpreted as syntactic variables for expressions.

We give an example. After having defined AND-I in AUT-QE the and introduction can be defined as follows in AUT-QE-SYNT:

|p1 : 'synt'| |q1 : 'synt'|

AND-I := AND-I(CAT(p1), CAT(q1),p1,q1) .

Now if a and b are propositions and p and q proofs of a and b then

$$\mathit{AND\text{-}I}\ (p,q) \overset{D}{=} \text{AND-I}(\text{CAT}(p), \text{CAT}(q), p, q) \overset{D}{=} \text{AND-I}(a,b,p,q)$$

which is the proof of $a \wedge b$.

It would be a great improvement if this language could be checked as well. Then a lot of dull mechanical work would be taken over by the computer.

3. Conclusions.

AUTOMATH is able to represent standard mathematics. At the moment, however, it is a dull and tedious experience. AUT-QE-SYNT is a great improvement but still there is a lot more to write than in standard mathematics. In the present stage it is certainly not for the mathematician who wants to check the theory he wrote. It is still to far from our everyday mathematical habits.

The question is what to improve first : AUTOMATH or our usual way to say things in mathematics. Probably our standard mathematical language needs more formalism at this moment. A significant step in this direction seems the development by de Bruijn |7| of WOT (Wiskundige Omgangstaal, which is Dutch for "mathematical vernacular"). This is some kind of intermediate language. On the one hand it is closely related to what we usually do in mathematics and it does not really increase the amount of writing. On the other hand it is formalized in such a way that translation into an AUTOMATH language is obvious.

REFERENCES.

[1] *S.T.M. Ackermans and J.H. van Lint,*
Algebra en Analyse, Wolters-Noordhof N.V., Groningen, 1970.

[2] *N.G. de Bruijn,*
The mathematical language AUTOMATH, its usage and some of its extensions. Symposium on Automatic Demonstration, IRIA, Versailles, Dec. 1968. (Lecture Notes in Mathematics, Vol. 125, Springer-Verlag, pp. 29-61, 1970).

[3] *N.G. de Bruijn,*
AUTOMATH, a language for mathematics. A series of lectures by N.G. de Bruijn, at the Séminaire de mathématiques supérieurs, Université de Montréal, June 1971. Les Presses de l'Université de Montréal, 1973. Lecture Notes prepared by B. Fawcett.

[4] *N.G. de Bruijn,*
The AUTOMATH Mathematics Checking Project. Proceedings of the Symposium APLASM. Vol. I, ed. P. Braffort, Orsay, France (Dec. 1973).

[5] *N.G. de Bruijn,*
A framework for the description of a number of members of the AUTOMATH family. (Internal Report, Department of Mathematics, T.H. Eindhoven, June 1974).

[6] *N.G. de Bruijn,*
Defining reals without the use of rationals, Proceedings of the Koninklijke Akademie van Wetenschappen, 79, 100-108, 1976.

[7] *N.G. de Bruijn,*
Wees context bewust in WOT. Euclides, 55, 7-12, 1979.

[8] *D.T. van Daalen,*
A description of AUTOMATH and some aspects of its language theory. Proceedings of the Symposium APLASM. Vol. I, ed. P. Braffort, Orsay, France (Dec. 1973).

[9] *D.T. van Daalen,*
The language theory of AUTOMATH. Thesis, Eindhoven University of Technology, 1980.

[10] *S. Feferman,*
The number sytem; foundation of algebra and analysis. Addison-Wesley, 1964 (Addison-Wesley series of Mathematics).

[11] *L.S. Jutting,*
The development of a text in AUT-QE. Proceedings of the Symposium APLASM. Vol. I, ed. P. Braffort, Orsay, France (Dec. 1973).

[12] *L.S. Jutting,*
Checking Landau's "Grundlagen" in the AUTOMATH system. Thesis, Eindhoven University of Technology, 1977.

[13] *K. Knopp,*
Theorie und Anwendung der unendlichen Reihen. Berlin, 1922 (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellung: Bd 2).

[14] *E. Landau,*
Grundlagen der Analysis. 3rd ed., Chelsea Publ. Comp., New York, 1960.

[15] *N. Metropolis and G.C. Rota,*
Significance Arithmatic, On the Algebra of Binary Strings.
In: Studies of Numerical Analysis, papers in honour of Cornelius Lanczos, ed. B.k.P Scaife, Published for the Royal Irish Academy by Academic Press, London-New York, 241-251 (1974).

[16] *N. Metropolis, G.C. Rota and S. Tanny,*
Significance Arithmatic : I. The carrying algorithm. Journal Combinatorial Theory Ser. A, 14, 386-421 (1973).

[17] *R.H.A. Wieringa,*
Representatie van reële getallen als oneindige rijtjes symbolen 0 en 1. Unpublished manuscript, 1976.

[18] *I. Zandleven,*
A verifying program for AUTOMATH. Proceedings of the Symposium APLASM, Vol. I, ed. P. Braffort, Orsay, France (Dec. 1973).

[19] *I. Zandleven,*
The use of paragraphs in AUTOMATH. Memorandum 1977-5, Eindhoven University of Technology, Department of Mathematics, 1977.

[20] *J. Zucker,*
Formalization of classical mathematics in AUTOMATH. Actes of the International Logic Colloquium, Clermont-Ferrand, July 1975.