FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 75–81, 2013
DOI: 10.2478/forma-2013-0008

VERSITA
degruyter.com/view/j/forma

# $N$-Dimensional Binary Vector Spaces

Kenichi Arai[1]
Tokyo University of Science
Chiba, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

**Summary.** The binary set $\{0,1\}$ together with modulo-2 addition and multiplication is called a binary field, which is denoted by $\mathbb{F}_2$. The binary field $\mathbb{F}_2$ is defined in [1]. A vector space over $\mathbb{F}_2$ is called a binary vector space. The set of all binary vectors of length $n$ forms an $n$-dimensional vector space $V_n$ over $\mathbb{F}_2$. Binary fields and $n$-dimensional binary vector spaces play an important role in practical computer science, for example, coding theory [15] and cryptology. In cryptology, binary fields and $n$-dimensional binary vector spaces are very important in proving the security of cryptographic systems [13]. In this article we define the $n$-dimensional binary vector space $V_n$. Moreover, we formalize some facts about the $n$-dimensional binary vector space $V_n$.

MSC: 15A03 03B35

Keywords: formalization of binary vector space

MML identifier: `NBVECTSP`, version: `8.1.01 5.13.1174`

The notation and terminology used in this paper have been introduced in the following articles: [6], [1], [2], [16], [5], [7], [11], [17], [8], [9], [18], [24], [14], [4], [25], [26], [19], [23], [12], [20], [21], [22], [27], and [10].

In this paper $m$, $n$, $s$ denote non zero elements of $\mathbb{N}$.

Now we state the proposition:

(1) Let us consider elements $u_1, v_1, w_1$ of $Boolean^n$. Then $\text{Op-XOR}((\text{Op-XOR}(u_1, v_1)), w_1) = \text{Op-XOR}(u_1, (\text{Op-XOR}(v_1, w_1)))$.

Let $n$ be a non zero element of $\mathbb{N}$. The functor $\text{XOR}_{\text{B}}(n)$ yielding a binary operation on $Boolean^n$ is defined by

(Def. 1) Let us consider elements $x, y$ of $Boolean^n$. Then $it(x, y) = \text{Op-XOR}(x, y)$.

The functor $\text{Zero}_{\text{B}}(n)$ yielding an element of $Boolean^n$ is defined by the term

(Def. 2) $n \mapsto 0$.

[1]This research was presented during the 2013 International Conference on Foundations of Computer Science FCS'13 in Las Vegas, USA.

© 2013 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(Print), 1898-9934(Online)



Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

The functor $n$-binary additive group yielding a strict additive loop structure is defined by the term

(Def. 3) $\langle Boolean^n, \mathrm{XOR_B}(n), \mathrm{Zero_B}(n)\rangle$.

Let us consider an element $u_1$ of $Boolean^n$. Now we state the propositions:

(2) $\text{Op-XOR}(u_1, \mathrm{Zero_B}(n)) = u_1$.

(3) $\text{Op-XOR}(u_1, u_1) = \mathrm{Zero_B}(n)$.

Let $n$ be a non zero element of $\mathbb{N}$. Note that $n$-binary additive group is add-associative right zeroed right complementable Abelian and non empty and every element of $\mathbf{Z}_2$ is Boolean.

Let $u$, $v$ be elements of $\mathbf{Z}_2$. We identify $u \oplus v$ with $u + v$. We identify $u \wedge v$ with $u \cdot v$. Let $n$ be a non zero element of $\mathbb{N}$. The functor $\mathrm{MLT_B}(n)$ yielding a function from (the carrier of $\mathbf{Z}_2$) $\times$ $Boolean^n$ into $Boolean^n$ is defined by

(Def. 4) Let us consider an element $a$ of $Boolean$, an element $x$ of $Boolean^n$, and a set $i$. If $i \in \mathrm{Seg}\, n$, then $it(a, x)(i) = a \wedge x(i)$.

The functor $n$-binary vector space yielding a vector space over $\mathbf{Z}_2$ is defined by the term

(Def. 5) $\langle Boolean^n, \mathrm{XOR_B}(n), \mathrm{Zero_B}(n), \mathrm{MLT_B}(n)\rangle$.

Let us note that $n$-binary vector space is finite.

Let us note that every subspace of $n$-binary vector space is finite.

Now we state the propositions:

(4) Let us consider a natural number $n$. Then $\sum n \mapsto 0_{\mathbf{Z}_2} = 0_{\mathbf{Z}_2}$.

(5) Let us consider a finite sequence $x$ of elements of $\mathbf{Z}_2$, an element $v$ of $\mathbf{Z}_2$, and a natural number $j$. Suppose

(i) $\mathrm{len}\, x = m$, and

(ii) $j \in \mathrm{Seg}\, m$, and

(iii) for every natural number $i$ such that $i \in \mathrm{Seg}\, m$ holds if $i = j$, then $x(i) = v$ and if $i \neq j$, then $x(i) = 0_{\mathbf{Z}_2}$.

Then $\sum x = v$. The theorem is a consequence of (4). PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non zero element $m$ of $\mathbb{N}$ for every finite sequence $x$ of elements of $\mathbf{Z}_2$ for every element $v$ of $\mathbf{Z}_2$ for every natural number $j$ such that $\$_1 = m$ and $\mathrm{len}\, x = m$ and $j \in \mathrm{Seg}\, m$ and for every natural number $i$ such that $i \in \mathrm{Seg}\, m$ holds if $i = j$, then $x(i) = v$ and if $i \neq j$, then $x(i) = 0_{\mathbf{Z}_2}$ holds $\sum x = v$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [3, (11)], [5, (59), (5), (1)]. For every natural number $k$, $\mathcal{P}[k]$ from [3, Sch. 2]. $\square$

(6) Let us consider a (the carrier of $n$-binary vector space)-valued finite sequence $L$ and a natural number $j$. Suppose

(i) $\mathrm{len}\, L = m$, and

(ii) $m \leqslant n$, and

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(iii) $j \in \operatorname{Seg} n$.

Then there exists a finite sequence $x$ of elements of $\mathbf{Z}_2$ such that

(iv) $\operatorname{len} x = m$, and

(v) for every natural number $i$ such that $i \in \operatorname{Seg} m$ there exists an element $K$ of $Boolean^n$ such that $K = L(i)$ and $x(i) = K(j)$.

PROOF: Define $\mathcal{Q}$[natural number, set] $\equiv$ there exists an element $K$ of $Boolean^n$ such that $K = L(\$_1)$ and $\$_2 = K(j)$. For every natural number $i$ such that $i \in \operatorname{Seg} m$ there exists an element $y$ of *Boolean* such that $\mathcal{Q}[i, y]$. Consider $x$ being a finite sequence of elements of *Boolean* such that $\operatorname{dom} x = \operatorname{Seg} m$ and for every natural number $i$ such that $i \in \operatorname{Seg} m$ holds $\mathcal{Q}[i, x(i)]$ from [5, Sch. 5]. $\square$

(7) Let us consider a (the carrier of $n$-binary vector space)-valued finite sequence $L$, an element $S$ of $Boolean^n$, and a natural number $j$. Suppose

(i) $\operatorname{len} L = m$, and

(ii) $m \leqslant n$, and

(iii) $S = \sum L$, and

(iv) $j \in \operatorname{Seg} n$.

Then there exists a finite sequence $x$ of elements of $\mathbf{Z}_2$ such that

(v) $\operatorname{len} x = m$, and

(vi) $S(j) = \sum x$, and

(vii) for every natural number $i$ such that $i \in \operatorname{Seg} m$ there exists an element $K$ of $Boolean^n$ such that $K = L(i)$ and $x(i) = K(j)$.

The theorem is a consequence of (6). PROOF: Consider $x$ being a finite sequence of elements of $\mathbf{Z}_2$ such that $\operatorname{len} x = m$ and for every natural number $i$ such that $i \in \operatorname{Seg} m$ there exists an element $K$ of $Boolean^n$ such that $K = L(i)$ and $x(i) = K(j)$. Consider $f$ being a function from $\mathbb{N}$ into $n$-binary vector space such that $\sum L = f(\operatorname{len} L)$ and $f(0) = 0_{n\text{-binary vector space}}$ and for every natural number $j$ and for every element $v$ of $n$-binary vector space such that $j < \operatorname{len} L$ and $v = L(j+1)$ holds $f(j+1) = f(j) + v$. Define $\mathcal{Q}$[natural number, set] $\equiv$ there exists an element $K$ of $Boolean^n$ such that $K = f(\$_1)$ and $\$_2 = K(j)$. For every element $i$ of $\mathbb{N}$, there exists an element $y$ of the carrier of $\mathbf{Z}_2$ such that $\mathcal{Q}[i, y]$ by [1, (3)]. Consider $g$ being a function from $\mathbb{N}$ into $\mathbf{Z}_2$ such that for every element $i$ of $\mathbb{N}$, $\mathcal{Q}[i, g(i)]$ from [9, Sch. 3]. Set $S_j = S(j)$. $S_j = g(\operatorname{len} x)$. $g(0) = 0_{\mathbf{Z}_2}$ by [1, (5)]. For every natural number $k$ and for every element $v_2$ of $\mathbf{Z}_2$ such that $k < \operatorname{len} x$ and $v_2 = x(k+1)$ holds $g(k+1) = g(k) + v_2$ by [3, (11), (13)]. $\square$

(8) Suppose $m \leqslant n$. Then there exists a finite sequence $A$ of elements of $Boolean^n$ such that

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(i) $\operatorname{len} A = m$, and

(ii) $A$ is one-to-one, and

(iii) $\overline{\overline{\operatorname{rng} A}} = m$, and

(iv) for every natural numbers $i$, $j$ such that $i \in \operatorname{Seg} m$ and $j \in \operatorname{Seg} n$ holds if $i = j$, then $A(i)(j) = \mathit{true}$ and if $i \neq j$, then $A(i)(j) = \mathit{false}$.

PROOF: Define $\mathcal{P}[\text{natural number}, \text{function}] \equiv$ for every natural number $j$ such that $j \in \operatorname{Seg} n$ holds if $\$_1 = j$, then $\$_2(j) = \mathit{true}$ and if $\$_1 \neq j$, then $\$_2(j) = \mathit{false}$. For every natural number $k$ such that $k \in \operatorname{Seg} m$ there exists an element $x$ of $\mathit{Boolean}^n$ such that $\mathcal{P}[k, x]$. Consider $A$ being a finite sequence of elements of $\mathit{Boolean}^n$ such that $\operatorname{dom} A = \operatorname{Seg} m$ and for every natural number $k$ such that $k \in \operatorname{Seg} m$ holds $\mathcal{P}[k, A(k)]$ from [5, Sch. 5]. For every elements $x$, $y$ such that $x, y \in \operatorname{dom} A$ and $A(x) = A(y)$ holds $x = y$ by [5, (5)]. $\square$

(9) Let us consider a finite sequence $A$ of elements of $\mathit{Boolean}^n$, a finite subset $B$ of $n$-binary vector space, a linear combination $l$ of $B$, and an element $S$ of $\mathit{Boolean}^n$. Suppose

(i) $\operatorname{rng} A = B$, and

(ii) $m \leqslant n$, and

(iii) $\operatorname{len} A = m$, and

(iv) $S = \sum l$, and

(v) $A$ is one-to-one, and

(vi) for every natural numbers $i$, $j$ such that $i \in \operatorname{Seg} n$ and $j \in \operatorname{Seg} m$ holds if $i = j$, then $A(i)(j) = \mathit{true}$ and if $i \neq j$, then $A(i)(j) = \mathit{false}$.

Let us consider a natural number $j$. If $j \in \operatorname{Seg} m$, then $S(j) = l(A(j))$. The theorem is a consequence of (7) and (5). PROOF: Set $V = n$-binary vector space. Reconsider $F_1 = A$ as a finite sequence of elements of $V$. Consider $x$ being a finite sequence of elements of $\mathbf{Z}_2$ such that $\operatorname{len} x = m$ and $S(j) = \sum x$ and for every natural number $i$ such that $i \in \operatorname{Seg} m$ there exists an element $K$ of $\mathit{Boolean}^n$ such that $K = (l \cdot F_1)(i)$ and $x(i) = K(j)$. For every natural number $i$ such that $i \in \operatorname{Seg} m$ holds if $i = j$, then $x(i) = l(A(j))$ and if $i \neq j$, then $x(i) = 0_{\mathbf{Z}_2}$ by [5, (5)], [1, (3), (5)]. $\square$

(10) Let us consider a finite sequence $A$ of elements of $\mathit{Boolean}^n$ and a finite subset $B$ of $n$-binary vector space. Suppose

(i) $\operatorname{rng} A = B$, and

(ii) $m \leqslant n$, and

(iii) $\operatorname{len} A = m$, and

(iv) $A$ is one-to-one, and

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(v) for every natural numbers $i$, $j$ such that $i \in \operatorname{Seg} n$ and $j \in \operatorname{Seg} m$ holds if $i = j$, then $A(i)(j) = \mathit{true}$ and if $i \neq j$, then $A(i)(j) = \mathit{false}$.

Then $B$ is linearly independent. The theorem is a consequence of (9). PROOF: Set $V = n$-binary vector space. For every linear combination $l$ of $B$ such that $\sum l = 0_V$ holds the support of $l = \emptyset$ by [1, (5)]. $\square$

(11) Let us consider a finite sequence $A$ of elements of $\mathit{Boolean}^n$, a finite subset $B$ of $n$-binary vector space, and an element $v$ of $\mathit{Boolean}^n$. Suppose

(i) $\operatorname{rng} A = B$, and

(ii) $\operatorname{len} A = n$, and

(iii) $A$ is one-to-one.

Then there exists a linear combination $l$ of $B$ such that for every natural number $j$ such that $j \in \operatorname{Seg} n$ holds $v(j) = l(A(j))$. PROOF: Set $V = n$-binary vector space. Define $\mathcal{Q}[\text{element}, \text{element}] \equiv$ there exists a natural number $j$ such that $j \in \operatorname{Seg} n$ and $\$_1 = A(j)$ and $\$_2 = v(j)$. For every element $x$ such that $x \in B$ there exists an element $y$ such that $y \in$ the carrier of $\mathbf{Z}_2$ and $\mathcal{Q}[x, y]$ by [1, (3)]. Consider $l_1$ being a function from $B$ into the carrier of $\mathbf{Z}_2$ such that for every element $x$ such that $x \in B$ holds $\mathcal{Q}[x, l_1(x)]$ from [9, Sch. 1]. For every natural number $j$ such that $j \in \operatorname{Seg} n$ holds $l_1(A(j)) = v(j)$ by [8, (3)]. Set $f =$ (the carrier of $V) \longmapsto 0_{\mathbf{Z}_2}$. Set $l = f{+}{\cdot}l_1$. For every element $v$ of $V$ such that $v \notin B$ holds $l(v) = 0_{\mathbf{Z}_2}$ by [17, (7)]. For every element $x$ such that $x \in$ the support of $l$ holds $x \in B$. For every natural number $j$ such that $j \in \operatorname{Seg} n$ holds $v(j) = l(A(j))$ by [8, (3)]. $\square$

(12) Let us consider a finite sequence $A$ of elements of $\mathit{Boolean}^n$ and a finite subset $B$ of $n$-binary vector space. Suppose

(i) $\operatorname{rng} A = B$, and

(ii) $\operatorname{len} A = n$, and

(iii) $A$ is one-to-one, and

(iv) for every natural numbers $i$, $j$ such that $i$, $j \in \operatorname{Seg} n$ holds if $i = j$, then $A(i)(j) = \mathit{true}$ and if $i \neq j$, then $A(i)(j) = \mathit{false}$.

Then $\operatorname{Lin}(B) = \langle$the carrier of $n$-binary vector space, the addition of $n$-bi$-$nary vector space, the zero of $n$-binary vector space, the left multiplication of $n$-binary vector space$\rangle$. The theorem is a consequence of (11) and (9). PROOF: Set $V = n$-binary vector space. For every element $x$, $x \in$ the carrier of $\operatorname{Lin}(B)$ iff $x \in$ the carrier of $V$ by [5, (13)], [22, (7)]. $\square$

(13) There exists a finite subset $B$ of $n$-binary vector space such that

(i) $B$ is a basis of $n$-binary vector space, and

(ii) $\overline{\overline{B}} = n$, and

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(iii) there exists a finite sequence $A$ of elements of $Boolean^n$ such that $\operatorname{len} A = n$ and $A$ is one-to-one and $\overline{\overline{\operatorname{rng} A}} = n$ and $\operatorname{rng} A = B$ and for every natural numbers $i$, $j$ such that $i, j \in \operatorname{Seg} n$ holds if $i = j$, then $A(i)(j) = \mathit{true}$ and if $i \neq j$, then $A(i)(j) = \mathit{false}$.

The theorem is a consequence of (8), (10), and (12).

(14) (i) $n$-binary vector space is finite dimensional, and

(ii) $\dim(n\text{-binary vector space}) = n$.

The theorem is a consequence of (13).

Let $n$ be a non zero element of $\mathbb{N}$. One can verify that $n$-binary vector space is finite dimensional.

Now we state the proposition:

(15) Let us consider a finite sequence $A$ of elements of $Boolean^n$ and a subset $C$ of $n$-binary vector space. Suppose

(i) $\operatorname{len} A = n$, and

(ii) $A$ is one-to-one, and

(iii) $\overline{\overline{\operatorname{rng} A}} = n$, and

(iv) for every natural numbers $i$, $j$ such that $i, j \in \operatorname{Seg} n$ holds if $i = j$, then $A(i)(j) = \mathit{true}$ and if $i \neq j$, then $A(i)(j) = \mathit{false}$, and

(v) $C \subseteq \operatorname{rng} A$.

Then

(vi) $\operatorname{Lin}(C)$ is a subspace of $n$-binary vector space, and

(vii) $C$ is a basis of $\operatorname{Lin}(C)$, and

(viii) $\dim(\operatorname{Lin}(C)) = \overline{\overline{C}}$.

The theorem is a consequence of (10).

## References


[1] Jesse Alama. The vector space of subsets of a set based on symmetric difference. *Formalized Mathematics*, 16(**1**):1–5, 2008. doi:10.2478/v10037-008-0001-7.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[6] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[7] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.


Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[13] X. Lai. Higher order derivatives and differential cryptoanalysis. *Communications and Cryptography*, pages 227–233, 1994.

[14] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(**3**):339–345, 1996.

[15] J.C. Moreira and P.G. Farrell. *Essentials of Error-Control Coding*. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, 2006.

[16] Hiroyuki Okazaki and Yasunari Shidama. Formalization of the data encryption standard. *Formalized Mathematics*, 20(**2**):125–146, 2012. doi:10.2478/v10037-012-0016-y.

[17] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

[18] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[19] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[20] Wojciech A. Trybulec. Subspaces and cosets of subspaces in vector space. *Formalized Mathematics*, 1(**5**):865–870, 1990.

[21] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1 (**5**):877–882, 1990.

[22] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.

[23] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[24] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

[25] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[26] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[27] Mariusz Żynel. The Steinitz theorem and the dimension of a vector space. *Formalized Mathematics*, 5(**3**):423–428, 1996.

*Received April 17, 2013*

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 83–85, 2013
DOI: 10.2478/forma-2013-0009

VERSITA
degruyter.com/view/j/forma

# Some Properties of the Sorgenfrey Line and the Sorgenfrey Plane

Adam St. Arnaud
University of Alberta
Edmonton, Canada

Piotr Rudnicki
University of Alberta
Edmonton, Canada

**Summary.** We first provide a modified version of the proof in [3] that the Sorgenfrey line is $T_1$. Here, we prove that it is in fact $T_2$, a stronger result. Next, we prove that all subspaces of $\mathbb{R}^1$ (that is the real line with the usual topology) are Lindelöf. We utilize this result in the proof that the Sorgenfrey line is Lindelöf, which is based on the proof found in [8]. Next, we construct the Sorgenfrey plane, as the product topology of the Sorgenfrey line and itself. We prove that the Sorgenfrey plane is not Lindelöf, and therefore the product space of two Lindelöf spaces need not be Lindelöf. Further, we note that the Sorgenfrey line is regular, following from [3]:59. Next, we observe that the Sorgenfrey line is normal since it is both regular and Lindelöf. Finally, we prove that the Sorgenfrey plane is not normal, and hence the product of two normal spaces need not be normal. The proof that the Sorgenfrey plane is not normal and many of the lemmas leading up to this result are modelled after the proof in [3], that the Niemytzki plane is not normal. Information was also gathered from [15].

MSC: 54D15 54B10 03B35

Keywords: topological spaces; products of normal spaces; Sorgenfrey line; Sorgenfrey plane; Lindelöf spaces

MML identifier: `TOPGEN_6`, version: `8.1.01 5.13.1174`

The notation and terminology used in this paper have been introduced in the following articles: [16], [1], [13], [12], [11], [14], [19], [18], [9], [2], [10], [3], [7], [20], and [6].

In this paper $T$ denotes a topological space, $x$, $y$, $a$, $b$, $U$, $U_1$, $r_1$ denote sets, $p$, $q$ denote rational numbers, $F$, $G$ denote families of subsets of $T$, and $U_2$, $I$ denote families of subsets of Sorgenfrey line.

Observe that Sorgenfrey line is $T_2$.

Now we state the proposition:

(1) Let us consider real numbers $x$, $a$, $b$. Suppose $x \in ]a, b[$. Then there exist rational numbers $p$, $r$ such that

© 2013 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(Print), 1898-9934(Online)



Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(i) $x \in ]p, r[$, and

(ii) $]p, r[ \subseteq ]a, b[$.

PROOF: Consider $p$ being a rational number such that $p > a$ and $x > p$. Consider $r$ being a rational number such that $x < r < b$. $]p, r[ \subseteq ]a, b[$. □

Let us observe that every subspace of $\mathbb{R}^{\mathbf{1}}$ is Lindelöf and Sorgenfrey line is Lindelöf.

The Sorgenfrey plane yielding a non empty strict topological space is defined by the term

(Def. 1) Sorgenfrey line $\times$ Sorgenfrey line.

The functor real-anti-diagonal yielding a subset of $\mathbb{R} \times \mathbb{R}$ is defined by the term

(Def. 2) $\{\langle x, y\rangle$, where $x$, $y$ are real numbers : $y = -x\}$.

Now we state the propositions:

(2) $\mathbb{Q} \times \mathbb{Q}$ is a dense subset of the Sorgenfrey plane. PROOF: $\mathbb{Q} \times \mathbb{Q} \subseteq \Omega_\alpha$, where $\alpha$ is the Sorgenfrey plane by [17, (12)]. Reconsider $C = \mathbb{Q} \times \mathbb{Q}$ as a subset of the Sorgenfrey plane. For every subset $A$ of the Sorgenfrey plane such that $A \neq \emptyset$ and $A$ is open holds $A$ meets $C$ by [16, (5)], [6, (90)], [4, (31)]. □

(3) $\overline{\overline{\text{real-anti-diagonal}}} = \mathfrak{c}$. PROOF: $\mathbb{R} \approx$ real-anti-diagonal by [5, (4)]. □

(4) real-anti-diagonal is a closed subset of the Sorgenfrey plane. PROOF: Set $L =$ real-anti-diagonal. Set $S =$ the Sorgenfrey plane. $L \subseteq \Omega_S$. Reconsider $L =$ real-anti-diagonal as a subset of the Sorgenfrey plane. Define $\mathcal{P}[\text{element}, \text{element}] \equiv$ there exist real numbers $x$, $y$ such that $\$_1 = \langle x, y\rangle$ and $\$_2 = x + y$. For every element $z$ such that $z \in$ the carrier of $S$ there exists an element $u$ such that $u \in$ the carrier of $\mathbb{R}^{\mathbf{1}}$ and $\mathcal{P}[z, u]$ by [7, (17)]. Consider $f$ being a function from $S$ into $\mathbb{R}^{\mathbf{1}}$ such that for every element $z$ such that $z \in$ the carrier of $S$ holds $\mathcal{P}[z, f(z)]$ from [5, Sch. 1]. For every elements $x$, $y$ of $\mathbb{R}$ such that $\langle x, y\rangle \in$ the carrier of $S$ holds $f(\langle x, y\rangle) = x + y$. For every point $p$ of $S$ and for every positive real number $r$, there exists an open subset $W$ of $S$ such that $p \in W$ and $f^\circ W \subseteq ]f(p) - r, f(p) + r[$ by [2, (11)], [16, (6)]. Reconsider $z_1 = 0$ as an element of $\mathbb{R}$. Reconsider $k = \{z_1\}$ as a subset of $\mathbb{R}^{\mathbf{1}}$. $L = f^{-1}(k)$ by [5, (38)]. □

(5) Let us consider a subset $A$ of the Sorgenfrey plane. Suppose $A =$ real-anti-diagonal. Then $\operatorname{Der} A$ is empty.

(6) Every subset of real-anti-diagonal is a closed subset of the Sorgenfrey plane. The theorem is a consequence of (4) and (5).

Note that the Sorgenfrey plane is non Lindelöf and Sorgenfrey line is regular and Sorgenfrey line is normal and the Sorgenfrey plane is non normal.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

Acknowledgement: I would like to thank Piotr Rudnicki for taking me on as his summer student and being a mentor to me. Piotr was an incredibly caring, intelligent, funny, passionate human being. I am proud to know I was his last student, in a long line of students he has mentored and cared about throughout his life. Thank you Piotr, for the opportunity you gave me, and for the faith, confidence and trust you showed in me. I will miss you.

## References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. On constructing topological spaces and Sorgenfrey line. *Formalized Mathematics*, 13(**1**):171–179, 2005.
[3] Grzegorz Bancerek. Niemytzki plane - an example of Tychonoff space which is not $T_4$. *Formalized Mathematics*, 13(**4**):515–524, 2005.
[4] Grzegorz Bancerek. Bases and refinements of topologies. *Formalized Mathematics*, 7(**1**): 35–43, 1998.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[7] Agata Darmochwał and Yatsuka Nakamura. Metric spaces as topological spaces – fundamental concepts. *Formalized Mathematics*, 2(**4**):605–608, 1991.
[8] Ryszard Engelking. *Outline of General Topology.* North-Holland Publishing Company, 1968.
[9] Adam Grabowski. On the boundary and derivative of a set. *Formalized Mathematics*, 13 (**1**):139–146, 2005.
[10] Adam Grabowski. On the Borel families of subsets of topological spaces. *Formalized Mathematics*, 13(**4**):453–461, 2005.
[11] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.
[12] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[13] Karol Pąk. Basic properties of metrizable topological spaces. *Formalized Mathematics*, 17(**3**):201–205, 2009. doi:10.2478/v10037-009-0024-8.
[14] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[15] Lynn Arthur Steen and J. Arthur Jr. Seebach. *Counterexamples in Topology.* Springer-Verlag, 1978.
[16] Andrzej Trybulec. A Borsuk theorem on homotopy types. *Formalized Mathematics*, 2(**4**): 535–545, 1991.
[17] Andrzej Trybulec. Subsets of complex numbers. *Mizar Mathematical Library.*
[18] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[19] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[20] Mirosław Wysocki and Agata Darmochwał. Subsets of topological spaces. *Formalized Mathematics*, 1(**1**):231–237, 1990.

*Received April 17, 2013*

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 87–94, 2013
DOI: 10.2478/forma-2013-0010

VERSITA
degruyter.com/view/j/forma

# More on Divisibility Criteria for Selected Primes

Adam Naumowicz
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Radosław Piliszek
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

**Summary.** This paper is a continuation of [19], where the divisibility criteria for initial prime numbers based on their representation in the decimal system were formalized. In the current paper we consider all primes up to 101 to demonstrate the method presented in [7].

MSC: 11A63 03B35

Keywords: divisibility; divisibility rules; decimal digits

MML identifier: NUMERAL2, version: 8.1.02 5.17.1179

The notation and terminology used in this paper have been introduced in the following articles: [21], [25], [18], [1], [14], [12], [8], [9], [23], [17], [22], [2], [16], [19], [3], [4], [5], [6], [10], [15], [13], [26], [27], [24], and [11].

## 1. Preliminaries on Finite Sequences

In this paper $n$, $k$, $b$ denote natural numbers and $i$ denotes an integer.

Let us consider a non empty finite 0-sequence $f$. Now we state the propositions:

(1) $f \restriction 1 = \langle f(0) \rangle$.

(2) $f = \langle f(0) \rangle \frown f_{\lfloor 1}$.

Now we state the proposition:

(3) Let us consider a finite 0-sequence $f$. Then $\mathrm{mid}(f, 2, \mathrm{len}\, f) = f_{\lfloor 1}$.

Let us consider finite natural-membered sets $X$, $Y$. Now we state the propositions:



© 2013 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(Print), 1898-9934(Online)

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(4) If $X$ misses $Y$, then $\operatorname{dom}(\mathrm{Sgm}_0 X \frown \mathrm{Sgm}_0 Y) = \operatorname{dom} \mathrm{Sgm}_0(X \cup Y)$.

(5) $\operatorname{rng}(\mathrm{Sgm}_0 X \frown \mathrm{Sgm}_0 Y) = \operatorname{rng} \mathrm{Sgm}_0(X \cup Y)$.

Now we state the proposition:

(6) Let us consider a finite 0-sequence $F$ and a set $X$.
Then dom the $X$-subsequence of $F = \operatorname{dom} \mathrm{Sgm}_0(X \cap \operatorname{dom} F)$.

One can check that the functor $\mathbb{N}_{\mathrm{even}}$ is defined by the term

(Def. 1) $\{n$, where $n$ is a natural number : $n$ is even$\}$.

Note that the functor $\mathbb{N}_{\mathrm{odd}}$ is defined by the term

(Def. 2) $\{n$, where $n$ is a natural number : $n$ is odd$\}$.

Now we state the propositions:

(7) $\mathbb{N}_{\mathrm{even}}$ misses $\mathbb{N}_{\mathrm{odd}}$. Proof: $\mathbb{N}_{\mathrm{even}} \cap \mathbb{N}_{\mathrm{odd}} \subseteq \emptyset$. $\square$

(8) $\mathbb{N}_{\mathrm{even}} \cup \mathbb{N}_{\mathrm{odd}} = \mathbb{N}$.

Let $F$ be a transfinite sequence and $P$ be a permutation of dom $F$. One can verify that $F \cdot P$ is transfinite sequence-like.

Now we state the propositions:

(9) Let us consider a finite 0-sequence $F$ and sets $X$, $Y$. Suppose $X$ misses $Y$. Then there exists a permutation $P$ of dom the $X \cup Y$-subsequence of $F$ such that (the $X \cup Y$-subsequence of $F) \cdot P =$ (the $X$-subsequence of $F) \frown$ (the $Y$-subsequence of $F$). The theorem is a consequence of (5), (4), and (6).

(10) Let us consider a complex-valued finite 0-sequence $\mathcal{F}$ and sets $B_1$, $B_2$. Suppose $B_1$ misses $B_2$. Then $\sum$ the $B_1 \cup B_2$-subsequence of $\mathcal{F} =$ $\sum$ the $B_1$-subsequence of $\mathcal{F} + \sum$ the $B_2$-subsequence of $\mathcal{F}$. The theorem is a consequence of (9).

(11) Let us consider a finite 0-sequence $F$. Then $F =$ the $\mathbb{N}$-subsequence of $F$.

Let us consider natural numbers $N$, $i$. Now we state the propositions:

(12) If $i \in \operatorname{dom} \mathrm{Sgm}_0(N \cap \mathbb{N}_{\mathrm{even}})$, then $(\mathrm{Sgm}_0(N \cap \mathbb{N}_{\mathrm{even}}))(i) = 2 \cdot i$.

(13) If $i \in \operatorname{dom} \mathrm{Sgm}_0(N \cap \mathbb{N}_{\mathrm{odd}})$, then $(\mathrm{Sgm}_0(N \cap \mathbb{N}_{\mathrm{odd}}))(i) = 2 \cdot i + 1$.

## 2. Lemmas on Some Divisibility Properties

Now we state the propositions:

(14) Let us consider integers $i$, $j$. Then $(i \bmod j) \bmod j = i \bmod j$.

(15) Let us consider integers $i$, $j$, $k$, $l$. Suppose $i \bmod l = j \bmod l$. Then $(k + i) \bmod l = (k + j) \bmod l$.

(16) Let us consider a finite 0-sequence $d$ of $\mathbb{Z}$ and an integer $n$. Suppose a natural number $i$. If $i \in \operatorname{dom} d$, then $n \mid d(i)$. Then $n \mid \sum d$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(17) Let us consider finite 0-sequences $d$, $e$ of $\mathbb{Z}$ and an integer $n$. Suppose

(i) $\operatorname{dom} d = \operatorname{dom} e$, and

(ii) for every natural number $i$ such that $i \in \operatorname{dom} d$ holds $e(i) = d(i) \bmod n$.

Then $\sum d \bmod n = \sum e \bmod n$. The theorem is a consequence of (14).
Proof: Define $\mathcal{P}[\text{finite 0-sequence of } \mathbb{Z}] \equiv$ for every finite 0-sequence $e$ of $\mathbb{Z}$ such that $\operatorname{dom} \$_1 = \operatorname{dom} e$ and for every natural number $i$ such that $i \in \operatorname{dom} \$_1$ holds $e(i) = \$_1(i) \bmod n$ holds $\sum \$_1 \bmod n = \sum e \bmod n$. For every finite 0-sequence $p$ of $\mathbb{Z}$ and for every element $l$ of $\mathbb{Z}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle l \rangle]$ by [2, (44), (13)], [25, (33)]. $\mathcal{P}[\langle\rangle_{\mathbb{Z}}]$ by [25, (15)]. For every finite 0-sequence $p$ of $\mathbb{Z}$, $\mathcal{P}[p]$ from [18, Sch. 2]. $\square$

(18) Let us consider finite 0-sequences $f$, $g$ of $\mathbb{N}$ and an integer $i$. Suppose

(i) $\operatorname{dom} f = \operatorname{dom} g$, and

(ii) for every element $n$ such that $n \in \operatorname{dom} f$ holds $f(n) = i \cdot g(n)$.

Then $\sum f = i \cdot \sum g$.

(19) If $b > 1$, then $n = b \cdot \operatorname{value}(\operatorname{mid}(\operatorname{digits}(n, b), 2, \operatorname{len} \operatorname{digits}(n, b)), b) + (\operatorname{digits}(n, b))(0)$. The theorem is a consequence of (2), (18), and (3).

Let us consider natural numbers $n$, $k$. Now we state the propositions:

(20) If $k = 10^{2 \cdot n} - 1$, then $11 \mid k$.

(21) If $k = 10^{2 \cdot n + 1} + 1$, then $11 \mid k$.

Now we state the propositions:

(22) 7 and 10 are relatively prime.

(23) 29 is prime.

(24) 31 is prime.

(25) 41 is prime.

(26) 47 is prime.

(27) 53 is prime.

(28) 59 is prime.

(29) 61 is prime.

(30) 67 is prime.

(31) 71 is prime.

(32) 73 is prime.

(33) 79 is prime.

(34) 89 is prime.

(35) 97 is prime.

(36) 101 is prime.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

## 3. Divisibility Criteria for Primes up to 101

Let us consider a prime natural number $p$ and natural numbers $n$, $f$, $b$. Now we state the propositions:

(37) Suppose there exists a natural number $k$ such that $b \cdot f + 1 = p \cdot k$ and $b > 1$ and $p$ and $b$ are relatively prime. Then $p \mid n$ if and only if $p \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, b), 2, \mathrm{len}\,\mathrm{digits}(n, b)), b) - f \cdot (\mathrm{digits}(n, b))(0)$.

(38) Suppose there exists a natural number $k$ such that $b \cdot f - 1 = p \cdot k$ and $b > 1$ and $p$ and $b$ are relatively prime. Then $p \mid n$ if and only if $p \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, b), 2, \mathrm{len}\,\mathrm{digits}(n, b)), b) + f \cdot (\mathrm{digits}(n, b))(0)$.

Now we state the propositions:

(39) Divisibility rule–Divisibility by 7: $7 \mid n$ if and only if $7 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\,\mathrm{digits}(n, 10)), 10) - 2 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (37) and (22).

(40) $7 \mid n$ if and only if $7 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\restriction 1}, 10) - 2 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (39).

(41) $11 \mid n$ if and only if $11 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\,\mathrm{digits}(n, 10)), 10) - (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (37).

(42) $11 \mid n$ if and only if $11 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\restriction 1}, 10) - (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (41).

Now we state the proposition:

(43) Divisibility rule–Divisibility by 11: $11 \mid n$ if and only if $11 \mid \sum$ the $\mathbb{N}_{\mathrm{even}}$-subsequence of $\mathrm{digits}(n, 10) - \sum$ the $\mathbb{N}_{\mathrm{odd}}$-subsequence of $\mathrm{digits}(n, 10)$. The theorem is a consequence of (10), (7), (8), (11), (6), (12), (13), (20), (16), (21), and (14). Proof: Set $d = \mathrm{digits}(n, 10)$. Consider $p$ being a finite 0-sequence of $\mathbb{N}$ such that $\mathrm{dom}\, p = \mathrm{dom}\, d$ and for every natural number $i$ such that $i \in \mathrm{dom}\, p$ holds $p(i) = d(i) \cdot 10^i$ and $\mathrm{value}(d, 10) = \sum p$. Set $p_3 =$ the $\mathbb{N}_{\mathrm{even}}$-subsequence of $p$. Set $p_2 =$ the $\mathbb{N}_{\mathrm{odd}}$-subsequence of $p$. Set $d_2 =$ the $\mathbb{N}_{\mathrm{even}}$-subsequence of $d$. Set $d_3 =$ the $\mathbb{N}_{\mathrm{odd}}$-subsequence of $d$. For every natural number $i$ such that $i \in \mathrm{dom}\, d_2$ holds $d_2(i) = d(2 \cdot i)$ by [8, (11), (12)]. For every natural number $i$ such that $i \in \mathrm{dom}\, p_3$ holds $p_3(i) = d_2(i) \cdot 10^{2 \cdot i}$ by [8, (11), (12)]. For every natural number $i$ such that $i \in \mathrm{dom}\, d_3$ holds $d_3(i) = d(2 \cdot i + 1)$ by [8, (11), (12)]. For every natural number $i$ such that $i \in \mathrm{dom}\, p_2$ holds $p_2(i) = d_3(i) \cdot 10^{2 \cdot i + 1}$ by [8, (11), (12)]. Define $\mathcal{E}[\mathrm{set}, \mathrm{set}] \equiv \$_2 = p_3(\$_1) - d_2(\$_1)$. For every natural number $k$ such that $k \in \mathbb{Z}_{\mathrm{dom}\, p_3}$ there exists an element $x$ of $\mathbb{Z}$ such that $\mathcal{E}[k, x]$. Consider $p_1$ being a finite 0-sequence of $\mathbb{Z}$ such that $\mathrm{dom}\, p_1 = \mathbb{Z}_{\mathrm{dom}\, p_3}$ and for every natural number $k$ such that $k \in \mathbb{Z}_{\mathrm{dom}\, p_3}$ holds $\mathcal{E}[k, p_1(k)]$ from [20, Sch. 5]. For every natural number $i$ such that $i \in \mathrm{dom}\, p_3$ holds $p_3(i) = +_{\mathbb{Z}}(p_1(i), d_2(i))$. Define $\mathcal{O}[\mathrm{set}, \mathrm{set}] \equiv \$_2 = p_2(\$_1) + d_3(\$_1)$. Consider $p_4$ being a finite 0-sequence of

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

$\mathbb{N}$ such that $\operatorname{dom} p_4 = \mathbb{Z}_{\operatorname{dom} p_2}$ and for every natural number $k$ such that $k \in \mathbb{Z}_{\operatorname{dom} p_2}$ holds $\mathcal{O}[k, p_4(k)]$ from [20, Sch. 5]. Set $m = (-1) \cdot d_3$. For every natural number $i$ such that $i \in \operatorname{dom} p_2$ holds $p_2(i) = +_{\mathbb{Z}}(p_4(i), m(i))$. If $11 \mid n$, then $11 \mid \sum d_2 - \sum d_3$ by [19, (5)], [23, (62)]. If $11 \mid \sum d_2 - \sum d_3$, then $11 \mid n$ by [23, (62)], [19, (5)]. $\square$

Now we state the propositions:

(44) Divisibility rule–Divisibility by 13:
$13 \mid n$ if and only if $13 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\,\mathrm{digits}(n, 10)), 10) + 4 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (38).

(45) $13 \mid n$ if and only if $13 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\downharpoonright 1}, 10) + 4 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (44).

(46) $17 \mid n$ if and only if $17 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\,\mathrm{digits}(n, 10)), 10) - 5 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (37).

(47) $17 \mid n$ if and only if $17 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\downharpoonright 1}, 10) - 5 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (46).

(48) $19 \mid n$ if and only if $19 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\,\mathrm{digits}(n, 10)), 10) + 2 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (38).

(49) $19 \mid n$ if and only if $19 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\downharpoonright 1}, 10) + 2 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (48).

(50) $23 \mid n$ if and only if $23 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\,\mathrm{digits}(n, 10)), 10) + 7 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (38).

(51) $23 \mid n$ if and only if $23 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\downharpoonright 1}, 10) + 7 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (50).

(52) $29 \mid n$ if and only if $29 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\,\mathrm{digits}(n, 10)), 10) + 3 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (23) and (38).

(53) $29 \mid n$ if and only if $29 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\downharpoonright 1}, 10) + 3 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (52).

(54) $31 \mid n$ if and only if $31 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\,\mathrm{digits}(n, 10)), 10) - 3 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (24) and (37).

(55) $31 \mid n$ if and only if $31 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\downharpoonright 1}, 10) - 3 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (54).

(56) $37 \mid n$ if and only if $37 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\,\mathrm{digits}(n, 10)), 10) - 11 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (37).

(57) $37 \mid n$ if and only if $37 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\downharpoonright 1}, 10) - 11 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (56).

(58) $41 \mid n$ if and only if $41 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\,\mathrm{digits}(n, 10)), 10) - 4 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (25) and (37).

(59) $41 \mid n$ if and only if $41 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\downharpoonright 1}, 10) - 4 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (58).

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(60) $43 \mid n$ if and only if $43 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n,10),2,\mathrm{len}\,\mathrm{digits}(n,10)),10)+13\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (38).

(61) $43 \mid n$ if and only if $43 \mid \mathrm{value}((\mathrm{digits}(n,10))_{\lfloor 1},10)+13\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (3) and (60).

(62) $47 \mid n$ if and only if $47 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n,10),2,\mathrm{len}\,\mathrm{digits}(n,10)),10)-14\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (26) and (37).

(63) $47 \mid n$ if and only if $47 \mid \mathrm{value}((\mathrm{digits}(n,10))_{\lfloor 1},10)-14\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (3) and (62).

(64) $53 \mid n$ if and only if $53 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n,10),2,\mathrm{len}\,\mathrm{digits}(n,10)),10)+16\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (27) and (38).

(65) $53 \mid n$ if and only if $53 \mid \mathrm{value}((\mathrm{digits}(n,10))_{\lfloor 1},10)+16\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (3) and (64).

(66) $59 \mid n$ if and only if $59 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n,10),2,\mathrm{len}\,\mathrm{digits}(n,10)),10)+6\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (28) and (38).

(67) $59 \mid n$ if and only if $59 \mid \mathrm{value}((\mathrm{digits}(n,10))_{\lfloor 1},10)+6\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (3) and (66).

(68) $61 \mid n$ if and only if $61 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n,10),2,\mathrm{len}\,\mathrm{digits}(n,10)),10)-6\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (29) and (37).

(69) $61 \mid n$ if and only if $61 \mid \mathrm{value}((\mathrm{digits}(n,10))_{\lfloor 1},10)-6\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (3) and (68).

(70) $67 \mid n$ if and only if $67 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n,10),2,\mathrm{len}\,\mathrm{digits}(n,10)),10)-20\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (30) and (37).

(71) $67 \mid n$ if and only if $67 \mid \mathrm{value}((\mathrm{digits}(n,10))_{\lfloor 1},10)-20\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (3) and (70).

(72) $71 \mid n$ if and only if $71 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n,10),2,\mathrm{len}\,\mathrm{digits}(n,10)),10)-7\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (31) and (37).

(73) $71 \mid n$ if and only if $71 \mid \mathrm{value}((\mathrm{digits}(n,10))_{\lfloor 1},10)-7\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (3) and (72).

(74) $73 \mid n$ if and only if $73 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n,10),2,\mathrm{len}\,\mathrm{digits}(n,10)),10)+22\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (32) and (38).

(75) $73 \mid n$ if and only if $73 \mid \mathrm{value}((\mathrm{digits}(n,10))_{\lfloor 1},10)+22\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (3) and (74).

(76) $79 \mid n$ if and only if $79 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n,10),2,\mathrm{len}\,\mathrm{digits}(n,10)),10)+8\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (33) and (38).

(77) $79 \mid n$ if and only if $79 \mid \mathrm{value}((\mathrm{digits}(n,10))_{\lfloor 1},10)+8\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (3) and (76).

(78) $83 \mid n$ if and only if $83 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n,10),2,\mathrm{len}\,\mathrm{digits}(n,10)),10)+25\cdot(\mathrm{digits}(n,10))(0)$. The theorem is a consequence of (38).

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(79) $83 \mid n$ if and only if $83 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\lfloor 1}, 10) + 25 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (78).

(80) $89 \mid n$ if and only if $89 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\, \mathrm{digits}(n, 10)), 10) + 9 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (34) and (38).

(81) $89 \mid n$ if and only if $89 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\lfloor 1}, 10) + 9 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (80).

(82) $97 \mid n$ if and only if $97 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\, \mathrm{digits}(n, 10)), 10) - 29 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (35) and (37).

(83) $97 \mid n$ if and only if $97 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\lfloor 1}, 10) - 29 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (82).

(84) $101 \mid n$ if and only if $101 \mid \mathrm{value}(\mathrm{mid}(\mathrm{digits}(n, 10), 2, \mathrm{len}\, \mathrm{digits}(n, 10)), 10) - 10 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (36) and (37).

(85) $101 \mid n$ if and only if $101 \mid \mathrm{value}((\mathrm{digits}(n, 10))_{\lfloor 1}, 10) - 10 \cdot (\mathrm{digits}(n, 10))(0)$. The theorem is a consequence of (3) and (84).

## References


[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[4] Grzegorz Bancerek. Sequences of ordinal numbers. *Formalized Mathematics*, 1(**2**):281–290, 1990.

[5] Grzegorz Bancerek. Increasing and continuous ordinal sequences. *Formalized Mathematics*, 1(**4**):711–714, 1990.

[6] Grzegorz Bancerek. Veblen hierarchy. *Formalized Mathematics*, 19(**2**):83–92, 2011. doi:10.2478/v10037-011-0014-5.

[7] C.C. Briggs. Simple divisibility rules for the 1st 1000 prime numbers. *arXiv preprint arXiv:math/0001012*, 2000.

[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[10] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[11] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[13] Krzysztof Hryniewiecki. Recursive definitions. *Formalized Mathematics*, 1(**2**):321–328, 1990.

[14] Magdalena Jastrzębska and Adam Grabowski. Some properties of Fibonacci numbers. *Formalized Mathematics*, 12(**3**):307–313, 2004.

[15] Artur Korniłowicz. On the real valued functions. *Formalized Mathematics*, 13(**1**):181–187, 2005.

[16] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[17] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[18] Yatsuka Nakamura and Hisashi Ito. Basic properties and concept of selected subsequence of zero based finite sequences. *Formalized Mathematics*, 16(**3**):283–288, 2008. doi:10.2478/v10037-008-0034-y.


Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

[19] Adam Naumowicz. On the representation of natural numbers in positional numeral systems. *Formalized Mathematics*, 14(**4**):221–223, 2006. doi:10.2478/v10037-006-0025-9.

[20] Karol Pąk. Stirling numbers of the second kind. *Formalized Mathematics*, 13(**2**):337–345, 2005.

[21] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[22] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[23] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[24] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[25] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.

[26] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[27] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

*Received May 19, 2013*

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 95–102, 2013
DOI: 10.2478/forma-2013-0011

VERSITA
degruyter.com/view/j/forma

# Differentiation in Normed Spaces[1]

Noboru Endou
Gifu National College of Technology
Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

**Summary.** In this article we formalized the Fréchet differentiation. It is defined as a generalization of the differentiation of a real-valued function of a single real variable to more general functions whose domain and range are subsets of normed spaces [14].

MSC: 58C20 46G05 03B35

Keywords: formalization of Fréchet derivative; Fréchet differentiability

MML identifier: `NDIFF_6`, version: `8.1.02 5.17.1179`

The notation and terminology used in this paper have been introduced in the following articles: [5], [1], [4], [10], [6], [7], [16], [15], [11], [12], [13], [3], [8], [19], [20], [17], [18], [21], and [9].

Let us consider non empty sets $D$, $E$, $F$. Now we state the propositions:

(1) There exists a function $I$ from $(F^E)^D$ into $F^{D \times E}$ such that

  (i) $I$ is bijective, and

  (ii) for every function $f$ from $D$ into $F^E$ and for every elements $d$, $e$ such that $d \in D$ and $e \in E$ holds $I(f)(d, e) = f(d)(e)$.

(2) There exists a function $I$ from $(F^E)^D$ into $F^{E \times D}$ such that

  (i) $I$ is bijective, and

  (ii) for every function $f$ from $D$ into $F^E$ and for every elements $e$, $d$ such that $e \in E$ and $d \in D$ holds $I(f)(e, d) = f(d)(e)$.

Now we state the propositions:

(3) Let us consider non-empty non empty finite sequences $D$, $E$ and a non empty set $F$. Then there exists a function $L$ from $(F^{\prod E})^{\prod D}$ into $F^{\prod (E ^\frown D)}$ such that

  (i) $L$ is bijective, and

[1] This work was supported by JSPS KAKENHI 23500029 and 22300285.

© 2013 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(Print), 1898-9934(Online)



Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(ii) for every function $f$ from $\prod D$ into $F^{\prod E}$ and for every finite sequences $e$, $d$ such that $e \in \prod E$ and $d \in \prod D$ holds $L(f)(e \frown d) = f(d)(e)$.

The theorem is a consequence of (2). PROOF: Consider $I$ being a function from $(F^{\prod E})^{\prod D}$ into $F^{\prod E \times \prod D}$ such that $I$ is bijective and for every function $f$ from $\prod D$ into $F^{\prod E}$ and for every elements $e$, $d$ such that $e \in \prod E$ and $d \in \prod D$ holds $I(f)(e, d) = f(d)(e)$. Consider $J$ being a function from $\prod E \times \prod D$ into $\prod(E \frown D)$ such that $J$ is one-to-one and onto and for every finite sequences $x$, $y$ such that $x \in \prod E$ and $y \in \prod D$ holds $J(x, y) = x \frown y$. Reconsider $K = J^{-1}$ as a function from $\prod(E \frown D)$ into $\prod E \times \prod D$. Define $\mathcal{G}(\text{element}) = I(\$_1) \cdot K$. For every element $x$ such that $x \in (F^{\prod E})^{\prod D}$ holds $\mathcal{G}(x) \in F^{\prod(E \frown D)}$ by [7, (5), (8), (128)]. Consider $L$ being a function from $(F^{\prod E})^{\prod D}$ into $F^{\prod(E \frown D)}$ such that for every element $e$ such that $e \in (F^{\prod E})^{\prod D}$ holds $L(e) = \mathcal{G}(e)$ from [7, Sch. 2]. For every function $f$ from $\prod D$ into $F^{\prod E}$ and for every finite sequences $e$, $d$ such that $e \in \prod E$ and $d \in \prod D$ holds $L(f)(e \frown d) = f(d)(e)$ by [9, (87)], [7, (26), (8), (5)]. □

(4) Let us consider non empty sets $X$, $Y$. Then there exists a function $I$ from $X \times Y$ into $X \times \prod\langle Y \rangle$ such that

(i) $I$ is bijective, and

(ii) for every elements $x$, $y$ such that $x \in X$ and $y \in Y$ holds $I(x, y) = \langle\!\langle x, \langle y \rangle\rangle\!\rangle$.

PROOF: Consider $J$ being a function from $Y$ into $\prod\langle Y \rangle$ such that $J$ is one-to-one and onto and for every element $y$ such that $y \in Y$ holds $J(y) = \langle y \rangle$. Define $\mathcal{P}[\text{element}, \text{element}, \text{element}] \equiv \$_3 = \langle\!\langle \$_1, \langle \$_2 \rangle\rangle\!\rangle$. For every elements $x$, $y$ such that $x \in X$ and $y \in Y$ there exists an element $z$ such that $z \in X \times \prod\langle Y \rangle$ and $\mathcal{P}[x, y, z]$ by [7, (5)], [9, (87)]. Consider $I$ being a function from $X \times Y$ into $X \times \prod\langle Y \rangle$ such that for every elements $x$, $y$ such that $x \in X$ and $y \in Y$ holds $\mathcal{P}[x, y, I(x, y)]$ from [5, Sch. 1]. □

(5) Let us consider a non-empty non empty finite sequence $X$ and a non empty set $Y$. Then there exists a function $K$ from $\prod X \times Y$ into $\prod(X \frown \langle Y \rangle)$ such that

(i) $K$ is bijective, and

(ii) for every finite sequence $x$ and for every element $y$ such that $x \in \prod X$ and $y \in Y$ holds $K(x, y) = x \frown \langle y \rangle$.

The theorem is a consequence of (4). PROOF: Consider $I$ being a function from $\prod X \times Y$ into $\prod X \times \prod\langle Y \rangle$ such that $I$ is bijective and for every element $x$ and for every element $y$ such that $x \in \prod X$ and $y \in Y$ holds $I(x, y) = \langle\!\langle x, \langle y \rangle\rangle\!\rangle$. Consider $J$ being a function from $\prod X \times \prod\langle Y \rangle$ into $\prod(X \frown \langle Y \rangle)$ such that $J$ is one-to-one and onto and for every finite sequences $x$, $y$ such that $x \in \prod X$ and $y \in \prod\langle Y \rangle$ holds $J(x, y) = x \frown y$. Set

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

$K = J \cdot I$. For every finite sequence $x$ and for every element $y$ such that $x \in \prod X$ and $y \in Y$ holds $K(x, y) = x \frown \langle y \rangle$ by [9, (87)], [7, (5), (15)]. $\square$

(6) Let us consider a non empty set $D$, a non-empty non empty finite sequence $E$, and a non empty set $F$. Then there exists a function $L$ from $(F^{\prod E})^D$ into $F^{\prod (E \frown \langle D \rangle)}$ such that

(i) $L$ is bijective, and

(ii) for every function $f$ from $D$ into $F^{\prod E}$ and for every finite sequence $e$ and for every element $d$ such that $e \in \prod E$ and $d \in D$ holds $L(f)(e \frown \langle d \rangle) = f(d)(e)$.

The theorem is a consequence of (2) and (5). Proof: Consider $I$ being a function from $(F^{\prod E})^D$ into $F^{\prod E \times D}$ such that $I$ is bijective and for every function $f$ from $D$ into $F^{\prod E}$ and for every elements $e$, $d$ such that $e \in \prod E$ and $d \in D$ holds $I(f)(e, d) = f(d)(e)$. Consider $J$ being a function from $\prod E \times D$ into $\prod (E \frown \langle D \rangle)$ such that $J$ is bijective and for every finite sequence $x$ and for every element $y$ such that $x \in \prod E$ and $y \in D$ holds $J(x, y) = x \frown \langle y \rangle$. Reconsider $K = J^{-1}$ as a function from $\prod (E \frown \langle D \rangle)$ into $\prod E \times D$. Define $\mathcal{G}(\text{element}) = I(\$_1) \cdot K$. For every element $x$ such that $x \in (F^{\prod E})^D$ holds $\mathcal{G}(x) \in F^{\prod (E \frown \langle D \rangle)}$ by [7, (5), (8), (128)]. Consider $L$ being a function from $(F^{\prod E})^D$ into $F^{\prod (E \frown \langle D \rangle)}$ such that for every element $e$ such that $e \in (F^{\prod E})^D$ holds $L(e) = \mathcal{G}(e)$ from [7, Sch. 2]. For every function $f$ from $D$ into $F^{\prod E}$ and for every finite sequence $e$ and for every element $d$ such that $e \in \prod E$ and $d \in D$ holds $L(f)(e \frown \langle d \rangle) = f(d)(e)$ by [7, (5), (26), (8)]. $\square$

In this paper $S$, $T$ denote real normed spaces, $f$, $f_1$, $f_2$ denote partial functions from $S$ to $T$, $Z$ denotes a subset of $S$, and $i$, $n$ denote natural numbers.

Let $S$ be a set. Assume $S$ is a real normed space. The functor $\mathrm{NormSp}_{\mathbb{R}}(S)$ yielding a real normed space is defined by the term

(Def. 1) $S$.

Let $S$, $T$ be real normed spaces. The functor $\mathrm{diff}_{\mathrm{SP}}(S, T)$ yielding a function is defined by

(Def. 2) (i) $\mathrm{dom}\, it = \mathbb{N}$, and

(ii) $it(0) = T$, and

(iii) for every natural number $i$, $it(i+1) =$ the real norm space of bounded linear operators from $S$ into $\mathrm{NormSp}_{\mathbb{R}}(it(i))$.

Now we state the proposition:

(7) (i) $(\mathrm{diff}_{\mathrm{SP}}(S, T))(0) = T$, and

(ii) $(\mathrm{diff}_{\mathrm{SP}}(S, T))(1) =$ the real norm space of bounded linear operators from $S$ into $T$, and

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(iii) $(\mathrm{diff}_{\mathrm{SP}}(S,T))(2) =$ the real norm space of bounded linear operators from $S$ into the real norm space of bounded linear operators from $S$ into $T$.

Let us consider a natural number $i$. Now we state the propositions:

(8) $(\mathrm{diff}_{\mathrm{SP}}(S,T))(i)$ is a real normed space.

(9) There exists a real normed space $H$ such that

(i) $H = (\mathrm{diff}_{\mathrm{SP}}(S,T))(i)$, and

(ii) $(\mathrm{diff}_{\mathrm{SP}}(S,T))(i+1) =$ the real norm space of bounded linear operators from $S$ into $H$.

Let $S$, $T$ be real normed spaces and $i$ be a natural number. The functor $\mathrm{diff}_{\mathrm{SP}}(S^i, T)$ yielding a real normed space is defined by the term

(Def. 3) $(\mathrm{diff}_{\mathrm{SP}}(S,T))(i)$.

Now we state the proposition:

(10) Let us consider a natural number $i$. Then $\mathrm{diff}_{\mathrm{SP}}(S^{(i+1)}, T) =$ the real norm space of bounded linear operators from $S$ into $\mathrm{diff}_{\mathrm{SP}}(S^i, T)$. The theorem is a consequence of (9).

Let $S, T$ be real normed spaces and $f$ be a set. Assume $f$ is a partial function from $S$ to $T$. The functor $\mathrm{PartFuncs}(f, S, T)$ yielding a partial function from $S$ to $T$ is defined by the term

(Def. 4) $f$.

Let $f$ be a partial function from $S$ to $T$ and $Z$ be a subset of $S$. The functor $f'(Z)$ yielding a function is defined by

(Def. 5) (i) $\mathrm{dom}\, it = \mathbb{N}$, and

(ii) $it(0) = f{\restriction}Z$, and

(iii) for every natural number $i$, $it(i+1) = (\mathrm{PartFuncs}(it(i), S, \mathrm{diff}_{\mathrm{SP}}(S^i, T)))'_{\restriction Z}$.

Now we state the propositions:

(11) (i) $f'(Z)(0) = f{\restriction}Z$, and

(ii) $f'(Z)(1) = (f{\restriction}Z)'_{\restriction Z}$, and

(iii) $f'(Z)(2) = ((f{\restriction}Z)'_{\restriction Z})'_{\restriction Z}$.

The theorem is a consequence of (7).

(12) Let us consider a natural number $i$. Then $f'(Z)(i)$ is a partial function from $S$ to $\mathrm{diff}_{\mathrm{SP}}(S^i, T)$. The theorem is a consequence of (7). PROOF: Define $\mathcal{P}[\text{natural number}] \equiv f'(Z)(\$_1)$ is a partial function from $S$ to $\mathrm{diff}_{\mathrm{SP}}(S^{\$_1}, T)$. For every natural number $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. □

Let $S$, $T$ be real normed spaces, $f$ be a partial function from $S$ to $T$, $Z$ be a subset of $S$, and $i$ be a natural number. The functor $\mathrm{diff}_Z(f, i)$ yielding a partial function from $S$ to $\mathrm{diff}_{\mathrm{SP}}(S^i, T)$ is defined by the term

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(Def. 6) $f'(Z)(i)$.

Now we state the proposition:

(13) $\mathrm{diff}_Z(f, i+1) = \mathrm{diff}_Z(f,i)'_{\restriction Z}$. The theorem is a consequence of (12) and (8).

Let $S$, $T$ be real normed spaces, $f$ be a partial function from $S$ to $T$, $Z$ be a subset of $S$, and $n$ be a natural number. We say that $f$ is differentiable $n$ times on $Z$ if and only if

(Def. 7) (i) $Z \subseteq \mathrm{dom}\, f$, and

(ii) for every natural number $i$ such that $i \leqslant n-1$ holds $\mathrm{PartFuncs}(f'(Z)(i), S, \mathrm{diff}_{\mathrm{SP}}(S^i, T))$ is differentiable on $Z$.

Now we state the propositions:

(14) $f$ is differentiable $n$ times on $Z$ if and only if $Z \subseteq \mathrm{dom}\, f$ and for every natural number $i$ such that $i \leqslant n-1$ holds $\mathrm{diff}_Z(f,i)$ is differentiable on $Z$.

(15) $f$ is differentiable 1 times on $Z$ if and only if $Z \subseteq \mathrm{dom}\, f$ and $f{\restriction}Z$ is differentiable on $Z$. The theorem is a consequence of (14) and (7). Proof: For every natural number $i$ such that $i \leqslant 1-1$ holds $\mathrm{diff}_Z(f,i)$ is differentiable on $Z$. $\square$

(16) $f$ is differentiable 2 times on $Z$ if and only if $Z \subseteq \mathrm{dom}\, f$ and $f{\restriction}Z$ is differentiable on $Z$ and $(f{\restriction}Z)'_{\restriction Z}$ is differentiable on $Z$. The theorem is a consequence of (14), (7), and (11). Proof: For every natural number $i$ such that $i \leqslant 2-1$ holds $\mathrm{diff}_Z(f,i)$ is differentiable on $Z$ by [2, (14)]. $\square$

(17) Let us consider real normed spaces $S$, $T$, a partial function $f$ from $S$ to $T$, a subset $Z$ of $S$, and a natural number $n$. Suppose $f$ is differentiable $n$ times on $Z$. Let us consider a natural number $m$. If $m \leqslant n$, then $f$ is differentiable $m$ times on $Z$.

(18) Let us consider a natural number $n$ and a partial function $f$ from $S$ to $T$. If $1 \leqslant n$ and $f$ is differentiable $n$ times on $Z$, then $Z$ is open. The theorem is a consequence of (17) and (15).

(19) Let us consider a natural number $n$ and a partial function $f$ from $S$ to $T$. Suppose

(i) $1 \leqslant n$, and

(ii) $f$ is differentiable $n$ times on $Z$.

Let us consider a natural number $i$. Suppose $i \leqslant n$. Then

(iii) $(\mathrm{diff}_{\mathrm{SP}}(S,T))(i)$ is a real normed space, and

(iv) $f'(Z)(i)$ is a partial function from $S$ to $\mathrm{diff}_{\mathrm{SP}}(S^i, T)$, and

(v) $\mathrm{dom}\,\mathrm{diff}_Z(f,i) = Z$.

The theorem is a consequence of (13) and (14).

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(20) Let us consider a natural number $n$ and partial functions $f$, $g$ from $S$ to $T$. Suppose

(i) $1 \leqslant n$, and

(ii) $f$ is differentiable $n$ times on $Z$, and

(iii) $g$ is differentiable $n$ times on $Z$.

Let us consider a natural number $i$. Suppose $i \leqslant n$. Then $\mathrm{diff}_Z(f+g,i) = \mathrm{diff}_Z(f,i) + \mathrm{diff}_Z(g,i)$. The theorem is a consequence of (18), (14), (19), (13), and (10). Proof: Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant n$, then $\mathrm{diff}_Z(f+g,\$_1) = \mathrm{diff}_Z(f,\$_1) + \mathrm{diff}_Z(g,\$_1)$. $\mathcal{P}[0]$ by [21, (27)]. For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [2, (11)], [11, (39)], [8, (5)]. For every natural number $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. □

(21) Let us consider a natural number $n$ and partial functions $f$, $g$ from $S$ to $T$. Suppose

(i) $1 \leqslant n$, and

(ii) $f$ is differentiable $n$ times on $Z$, and

(iii) $g$ is differentiable $n$ times on $Z$.

Then $f+g$ is differentiable $n$ times on $Z$. The theorem is a consequence of (18), (14), (19), and (20). Proof: For every natural number $i$ such that $i \leqslant n-1$ holds $\mathrm{diff}_Z(f+g,i)$ is differentiable on $Z$ by [11, (39)]. □

(22) Let us consider a natural number $n$ and partial functions $f$, $g$ from $S$ to $T$. Suppose

(i) $1 \leqslant n$, and

(ii) $f$ is differentiable $n$ times on $Z$, and

(iii) $g$ is differentiable $n$ times on $Z$.

Let us consider a natural number $i$. Suppose $i \leqslant n$. Then $\mathrm{diff}_Z(f-g,i) = \mathrm{diff}_Z(f,i) - \mathrm{diff}_Z(g,i)$. The theorem is a consequence of (18), (14), (19), (13), and (10). Proof: Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant n$, then $\mathrm{diff}_Z(f-g,\$_1) = \mathrm{diff}_Z(f,\$_1) - \mathrm{diff}_Z(g,\$_1)$. $\mathcal{P}[0]$ by [21, (30)]. For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [2, (11)], [11, (40)], [8, (5)]. For every natural number $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. □

(23) Let us consider a natural number $n$ and partial functions $f$, $g$ from $S$ to $T$. Suppose

(i) $1 \leqslant n$, and

(ii) $f$ is differentiable $n$ times on $Z$, and

(iii) $g$ is differentiable $n$ times on $Z$.

Then $f-g$ is differentiable $n$ times on $Z$. The theorem is a consequence of (18), (14), (19), and (22). Proof: For every natural number $i$ such that $i \leqslant n-1$ holds $\mathrm{diff}_Z(f-g,i)$ is differentiable on $Z$ by [11, (40)]. □

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

(24) Let us consider a natural number $n$, a real number $r$, and a partial function $f$ from $S$ to $T$. Suppose

(i) $1 \leqslant n$, and

(ii) $f$ is differentiable $n$ times on $Z$.

Let us consider a natural number $i$. If $i \leqslant n$, then $\mathrm{diff}_Z(r \cdot f, i) = r \cdot \mathrm{diff}_Z(f, i)$. The theorem is a consequence of (18), (14), (19), (10), and (13). Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant n$, then $\mathrm{diff}_Z(r \cdot f, \$_1) = r \cdot \mathrm{diff}_Z(f, \$_1)$. $\mathcal{P}[0]$ by [21, (31)]. For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [2, (11)], [11, (41)]. For every natural number $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. □

(25) Let us consider a natural number $n$, a real number $r$, and a partial function $f$ from $S$ to $T$. Suppose

(i) $1 \leqslant n$, and

(ii) $f$ is differentiable $n$ times on $Z$.

Then $r \cdot f$ is differentiable $n$ times on $Z$. The theorem is a consequence of (18), (14), (24), and (19). Proof: For every natural number $i$ such that $i \leqslant n - 1$ holds $\mathrm{diff}_Z(r \cdot f, i)$ is differentiable on $Z$ by [11, (41)]. □

(26) Let us consider a natural number $n$ and a partial function $f$ from $S$ to $T$. Suppose

(i) $1 \leqslant n$, and

(ii) $f$ is differentiable $n$ times on $Z$.

Let us consider a natural number $i$. Suppose $i \leqslant n$. Then $\mathrm{diff}_Z(-f, i) = -\mathrm{diff}_Z(f, i)$. The theorem is a consequence of (24).

(27) Let us consider a natural number $n$ and a partial function $f$ from $S$ to $T$. Suppose

(i) $1 \leqslant n$, and

(ii) $f$ is differentiable $n$ times on $Z$.

Then $-f$ is differentiable $n$ times on $Z$. The theorem is a consequence of (25).

## References


[1] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[5] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.


Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Hiroshi Imura, Morishige Kimura, and Yasunari Shidama. The differentiable functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):321–327, 2004.
[12] Takaya Nishiyama, Keiji Ohkubo, and Yasunari Shidama. The continuous functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):269–275, 2004.
[13] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[14] Laurent Schwartz. *Cours d'analyse*. Hermann, 1981.
[15] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.
[16] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[17] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[18] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[19] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[20] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[21] Hiroshi Yamazaki and Yasunari Shidama. Algebra of vector functions. *Formalized Mathematics*, 3(**2**):171–175, 1992.

*Received May 19, 2013*

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:41 AM

FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 103–113, 2013
DOI: 10.2478/forma-2013-0012

VERSITA
degruyter.com/view/j/forma

# Polygonal Numbers

Adam Grabowski
Institute of Informatics
University of Białystok
Akademicka 2, 15-267 Białystok
Poland

**Summary.** In the article the formal characterization of triangular numbers (famous from [15] and words "EYPHKA! num $= \Delta + \Delta + \Delta$") [17] is given. Our primary aim was to formalize one of the items (#42) from Wiedijk's Top 100 Mathematical Theorems list [33], namely that the sequence of sums of reciprocals of triangular numbers converges to 2. This Mizar representation was written in 2007. As the Mizar language evolved and attributes with arguments were implemented, we decided to extend these lines and we characterized polygonal numbers.

We formalized centered polygonal numbers, the connection between triangular and square numbers, and also some equalities involving Mersenne primes and perfect numbers. We gave also explicit formula to obtain from the polygonal number its ordinal index. Also selected congruences modulo 10 were enumerated. Our work basically covers the Wikipedia item for triangular numbers and the Online Encyclopedia of Integer Sequences (`http://oeis.org/A000217`).

An interesting related result [16] could be the proof of Lagrange's four-square theorem or Fermat's polygonal number theorem [32].

MSC: 11E25 03B35

Keywords: triangular number; polygonal number; reciprocals of triangular numbers

MML identifier: `NUMPOLY1`, version: `8.1.02 5.17.1179`

The notation and terminology used in this paper have been introduced in the following articles: [27], [24], [14], [4], [5], [11], [6], [7], [1], [30], [22], [28], [2], [26], [21], [3], [8], [13], [34], [18], [35], [9], [19], [20], [25], [29], [31], and [10].

## 1. Preliminaries

The scheme *LNatRealSeq* deals with a unary functor $\mathcal{F}$ yielding a real number and states that



© 2013 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(Print), 1898-9934(Online)

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(Sch. 1) there exists a sequence $s_3$ of real numbers such that for every natural number $n$, $s_3(n) = \mathcal{F}(n)$ and for every sequences $s_1$, $s_2$ of real numbers such that for every natural number $n$, $s_1(n) = \mathcal{F}(n)$ and for every natural number $n$, $s_2(n) = \mathcal{F}(n)$ holds $s_1 = s_2$.

Now we state the proposition:

(1) Let us consider non zero natural numbers $n$, $a$. Then $1 \leqslant a \cdot n$.

Let $n$ be an integer. One can verify that $n \cdot (n-1)$ is even and $n \cdot (n+1)$ is even.

Now we state the proposition:

(2) Let us consider an even integer $n$. Then $\frac{n}{2}$ is an integer.

Let $n$ be an even natural number. One can verify that $\frac{n}{2}$ is natural.

Let $n$ be an odd natural number. One can verify that $n - 1$ is natural.

Let us note that $n - 1$ is even.

In this paper $n$, $s$ denote natural numbers.

Now we state the propositions:

(3) $n \bmod 5 = 0$ or ... or $n \bmod 5 = 4$.

(4) Let us consider a natural number $k$. If $k \neq 0$, then $n \equiv n \bmod k \pmod{k}$.

(5) $n \equiv 0 \pmod{5}$ or ... or $n \equiv 4 \pmod{5}$. The theorem is a consequence of (3) and (4).

Now we state the propositions:

(6) $n \cdot n + n \not\equiv 4 \pmod{5}$.

(7) $n \cdot n + n \not\equiv 3 \pmod{5}$.

Now we state the propositions:

(8) $n \bmod 10 = 0$ or ... or $n \bmod 10 = 9$.

(9) $n \equiv 0 \pmod{10}$ or ... or $n \equiv 9 \pmod{10}$. The theorem is a consequence of (8) and (4).

Note that every natural number which is non trivial is also 2 or greater and every natural number which is 2 or greater is also non trivial and every natural number which is 4 or greater is also 3 or greater and non zero and every natural number which is 4 or greater is also non trivial and there exists a natural number which is 4 or greater and there exists a natural number which is 3 or greater.

## 2. Triangular Numbers

Let $n$ be a natural number. The functor Triangle $n$ yielding a real number is defined by the term

(Def. 1) $\sum \mathrm{idseq}(n)$.

Let $n$ be a number. We say that $n$ is triangular if and only if

(Def. 2) There exists a natural number $k$ such that $n = \mathrm{Triangle}\, k$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Let $n$ be a zero number. Let us observe that Triangle $n$ is zero.

Now we state the propositions:

(10) Triangle$(n+1)$ = Triangle $n+(n+1)$. PROOF: Define $\mathcal{P}$[natural number] $\equiv$ Triangle $\$_1 + (\$_1 + 1)$ = Triangle$(\$_1 + 1)$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [5, (51)], [9, (74)]. For every natural number $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. $\square$

(11) Triangle $1 = 1$.

(12) Triangle $2 = 3$.

(13) Triangle $3 = 6$.

(14) Triangle $4 = 10$. The theorem is a consequence of (10) and (13).

(15) Triangle $5 = 15$. The theorem is a consequence of (10) and (14).

(16) Triangle $6 = 21$. The theorem is a consequence of (10) and (15).

(17) Triangle $7 = 28$. The theorem is a consequence of (10) and (16).

(18) Triangle $8 = 36$. The theorem is a consequence of (10) and (17).

(19) Triangle $n = \frac{n\cdot(n+1)}{2}$. The theorem is a consequence of (10). PROOF: Define $\mathcal{P}$[natural number] $\equiv$ Triangle $\$_1 = \frac{\$_1\cdot(\$_1+1)}{2}$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. $\square$

(20) Triangle $n \geqslant 0$. The theorem is a consequence of (19).

Let $n$ be a natural number. Observe that Triangle $n$ is non negative.

Let $n$ be a non zero natural number. Let us note that Triangle $n$ is positive.

Let $n$ be a natural number. Observe that Triangle $n$ is natural.

Now we state the proposition:

(21) Triangle$(n -' 1) = \frac{n\cdot(n-1)}{2}$. The theorem is a consequence of (1) and (19).

One can check that every number which is triangular is also natural and there exists a number which is triangular and non zero.

Let us consider a triangular number $n$. Now we state the propositions:

(22) $n \not\equiv 7 \pmod{10}$.

(23) $n \not\equiv 9 \pmod{10}$.

(24) $n \not\equiv 2 \pmod{10}$.

(25) $n \not\equiv 4 \pmod{10}$.

Now we state the proposition:

(26) Let us consider a triangular number $n$. Then

(i) $n \equiv 0 \pmod{10}$, or

(ii) $n \equiv 1 \pmod{10}$, or

(iii) $n \equiv 3 \pmod{10}$, or

(iv) $n \equiv 5 \pmod{10}$, or

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(v) $n \equiv 6 \pmod{10}$, or

(vi) $n \equiv 8 \pmod{10}$.

The theorem is a consequence of (9), (24), (25), (22), and (23).

## 3. Polygonal Numbers

Let $s$, $n$ be natural numbers. The functor $\mathrm{Polygon}(s, n)$ yielding an integer is defined by the term

(Def. 3) $\frac{n^{\mathbf{2}} \cdot (s-2) - n \cdot (s-4)}{2}$.

Now we state the propositions:

(27) If $s \geqslant 2$, then $\mathrm{Polygon}(s, n)$ is natural.

(28) $\mathrm{Polygon}(s, n) = \frac{(n \cdot (s-2)) \cdot (n-1)}{2} + n$.

Let $s$ be a natural number and $x$ be an element. We say that $x$ is $s$-gonal if and only if

(Def. 4) There exists a natural number $n$ such that $x = \mathrm{Polygon}(s, n)$.

We say that $x$ is polygonal if and only if

(Def. 5) There exists a natural number $s$ such that $x$ is $s$-gonal.

Now we state the propositions:

(29) $\mathrm{Polygon}(s, 1) = 1$.

(30) $\mathrm{Polygon}(s, 2) = s$.

Let $s$ be a natural number. Note that there exists a number which is $s$-gonal.

Let $s$ be a non zero natural number. One can verify that there exists a number which is non zero and $s$-gonal.

Let $s$ be a natural number. One can verify that every number which is $s$-gonal is also real.

Let $s$ be a non trivial natural number. Let us observe that every number which is $s$-gonal is also natural.

Now we state the proposition:

(31) $\mathrm{Polygon}(s, n+1) - \mathrm{Polygon}(s, n) = (s-2) \cdot n + 1$.

Let $s$ be a natural number and $x$ be an $s$-gonal number. The functor $\mathrm{IndexPoly}(s, x)$ yielding a real number is defined by the term

(Def. 6) $\frac{(\sqrt{(8 \cdot s - 16) \cdot x + (s-4)^{\mathbf{2}}} + s) - 4}{2 \cdot s - 4}$.

Let us consider a non zero natural number $s$ and a non zero $s$-gonal number $x$. Now we state the propositions:

(32) If $x = \mathrm{Polygon}(s, n)$, then $(8 \cdot s - 16) \cdot x + (s-4)^{\mathbf{2}} = ((2 \cdot n) \cdot (s-2) - (s-4))^{\mathbf{2}}$.

(33) If $s \geqslant 4$, then $(8 \cdot s - 16) \cdot x + (s-4)^{\mathbf{2}}$ is square.

(34) If $s \geqslant 4$, then $\mathrm{IndexPoly}(s, x) \in \mathbb{N}$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Now we state the propositions:

(35) Let us consider a non trivial natural number $s$ and an $s$-gonal number $x$. Then $0 \leqslant (8 \cdot s - 16) \cdot x + (s-4)^{\mathbf{2}}$.

(36) Let us consider an odd natural number $n$. If $s \geqslant 2$, then $n \mid \mathrm{Polygon}(s, n)$.

## 4. Centered Polygonal Numbers

Let $s$, $n$ be natural numbers. The functor $\mathrm{CentPoly}(s, n)$ yielding an integer is defined by the term

(Def. 7) $\frac{s \cdot n}{2} \cdot (n-1) + 1$.

Let $s$ be a natural number and $n$ be a non zero natural number. One can verify that $\mathrm{CentPoly}(s, n)$ is natural.

Now we state the propositions:

(37) $\mathrm{CentPoly}(0, n) = 1$.

(38) $\mathrm{CentPoly}(s, 0) = 1$.

(39) $\mathrm{CentPoly}(s, n) = s \cdot \mathrm{Triangle}(n -' 1) + 1$. The theorem is a consequence of (21).

## 5. On the Connection between Triangular and Other Polygonal Numbers

Now we state the propositions:

(40) $\mathrm{Triangle}\, n = \mathrm{Polygon}(3, n)$. The theorem is a consequence of (19).

(41) Let us consider an odd natural number $n$. Then $n \mid \mathrm{Triangle}\, n$. The theorem is a consequence of (36) and (40).

(42) $\mathrm{Triangle}\, n \leqslant \mathrm{Triangle}(n + 1)$. The theorem is a consequence of (10).

(43) Let us consider a natural number $k$. If $k \leqslant n$, then $\mathrm{Triangle}\, k \leqslant \mathrm{Triangle}\, n$. The theorem is a consequence of (42). Proof: Consider $i$ being a natural number such that $n = k + i$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every natural number $n$, $\mathrm{Triangle}\, n \leqslant \mathrm{Triangle}(n + \$_1)$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. □

(44) $n \leqslant \mathrm{Triangle}\, n$. The theorem is a consequence of (10). Proof: Define $\mathcal{P}[\text{natural number}] \equiv \$_1 \leqslant \mathrm{Triangle}\, \$_1$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k + 1]$ by [2, (11)]. For every natural number $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. □

(45) Let us consider a non trivial natural number $n$. Then $n < \mathrm{Triangle}\, n$. The theorem is a consequence of (12) and (10). Proof: Define $\mathcal{P}[\text{natural number}] \equiv \$_1 < \mathrm{Triangle}\, \$_1$. For every non trivial natural number $k$ such

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [2, (16)]. For every non trivial natural number $n$, $\mathcal{P}[n]$ from [23, Sch. 2]. $\square$

(46) If $n \neq 2$, then Triangle $n$ is not prime. The theorem is a consequence of (11), (41), (45), and (19).

Let $n$ be a 3 or greater natural number. Observe that Triangle $n$ is non prime and every 4 or greater natural number which is triangular is also non prime.

Let $s$ be a 4 or greater non zero natural number and $x$ be a non zero $s$-gonal number. Note that $\mathrm{IndexPoly}(s,x)$ is natural.

Now we state the propositions:

(47) Let us consider a 4 or greater natural number $s$ and a non zero $s$-gonal number $x$. If $s \neq 2$, then $\mathrm{Polygon}(s, \mathrm{IndexPoly}(s,x)) = x$. The theorem is a consequence of (35).

(48) 36 is square and triangular. The theorem is a consequence of (19).

Let $n$ be a natural number. One can check that $\mathrm{Polygon}(3,n)$ is natural.

Observe that $\mathrm{Polygon}(3,n)$ is triangular.

Now we state the propositions:

(49) $\mathrm{Polygon}(s,n) = (s-2)\cdot \mathrm{Triangle}(n-'1)+n$. The theorem is a consequence of (21).

(50) $\mathrm{Polygon}(s,n) = (s-3)\cdot \mathrm{Triangle}(n-'1) + \mathrm{Triangle}\, n$. The theorem is a consequence of (21) and (19).

(51) $\mathrm{Polygon}(0,n) = n\cdot(2-n)$.

(52) $\mathrm{Polygon}(1,n) = \frac{n\cdot(3-n)}{2}$.

(53) $\mathrm{Polygon}(2,n) = n$.

Let $s$ be a non trivial natural number and $n$ be a natural number. Observe that $\mathrm{Polygon}(s,n)$ is natural.

One can check that $\mathrm{Polygon}(4,n)$ is square and every natural number which is 3-gonal is also triangular and every natural number which is triangular is also 3-gonal and every natural number which is 4-gonal is also square and every natural number which is square is also 4-gonal.

Now we state the propositions:

(54) $\mathrm{Triangle}(n-'1)+\mathrm{Triangle}\, n = n^{\mathbf{2}}$. The theorem is a consequence of (19).

(55) $\mathrm{Triangle}\, n + \mathrm{Triangle}(n+1) = (n+1)^{\mathbf{2}}$. The theorem is a consequence of (19).

Let $n$ be a natural number. Observe that $\mathrm{Triangle}\, n + \mathrm{Triangle}(n+1)$ is square.

Let us consider a non trivial natural number $n$. Now we state the propositions:

(56) $\frac{1}{3}\cdot \mathrm{Triangle}(3\cdot n -' 1) = \frac{n\cdot(3\cdot n-1)}{2}$.

(57) $\mathrm{Triangle}(2\cdot n -' 1) = \frac{n\cdot(4\cdot n-2)}{2}$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Let $n$, $k$ be natural numbers. The functor $\mathrm{Power}_{\mathbb{N}}(n,k)$ yielding a finite sequence of elements of $\mathbb{R}$ is defined by

(Def. 8) (i) $\mathrm{dom}\, it = \mathrm{Seg}\, k$, and

(ii) for every natural number $i$ such that $i \in \mathrm{dom}\, it$ holds $it(i) = i^n$.

Now we state the proposition:

(58) Let us consider a natural number $k$. Then $\mathrm{Power}_{\mathbb{N}}(n,k+1) = \mathrm{Power}_{\mathbb{N}}(n,k) ^\frown \langle (k+1)^n \rangle$. PROOF: $\mathrm{dom}\, \mathrm{Power}_{\mathbb{N}}(n,k+1) = \mathrm{dom}(\mathrm{Power}_{\mathbb{N}}(n,k) ^\frown \langle (k+1)^n \rangle)$ by [4, (6), (40)]. For every natural number $l$ such that $l \in \mathrm{dom}\, \mathrm{Power}_{\mathbb{N}}(n,k+1)$ holds $(\mathrm{Power}_{\mathbb{N}}(n,k+1))(l) = (\mathrm{Power}_{\mathbb{N}}(n,k) ^\frown \langle (k+1)^n \rangle)(l)$ by [4, (1)], [2, (8)], [4, (6), (42)]. $\square$

Let $n$ be a natural number. Let us observe that $\sum \mathrm{Power}_{\mathbb{N}}(n,0)$ reduces to 0.

Now we state the propositions:

(59) $(\mathrm{Triangle}\, n)^2 = \sum \mathrm{Power}_{\mathbb{N}}(3,n)$. The theorem is a consequence of (19) and (58). PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (\mathrm{Triangle}\, \$_1)^2 = \sum \mathrm{Power}_{\mathbb{N}}(3,\$_1)$. $\mathcal{P}[0]$ by [21, (81)]. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [21, (81), (7)], [12, (27)]. For every natural number $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. $\square$

(60) Let us consider a non trivial natural number $n$. Then $\mathrm{Triangle}\, n + \mathrm{Triangle}(n -' 1) \cdot \mathrm{Triangle}(n+1) = (\mathrm{Triangle}\, n)^2$. The theorem is a consequence of (19).

(61) $(\mathrm{Triangle}\, n)^2 + (\mathrm{Triangle}(n+1))^2 = \mathrm{Triangle}\,(n+1)^2$. The theorem is a consequence of (19).

(62) $(\mathrm{Triangle}(n+1))^2 - (\mathrm{Triangle}\, n)^2 = (n+1)^3$. The theorem is a consequence of (19).

(63) Let us consider a non zero natural number $n$. Then $3 \cdot \mathrm{Triangle}\, n + \mathrm{Triangle}(n -' 1) = \mathrm{Triangle}(2 \cdot n)$. The theorem is a consequence of (19).

(64) $3 \cdot \mathrm{Triangle}\, n + \mathrm{Triangle}(n+1) = \mathrm{Triangle}(2 \cdot n + 1)$. The theorem is a consequence of (19).

Let us consider a non zero natural number $n$. Now we state the propositions:

(65) $(\mathrm{Triangle}(n -' 1) + 6 \cdot \mathrm{Triangle}\, n) + \mathrm{Triangle}(n+1) = 8 \cdot \mathrm{Triangle}\, n + 1$.

(66) $\mathrm{Triangle}\, n + \mathrm{Triangle}(n -' 1) = \frac{((1+2 \cdot n)-1) \cdot n}{2}$.

Now we state the propositions:

(67) $1 + 9 \cdot \mathrm{Triangle}\, n = \mathrm{Triangle}(3 \cdot n + 1)$. The theorem is a consequence of (19).

(68) Let us consider a natural number $m$. Then $\mathrm{Triangle}(n+m) = (\mathrm{Triangle}\, n + \mathrm{Triangle}\, m) + n \cdot m$. The theorem is a consequence of (19).

(69) Let us consider non trivial natural numbers $n$, $m$. Then $\mathrm{Triangle}\, n \cdot \mathrm{Triangle}\, m + \mathrm{Triangle}(n -' 1) \cdot \mathrm{Triangle}(m -' 1) = \mathrm{Triangle}(n \cdot m)$. The theorem is a consequence of (19).

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

## 6. Sets of Polygonal Numbers

Let $s$ be a natural number. The functor PolyNum $s$ yielding a set is defined by the term

(Def. 9) the set of all Polygon$(s, n)$ where $n$ is a natural number.

Let $s$ be a non trivial natural number. Let us observe that the functor PolyNum $s$ yields a subset of $\mathbb{N}$. The functors: the set of all triangular numbers and the set of all square numbers yielding subsets of $\mathbb{N}$ are defined by terms, respectively.

(Def. 10) PolyNum 3.

(Def. 11) PolyNum 4.

Let $s$ be a non trivial natural number. Note that PolyNum $s$ is non empty and the set of all triangular numbers is non empty and the set of all square numbers is non empty and every element of the set of all triangular numbers is triangular and every element of the set of all square numbers is square.

Let us consider a number $x$. Now we state the propositions:

(70) $x \in$ the set of all triangular numbers if and only if $x$ is triangular.

(71) $x \in$ the set of all square numbers if and only if $x$ is square.

## 7. Some Well-known Properties

Now we state the propositions:

(72) $\binom{n+1}{2} = \frac{n \cdot (n+1)}{2}$.

(73) Triangle $n = \binom{n+1}{2}$. The theorem is a consequence of (72) and (19).

(74) Let us consider a non zero natural number $n$. If $n$ is even and perfect, then $n$ is triangular. The theorem is a consequence of (19). Proof: Consider $p$ being a natural number such that $2^p -' 1$ is prime and $n = 2^{p -' 1} \cdot (2^p -' 1)$. $p \neq 0$ by [21, (4)]. □

Let $n$ be a non zero natural number. Let us note that $M_n$ is non zero.

Let $n$ be a number. We say that $n$ is Mersenne if and only if

(Def. 12) There exists a natural number $p$ such that $n = M_p$.

Note that there exists a prime number which is Mersenne and there exists a natural number which is non prime and there exists a natural number which is Mersenne and non prime and every prime number is non zero.

Let $n$ be a Mersenne prime number. One can check that Triangle $n$ is perfect and every non zero natural number which is even and perfect is also triangular.

Now we state the propositions:

(75) $8 \cdot \text{Triangle}\, n + 1 = (2 \cdot n + 1)^{\mathbf{2}}$. The theorem is a consequence of (19).

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(76) If $n$ is triangular, then $8 \cdot n + 1$ is square. The theorem is a consequence of (75).

(77) If $n$ is triangular, then $9 \cdot n + 1$ is triangular. The theorem is a consequence of (67).

(78) If $\mathrm{Triangle}\, n$ is triangular and square, then $\mathrm{Triangle}((4 \cdot n) \cdot (n+1))$ is triangular and square. The theorem is a consequence of (19).

Let us observe that the set of all triangular numbers is infinite and the set of all square numbers is infinite and there exists a natural number which is triangular, square, and non zero.

Now we state the proposition:

(79) 0 is triangular and square.

Let us observe that every number which is zero is also triangular and square.

Now we state the proposition:

(80) 1 is triangular and square. The theorem is a consequence of (11).

Now we state the propositions:

(81) Square triangular number:
36 is triangular and square. The theorem is a consequence of (11), (80), (78), and (18).

(82) 1225 is triangular and square. The theorem is a consequence of (19).

Let $n$ be a triangular natural number. One can check that $9 \cdot n + 1$ is triangular.

Let us note that $8 \cdot n + 1$ is square.

## 8. Reciprocals of Triangular Numbers

Let $a$ be a real number. One can verify that $\lim\{a\}_{n \in \mathbb{N}}$ reduces to $a$.

The functor ReciTriang yielding a sequence of real numbers is defined by

(Def. 13) Let us consider a natural number $i$. Then $it(i) = \frac{1}{\mathrm{Triangle}\, i}$.

Let us note that $(\mathrm{ReciTriang})(0)$ reduces to 0.

Now we state the propositions:

(83) $\frac{1}{\mathrm{Triangle}\, n} = \frac{2}{n \cdot (n+1)}$. The theorem is a consequence of (19).

(84) $(\sum_{\alpha=0}^{\kappa} (\mathrm{ReciTriang})(\alpha))_{\kappa \in \mathbb{N}}(n) = 2 - \frac{2}{n+1}$. The theorem is a consequence of (83). Proof: Define $\mathcal{P}[\text{natural number}] \equiv (\sum_{\alpha=0}^{\kappa} (\mathrm{ReciTriang})(\alpha))_{\kappa \in \mathbb{N}}(\$_1)$ $= 2 - \frac{2}{\$_1 + 1}$. $\mathcal{P}[0]$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number $k$, $\mathcal{P}[k]$ from [2, Sch. 2]. $\square$

The functors: SumsReciTriang and $\mathrm{GeoSeq}(a, b)$ yielding sequences of real numbers are defined by conditions, respectively.

(Def. 14) Let us consider a natural number $n$. Then $(\mathrm{SumsReciTriang})(n) = 2 - \frac{2}{n+1}$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(Def. 15) Let us consider a natural number $n$. Then $(\mathrm{GeoSeq}(a,b))(n) = \frac{a}{n+b}$.

Let $a$, $b$ be real numbers.

Now we state the propositions:

(85) Let us consider real numbers $a$, $b$. Suppose $b > 0$. Then

(i) $\mathrm{GeoSeq}(a,b)$ is convergent, and

(ii) $\lim \mathrm{GeoSeq}(a,b) = 0$.

(86) $\mathrm{SumsReciTriang} = \{2\}_{n\in\mathbb{N}} + -\mathrm{GeoSeq}(2,1)$. PROOF: For every natural number $k$, $(\mathrm{SumsReciTriang})(k) = (\{2\}_{n\in\mathbb{N}})(k) + (-\mathrm{GeoSeq}(2,1))(k)$ by [19, (57)]. $\square$

(87) (i) SumsReciTriang is convergent, and

(ii) $\lim \mathrm{SumsReciTriang} = 2$.

The theorem is a consequence of (85) and (86).

(88) $(\sum_{\alpha=0}^{\kappa}(\mathrm{ReciTriang})(\alpha))_{\kappa\in\mathbb{N}} = \mathrm{SumsReciTriang}$.

Now we state the proposition:

(89) RECIPROCALS OF TRIANGULAR NUMBERS:
$\sum \mathrm{ReciTriang} = 2$.

## References


[1] Kenichi Arai and Hiroyuki Okazaki. Properties of primes and multiplicative group of a field. *Formalized Mathematics*, 17(**2**):151–155, 2009. doi:10.2478/v10037-009-0017-7.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[9] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[12] Yuzhong Ding and Xiquan Liang. Solving roots of polynomial equation of degree 2 and 3 with complex coefficients. *Formalized Mathematics*, 12(**2**):85–92, 2004.

[13] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.

[14] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Operations of points on elliptic curve in projective coordinates. *Formalized Mathematics*, 20(**1**):87–95, 2012. doi:10.2478/v10037-012-0012-2.

[15] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Springer, New York, 1986. English translation.


Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

[16] Richard K. Guy. Every number is expressible as a sum of how many polygonal numbers? *American Mathematical Monthly*, 101:169–172, 1994.

[17] Thomas L. Heath. *A History of Greek Mathematics: From Thales to Euclid, Vol. I.* Courier Dover Publications, 1921.

[18] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[19] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[20] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.

[21] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[22] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[23] Robert Milewski. Natural numbers. *Formalized Mathematics*, 7(**1**):19–22, 1998.

[24] Adam Naumowicz. Conjugate sequences, bounded complex sequences and convergent complex sequences. *Formalized Mathematics*, 6(**2**):265–268, 1997.

[25] Konrad Raczkowski and Andrzej Nędzusiak. Series. *Formalized Mathematics*, 2(**4**):449–452, 1991.

[26] Marco Riccardi. The perfect number theorem and Wilson's theorem. *Formalized Mathematics*, 17(**2**):123–128, 2009. doi:10.2478/v10037-009-0013-y.

[27] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[28] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[29] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[30] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[32] André Weil. *Number Theory. An Approach through History from Hammurapi to Legendre.* Birkhäuser, Boston, Mass., 1983.

[33] Freek Wiedijk. Formalizing 100 theorems.

[34] Freek Wiedijk. Pythagorean triples. *Formalized Mathematics*, 9(**4**):809–812, 2001.

[35] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.


*Received May 19, 2013*

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 115–125, 2013
DOI: 10.2478/forma-2013-0013

VERSITA
degruyter.com/view/j/forma

# Gaussian Integers[1]

Yuichi Futa
Japan Advanced Institute
of Science and Technology
Ishikawa, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Daichi Mizushima[2]
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

**Summary.** Gaussian integer is one of basic algebraic integers. In this article we formalize some definitions about Gaussian integers [27]. We also formalize ring (called Gaussian integer ring), $\mathbb{Z}$-module and $\mathbb{Z}$-algebra generated by Gaussian integer mentioned above. Moreover, we formalize some definitions about Gaussian rational numbers and Gaussian rational number field. Then we prove that the Gaussian rational number field and a quotient field of the Gaussian integer ring are isomorphic.

MSC: 11R04 03B35

Keywords: formalization of Gaussian integers; algebraic integers

MML identifier: `GAUSSINT`, version: `8.1.02 5.17.1179`

The notation and terminology used in this paper have been introduced in the following articles: [5], [1], [2], [6], [12], [11], [7], [8], [18], [24], [23], [16], [19], [21], [3], [9], [20], [14], [4], [28], [25], [22], [26], [15], [17], [10], and [13].

## 1. Gaussian Integer Ring

Now we state the proposition:

(1) Let us consider natural numbers $x$, $y$. If $x+y=1$, then $x=1$ and $y=0$ or $x=0$ and $y=1$. Proof: $x \leqslant 1$. $\square$

[1]This work was supported by JSPS KAKENHI 21240001 and 22300285.

[2]This research was presented during the 2012 International Symposium on Information Theory and its Applications (ISITA2012) in Honolulu, USA.

© 2013 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(Print), 1898-9934(Online)



Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Let $z$ be a complex. We say that $z$ is Gaussian integer if and only if

(Def. 1) $\Re(z)$, $\Im(z) \in \mathbb{Z}$.

Note that every integer is Gaussian integer.

An element of Gaussian integers is a Gaussian integer complex. Let $z$ be an element of Gaussian integers. Note that $\Re(z)$ is integer and $\Im(z)$ is integer.

Let $z_1$, $z_2$ be elements of Gaussian integers. One can verify that $z_1 + z_2$ is Gaussian integer and $z_1 - z_2$ is Gaussian integer and $z_1 \cdot z_2$ is Gaussian integer and $i$ is Gaussian integer.

Let $z$ be an element of Gaussian integers. Let us note that $-z$ is Gaussian integer and $\overline{z}$ is Gaussian integer.

Let $n$ be an integer. One can check that $n \cdot z$ is Gaussian integer.

The set of Gaussian integers yielding a subset of $\mathbb{C}$ is defined by the term

(Def. 2) the set of all $z$ where $z$ is an element of Gaussian integers.

Note that the set of Gaussian integers is non empty.

Let $i$ be an integer. Let us observe that $i$($\in$ the set of Gaussian integers) reduces to $i$.

Let us consider a set $x$. Now we state the propositions:

(2) If $x \in$ the set of Gaussian integers, then $x$ is an element of Gaussian integers.

(3) If $x$ is an element of Gaussian integers, then $x \in$ the set of Gaussian integers.

The addition of Gaussian integers yielding a binary operation on the set of Gaussian integers is defined by the term

(Def. 3) $+_{\mathbb{C}} \restriction$ the set of Gaussian integers.

The multiplication of Gaussian integers yielding a binary operation on the set of Gaussian integers is defined by the term

(Def. 4) $\cdot_{\mathbb{C}} \restriction$ the set of Gaussian integers.

The scalar multiplication of Gaussian integers yielding a function from $\mathbb{Z} \times$ the set of Gaussian integers into the set of Gaussian integers is defined by the term

(Def. 5) $\cdot_{\mathbb{C}}\restriction$($\mathbb{Z} \times$ the set of Gaussian integers).

Now we state the propositions:

(4) Let us consider elements $z$, $w$ of Gaussian integers. Then (the addition of Gaussian integers)$(z, w) = z + w$.

(5) Let us consider an element $z$ of Gaussian integers and an integer $i$. Then (the scalar multiplication of Gaussian integers)$(i, z) = i \cdot z$.

The Gaussian integer module yielding a strict non empty $\mathbb{Z}$-module structure is defined by the term

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(Def. 6) $\langle$the set of Gaussian integers, $0(\in$ the set of Gaussian integers$)$, the addition of Gaussian integers, the scalar multiplication of Gaussian integers$\rangle$.

Observe that the Gaussian integer module is Abelian add-associative right zeroed right complementable scalar distributive vector distributive scalar associative and scalar unital.

Now we state the proposition:

(6) Let us consider elements $z$, $w$ of Gaussian integers. Then (the multiplication of Gaussian integers)$(z, w) = z \cdot w$.

The Gaussian integer ring yielding a strict non empty double loop structure is defined by the term

(Def. 7) $\langle$the set of Gaussian integers, the addition of Gaussian integers, the multiplication of Gaussian integers, $1(\in$ the set of Gaussian integers$)$, $0(\in$ the set of Gaussian integers$)\rangle$.

One can check that the Gaussian integer ring is Abelian add-associative right zeroed right complementable associative well unital and distributive, and the Gaussian integer ring is integral domain-like, and the Gaussian integer ring is commutative.

Now we state the propositions:

(7) Every element of the Gaussian integer ring is an element of Gaussian integers.

(8) Every element of Gaussian integers is an element of the Gaussian integer ring.

## 2. $\mathbb{Z}$-Algebra

We consider $\mathbb{Z}$-algebra structures which extend double loop structures and $\mathbb{Z}$-module structures and are systems

$$\langle \text{a carrier, a multiplication, an addition, an external multiplication,}$$
$$\text{a one, a zero}\rangle$$

where the carrier is a set, the multiplication and the addition are binary operations on the carrier, the external multiplication is a function from $\mathbb{Z} \times$ the carrier into the carrier, the one and the zero are elements of the carrier.

Let us observe that there exists a $\mathbb{Z}$-algebra structure which is non empty.

Let $I_1$ be a non empty $\mathbb{Z}$-algebra structure. We say that $I_1$ is vector associative if and only if

(Def. 8) Let us consider elements $x$, $y$ of $I_1$ and an integer $a_1$. Then $a_1 \cdot (x \cdot y) = (a_1 \cdot x) \cdot y$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Let us observe that $\langle$the set of Gaussian integers, (the multiplication of Gaussian integers), (the addition of Gaussian integers), (the scalar multiplication of Gaussian integers), $1(\in$ the set of Gaussian integers), $0(\in$ the set of Gaussian integers)$\rangle$ is non empty and $\langle$the set of Gaussian integers, (the multiplication of Gaussian integers), (the addition of Gaussian integers), (the scalar multiplication of Gaussian integers), $1(\in$ the set of Gaussian integers), $0(\in$ the set of Gaussian integers)$\rangle$ is strict Abelian add-associative right zeroed right complementable commutative associative right unital right distributive vector associative scalar associative vector distributive and scalar distributive and there exists a non empty $\mathbb{Z}$-algebra structure which is strict, Abelian, add-associative, right zeroed, right complementable, commutative, associative, right unital, right distributive, vector associative, scalar associative, vector distributive, and scalar distributive.

A $\mathbb{Z}$-algebra is an Abelian add-associative right zeroed right complementable commutative associative right unital right distributive vector associative scalar associative vector distributive scalar distributive non empty $\mathbb{Z}$-algebra structure. Now we state the proposition:

(9) $\langle$the set of Gaussian integers, (the multiplication of Gaussian integers), (the addition of Gaussian integers), (the scalar multiplication of Gaussian integers), $1(\in$ the set of Gaussian integers), $0(\in$ the set of Gaussian integers)$\rangle$ is a right complementable associative commutative right distributive right unital Abelian add-associative right zeroed vector distributive scalar distributive scalar associative strict vector associative non empty $\mathbb{Z}$-algebra structure.

One can verify that $\mathbb{Z}$ is denumerable and the set of Gaussian integers is denumerable and the Gaussian integer ring is non degenerated.

## 3. Quotient Field of Gaussian Integer Ring

The Gaussian number field yielding a strict non empty double loop structure is defined by the term

(Def. 9) The field of quotients of the Gaussian integer ring.

Observe that the Gaussian number field is non degenerated almost left invertible strict Abelian associative and distributive.

Let $z$ be a complex. We say that $z$ is Gaussian rational if and only if

(Def. 10) $\Re(z)$, $\Im(z) \in \mathbb{Q}$.

One can verify that every rational number is Gaussian rational.

An element of Gaussian rationals is a Gaussian rational complex. Let $z$ be an element of Gaussian rationals. One can verify that $\Re(z)$ is rational and $\Im(z)$ is rational.

Let $z_1$, $z_2$ be elements of Gaussian rationals. Observe that $z_1+z_2$ is Gaussian rational and $z_1 - z_2$ is Gaussian rational and $z_1 \cdot z_2$ is Gaussian rational.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Let $z$ be an element of Gaussian rationals and $n$ be a rational number. One can check that $n \cdot z$ is Gaussian rational.

Let us observe that $-z$ is Gaussian rational and $z^{-1}$ is Gaussian rational.

The set of Gaussian rationals yielding a subset of $\mathbb{C}$ is defined by the term

(Def. 11) the set of all $z$ where $z$ is an element of Gaussian rationals.

Let us observe that the set of Gaussian rationals is non empty and every element of Gaussian integers is Gaussian rational.

Let us consider a set $x$. Now we state the propositions:

(10) If $x \in$ the set of Gaussian rationals, then $x$ is an element of Gaussian rationals.

(11) If $x$ is an element of Gaussian rationals, then $x \in$ the set of Gaussian rationals.

Now we state the proposition:

(12) Let us consider an element $p$ of Gaussian rationals. Then there exist elements $x$, $y$ of Gaussian integers such that

(i) $y \neq 0$, and

(ii) $p = \frac{x}{y}$.

The addition of Gaussian rationals yielding a binary operation on the set of Gaussian rationals is defined by the term

(Def. 12) $+_{\mathbb{C}} \restriction$ the set of Gaussian rationals.

The multiplication of Gaussian rationals yielding a binary operation on the set of Gaussian rationals is defined by the term

(Def. 13) $\cdot_{\mathbb{C}} \restriction$ the set of Gaussian rationals.

## 4. Rational Field

Let $i$ be an integer. One can check that $i(\in \mathbb{Q})$ reduces to $i$.

The rational number field yielding a strict non empty double loop structure is defined by the term

(Def. 14) $\langle \mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, 1(\in \mathbb{Q}), 0(\in \mathbb{Q}) \rangle$.

Now we state the propositions:

(13) (i) the carrier of the rational number field is a subset of the carrier of $\mathbb{R}_{\rm F}$, and

(ii) the addition of the rational number field $=$ (the addition of $\mathbb{R}_{\rm F}$) $\restriction$ (the carrier of the rational number field), and

(iii) the multiplication of the rational number field $=$ (the multiplication of $\mathbb{R}_{\rm F}$) $\restriction$ (the carrier of the rational number field), and

(iv) $1_\alpha = 1_{\mathbb{R}_{\rm F}}$, and

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(v) $0_\alpha = 0_{\mathbb{R}_\mathrm{F}}$, and

(vi) the rational number field is right complementable, commutative, almost left invertible, and non degenerated,

where $\alpha$ is the rational number field. PROOF: Every element of the rational number field is right complementable. For every element $v$ of the rational number field such that $v \neq 0_\alpha$ holds $v$ is left invertible, where $\alpha$ is the rational number field. □

(14) The rational number field is a subfield of $\mathbb{R}_\mathrm{F}$.

Let us note that the rational number field is add-associative right zeroed right complementable Abelian commutative associative left and right unital distributive almost left invertible and non degenerated and the rational number field is well unital and every element of the rational number field is rational.

Let $x$ be an element of the rational number field and $y$ be a rational number. We identify $-y$ with $-x$ where $x = y$. Now we state the propositions:

(15) Let us consider an element $x$ of the rational number field and a rational number $x_1$. If $x \neq 0_\alpha$ and $x_1 = x$, then $x^{-1} = {x_1}^{-1}$, where $\alpha$ is the rational number field.

(16) Let us consider elements $x$, $y$ of the rational number field and rational numbers $x_1$, $y_1$. Suppose

(i) $x_1 = x$, and

(ii) $y_1 = y$, and

(iii) $y \neq 0_\alpha$.

Then $\frac{x}{y} = \frac{x_1}{y_1}$, where $\alpha$ is the rational number field. The theorem is a consequence of (15).

Let us consider a field $K$, a subfield $K_1$ of $K$, elements $x$, $y$ of $K$, and elements $x_1$, $y_1$ of $K_1$. Now we state the propositions:

(17) If $x = x_1$ and $y = y_1$, then $x + y = x_1 + y_1$.

(18) If $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.

Now we state the proposition:

(19) Let us consider a field $K$, a subfield $K_1$ of $K$, an element $x$ of $K$, and an element $x_1$ of $K_1$. If $x = x_1$, then $-x = -x_1$. The theorem is a consequence of (17).

Let us consider a field $K$, a subfield $K_1$ of $K$, elements $x$, $y$ of $K$, and elements $x_1$, $y_1$ of $K_1$. Now we state the propositions:

(20) If $x = x_1$ and $y = y_1$, then $x - y = x_1 - y_1$.

(21) If $x = x_1$ and $x \neq 0_K$, then $x^{-1} = {x_1}^{-1}$.

(22) If $x = x_1$ and $y = y_1$ and $y \neq 0_K$, then $\frac{x}{y} = \frac{x_1}{y_1}$.

Let us consider a subfield $K_1$ of the rational number field. Now we state the propositions:

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(23) $\mathbb{N} \subseteq$ the carrier of $K_1$.

(24) $\mathbb{Z} \subseteq$ the carrier of $K_1$.

(25) The carrier of $K_1 =$ the carrier of the rational number field.

Now we state the proposition:

(26) Let us consider a strict subfield $K_1$ of the rational number field. Then $K_1 =$ the rational number field. The theorem is a consequence of (25).

One can verify that the rational number field is prime.

## 5. Gaussian Rational Number Field

Let $i$ be a rational number. Note that $i(\in$ the set of Gaussian rationals) reduces to $i$.

The scalar multiplication of Gaussian rationals yielding a function from (the carrier of the rational number field) $\times$ the set of Gaussian rationals into the set of Gaussian rationals is defined by the term

(Def. 15) $\cdot_{\mathbb{C}}\restriction$((the carrier of the rational number field)$\times$the set of Gaussian rationals).

Now we state the propositions:

(27) Let us consider elements $z$, $w$ of Gaussian rationals. Then (the addition of Gaussian rationals)$(z, w) = z + w$.

(28) Let us consider an element $z$ of Gaussian rationals and an element $i$ of $\mathbb{Q}$. Then (the scalar multiplication of Gaussian rationals)$(i, z) = i \cdot z$.

The Gaussian rational module yielding a strict non empty vector space structure over the rational number field is defined by the term

(Def. 16) $\langle$the set of Gaussian rationals, the addition of Gaussian rationals, $0(\in$ the set of Gaussian rationals), the scalar multiplication of Gaussian rationals$\rangle$.

Observe that the Gaussian rational module is scalar distributive vector distributive scalar associative scalar unital add-associative right zeroed right complementable and Abelian.

Now we state the proposition:

(29) Let us consider elements $z, w$ of Gaussian rationals. Then (the multiplication of Gaussian rationals)$(z, w) = z \cdot w$.

The Gaussian rational ring yielding a strict non empty double loop structure is defined by the term

(Def. 17) $\langle$the set of Gaussian rationals, the addition of Gaussian rationals, the multiplication of Gaussian rationals, $1(\in$ the set of Gaussian rationals), $0(\in$ the set of Gaussian rationals)$\rangle$.

Let us note that the Gaussian rational ring is add-associative right zeroed right complementable Abelian commutative associative well unital distributive almost left invertible and non degenerated.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Now we state the proposition:

(30) There exists a function $I$ from the Gaussian number field into the Gaussian rational ring such that

(i) for every element $z$ such that $z \in$ the carrier of the Gaussian number field there exist elements $x$, $y$ of Gaussian integers and there exists an element $u$ of Q(the Gaussian integer ring) such that $y \neq 0$ and $u = \langle x, y \rangle$ and $z = \mathrm{QClass}(u)$ and $I(z) = \frac{x}{y}$, and

(ii) $I$ is one-to-one and onto, and

(iii) for every elements $x$, $y$ of the Gaussian number field, $I(x + y) = I(x) + I(y)$ and $I(x \cdot y) = I(x) \cdot I(y)$, and

(iv) $I(0_{\alpha}) = 0$, and

(v) $I(1_{\alpha}) = 1$,

where $\alpha$ is the Gaussian number field. The theorem is a consequence of (2), (10), (12), (3), (6), (4), (27), and (29). PROOF: Define $\mathcal{P}[\text{element}, \text{element}] \equiv$ there exist elements $x$, $y$ of Gaussian integers and there exists an element $u$ of Q(the Gaussian integer ring) such that $y \neq 0$ and $u = \langle x, y \rangle$ and $\$_1 = \mathrm{QClass}(u)$ and $\$_2 = \frac{x}{y}$. For every element $z$ such that $z \in$ the carrier of the Gaussian number field there exists an element $w$ such that $w \in$ the carrier of the Gaussian rational ring and $\mathcal{P}[z, w]$. Consider $I$ being a function from the Gaussian number field into the Gaussian rational ring such that for every element $z$ such that $z \in$ the carrier of the Gaussian number field holds $\mathcal{P}[z, I(z)]$ from [8, Sch. 1]. For every elements $z_1$, $z_2$ of the Gaussian number field, $I(z_1 + z_2) = I(z_1) + I(z_2)$ and $I(z_1 \cdot z_2) = I(z_1) \cdot I(z_2)$ by [20, (9), (5), (10)]. $\square$

## 6. Gaussian Integer Ring is Euclidean

Let $a_1$, $b_1$ be elements of Gaussian integers. We say that $a_1$ divides $b_1$ if and only if

(Def. 18) There exists an element $c$ of Gaussian integers such that $b_1 = a_1 \cdot c$.

Note that the predicate is reflexive.

Let us consider elements $a_1$, $b_1$ of the Gaussian integer ring and elements $a_2$, $b_2$ of Gaussian integers. Now we state the propositions:

(31) If $a_1 = a_2$ and $b_1 = b_2$, then if $a_1 \mid b_1$, then $a_2$ divides $b_2$.

(32) If $a_1 = a_2$ and $b_1 = b_2$, then if $a_2$ divides $b_2$, then $a_1 \mid b_1$.

Let $z$ be an element of Gaussian rationals. Observe that the functor $\overline{z}$ yields an element of Gaussian rationals. The functor Norm $z$ yielding a rational number is defined by the term

(Def. 19) $z \cdot \overline{z}$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Let us observe that Norm $z$ is non negative.

Let $z$ be an element of Gaussian integers. Observe that Norm $z$ is natural.

Now we state the propositions:

(33) Let us consider an element $x$ of Gaussian rationals. Then $\text{Norm}\,\overline{x} = \text{Norm}\,x$.

(34) Let us consider elements $x$, $y$ of Gaussian rationals. Then $\text{Norm}(x \cdot y) = \text{Norm}\,x \cdot \text{Norm}\,y$.

Let us consider an element $x$ of Gaussian integers. Now we state the propositions:

(35) $\text{Norm}\,x = 1$ if and only if $x = 1$ or $x = -1$ or $x = i$ or $x = -i$.

(36) If $\text{Norm}\,x = 0$, then $x = 0$.

Let $z$ be an element of Gaussian integers. We say that $z$ is unit of Gaussian integers if and only if

(Def. 20) $\text{Norm}\,z = 1$.

Let $x$, $y$ be elements of Gaussian integers. We say that $x$ is associated to $y$ if and only if

(Def. 21) (i) $x$ divides $y$, and

(ii) $y$ divides $x$.

Let us observe that the predicate is symmetric.

Let us consider elements $a_1$, $b_1$ of the Gaussian integer ring and elements $a_2$, $b_2$ of Gaussian integers. Now we state the propositions:

(37) If $a_1 = a_2$ and $b_1 = b_2$, then if $a_1$ is associated to $b_1$, then $a_2$ is associated to $b_2$.

(38) If $a_1 = a_2$ and $b_1 = b_2$, then if $a_2$ is associated to $b_2$, then $a_1$ is associated to $b_1$.

Now we state the propositions:

(39) Let us consider an element $z$ of the Gaussian integer ring and an element $z_3$ of Gaussian integers. If $z_3 = z$, then $z$ is unital iff $z_3$ is unit of Gaussian integers. The theorem is a consequence of (2), (6), (34), (35), and (3). Proof: There exists an element $w$ of the Gaussian integer ring such that $1_\alpha = z \cdot w$, where $\alpha$ is the Gaussian integer ring. □

(40) Let us consider elements $x$, $y$ of Gaussian integers. Then $x$ is associated to $y$ if and only if there exists an element $c$ of Gaussian integers such that $c$ is unit of Gaussian integers and $x = c \cdot y$. The theorem is a consequence of (3), (38), (2), (39), (6), and (37).

(41) Let us consider an element $x$ of Gaussian integers. Suppose

(i) $\Re(x) \neq 0$, and

(ii) $\Im(x) \neq 0$, and

(iii) $\Re(x) \neq \Im(x)$, and

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(iv) $-\Re(x) \neq \Im(x)$.

Then $\overline{x}$ is not associated to $x$. The theorem is a consequence of (40) and (35).

(42) Let us consider elements $x$, $y$, $z$ of Gaussian integers. Suppose

(i) $x$ is associated to $y$, and

(ii) $y$ is associated to $z$.

Then $x$ is associated to $z$. The theorem is a consequence of (40) and (34).

Let us consider elements $x$, $y$ of Gaussian integers. Now we state the propositions:

(43) If $x$ is associated to $y$, then $\overline{x}$ is associated to $\overline{y}$.

(44) Suppose $\Re(y) \neq 0$ and $\Im(y) \neq 0$ and $\Re(y) \neq \Im(y)$ and $-\Re(y) \neq \Im(y)$ and $\overline{x}$ is associated to $y$. Then

(i) does not $x$ divide $y$, and

(ii) does not $y$ divide $x$.

Let $p$ be an element of Gaussian integers. We say that $p$ is Gaussian prime if and only if

(Def. 22) (i) $\operatorname{Norm} p > 1$, and

(ii) for every element $z$ of Gaussian integers, does not $z$ divide $p$ or $z$ is unit of Gaussian integers or $z$ is associated to $p$.

Let us consider an element $q$ of Gaussian integers. Now we state the propositions:

(45) If $\operatorname{Norm} q$ is a prime number and $\operatorname{Norm} q \neq 2$, then $\Re(q) \neq 0$ and $\Im(q) \neq 0$ and $\Re(q) \neq \Im(q)$ and $-\Re(q) \neq \Im(q)$.

(46) If $\operatorname{Norm} q$ is a prime number, then $q$ is Gaussian prime.

Now we state the propositions:

(47) Let us consider an element $q$ of Gaussian rationals. Then $\operatorname{Norm} q = |\Re(q)|^{\mathbf{2}} + |\Im(q)|^{\mathbf{2}}$.

(48) Let us consider an element $q$ of $\mathbb{R}$. Then there exists an element $m$ of $\mathbb{Z}$ such that $|q - m| \leqslant \frac{1}{2}$.

One can check that the Gaussian integer ring is Euclidean.

## References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[5] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[6] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[12] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Set of points on elliptic curve in projective coordinates. *Formalized Mathematics*, 19(**3**):131–138, 2011. doi:10.2478/v10037-011-0021-6.
[13] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.
[14] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.
[15] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[16] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[17] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[18] Christoph Schwarzweller. The correctness of the generic algorithms of Brown and Henrici concerning addition and multiplication in fraction fields. *Formalized Mathematics*, 6(**3**): 381–388, 1997.
[19] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[20] Christoph Schwarzweller. The field of quotients over an integral domain. *Formalized Mathematics*, 7(**1**):69–79, 1998.
[21] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.
[22] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[23] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[24] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[25] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[26] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[27] André Weil. *Number Theory for Beginners*. Springer-Verlag, 1979.
[28] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

*Received May 19, 2013*

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 127–131, 2013
DOI: 10.2478/forma-2013-0014

VERSITA
degruyter.com/view/j/forma

# Commutativeness of Fundamental Groups of Topological Groups

Artur Korniłowicz
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

**Summary.** In this article we prove that fundamental groups based at the unit point of topological groups are commutative [11].

MSC: 55Q52 03B35

Keywords: fundamental group; topological group

MML identifier: TOPALG_7, version: 8.1.02 5.17.1179

The notation and terminology used in this paper have been introduced in the following articles: [3], [19], [9], [10], [16], [20], [4], [5], [22], [23], [21], [1], [6], [17], [18], [2], [25], [26], [24], [15], [12], [13], [8], [14], and [7].

Let $A$ be a non empty set, $x$ be an element, and $a$ be an element of $A$. Let us observe that $(A \longmapsto x)(a)$ reduces to $x$.

Let $A$, $B$ be non empty topological spaces, $C$ be a set, and $f$ be a function from $A \times B$ into $C$. Let $b$ be an element of $B$. Let us note that the functor $f(a, b)$ yields an element of $C$. Let $G$ be a multiplicative magma and $g$ be an element of $G$. We say that $g$ is unital if and only if

(Def. 1) $g = \mathbf{1}_G$.

One can check that $\mathbf{1}_G$ is unital.

Let $G$ be a unital multiplicative magma. Let us note that there exists an element of $G$ which is unital.

Let $g$ be an element of $G$ and $h$ be a unital element of $G$. One can check that $g \cdot h$ reduces to $g$. One can check that $h \cdot g$ reduces to $g$.

Let $G$ be a group. One can verify that $(\mathbf{1}_G)^{-1}$ reduces to $\mathbf{1}_G$.

The scheme *TopFuncEx* deals with non empty topological spaces $\mathcal{S}$, $\mathcal{T}$ and a non empty set $\mathcal{X}$ and a binary functor $\mathcal{F}$ yielding an element of $\mathcal{X}$ and states that

© 2013 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(Print), 1898-9934(Online)



Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(Sch. 1) There exists a function $f$ from $\mathcal{S} \times \mathcal{T}$ into $\mathcal{X}$ such that for every point $s$ of $\mathcal{S}$ for every point $t$ of $\mathcal{T}$, $f(s,t) = \mathcal{F}(s,t)$.

The scheme *TopFuncEq* deals with non empty topological spaces $\mathcal{S}$, $\mathcal{T}$ and a non empty set $\mathcal{X}$ and a binary functor $\mathcal{F}$ yielding an element of $\mathcal{X}$ and states that

(Sch. 2) For every functions $f$, $g$ from $\mathcal{S} \times \mathcal{T}$ into $\mathcal{X}$ such that for every point $s$ of $\mathcal{S}$ and for every point $t$ of $\mathcal{T}$, $f(s,t) = \mathcal{F}(s,t)$ and for every point $s$ of $\mathcal{S}$ and for every point $t$ of $\mathcal{T}$, $g(s,t) = \mathcal{F}(s,t)$ holds $f = g$.

Let $X$ be a non empty set, $T$ be a non empty multiplicative magma, and $f$, $g$ be functions from $X$ into $T$. The functor $f \cdot g$ yielding a function from $X$ into $T$ is defined by

(Def. 2) Let us consider an element $x$ of $X$. Then $it(x) = f(x) \cdot g(x)$.

Now we state the proposition:

(1) Let us consider a non empty set $X$, an associative non empty multiplicative magma $T$, and functions $f$, $g$, $h$ from $X$ into $T$. Then $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.

Let $X$ be a non empty set, $T$ be a commutative non empty multiplicative magma, and $f$, $g$ be functions from $X$ into $T$. Observe that the functor $f \cdot g$ is commutative.

Let $T$ be a non empty topological group structure, $t$ be a point of $T$, and $f$, $g$ be loops of $t$. The functor $f \bullet g$ yielding a function from $\mathbb{I}$ into $T$ is defined by the term

(Def. 3) $f \cdot g$.

In this paper $T$ denotes a continuous unital topological space-like non empty topological group structure, $x$, $y$ denote points of $\mathbb{I}$, $s$, $t$ denote unital points of $T$, $f$, $g$ denote loops of $t$, and $c$ denotes a constant loop of $t$.

Let us consider $T$, $t$, $f$, and $g$. One can check that the functor $f \bullet g$ yields a loop of $t$. Let $T$ be an inverse-continuous semi topological group. Observe that $\cdot_T^{-1}$ is continuous.

Let $T$ be a semi topological group, $t$ be a point of $T$, and $f$ be a loop of $t$. The functor $f^{-1}$ yielding a function from $\mathbb{I}$ into $T$ is defined by the term

(Def. 4) $\cdot_T^{-1} \cdot f$.

Let us consider a semi topological group $T$, a point $t$ of $T$, and a loop $f$ of $t$. Now we state the propositions:

(2) $(f^{-1})(x) = f(x)^{-1}$.

(3) $(f^{-1})(x) \cdot f(x) = \mathbf{1}_T$.

(4) $f(x) \cdot (f^{-1})(x) = \mathbf{1}_T$.

Let $T$ be an inverse-continuous semi topological group, $t$ be a unital point of $T$, and $f$ be a loop of $t$. One can check that the functor $f^{-1}$ yields a loop of

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

$t$. Let $s$, $t$ be points of $\mathbb{I}$. One can check that the functor $s \cdot t$ yields a point of $\mathbb{I}$. The functor $\otimes_{\mathbb{R}^1}$ yielding a function from $\mathbb{R}^{\mathbf{1}} \times \mathbb{R}^{\mathbf{1}}$ into $\mathbb{R}^{\mathbf{1}}$ is defined by

(Def. 5) Let us consider points $x$, $y$ of $\mathbb{R}^{\mathbf{1}}$. Then $it(x, y) = x \cdot y$.

Observe that $\otimes_{\mathbb{R}^1}$ is continuous.

Now we state the proposition:

(5) $(\mathbb{R}^{\mathbf{1}} \times \mathbb{R}^{\mathbf{1}}) \restriction (R^1[0,1] \times R^1[0,1]) = \mathbb{I} \times \mathbb{I}$.

The functor $\otimes_{\mathbb{I}}$ yielding a function from $\mathbb{I} \times \mathbb{I}$ into $\mathbb{I}$ is defined by the term

(Def. 6) $\otimes_{\mathbb{R}^1} \restriction R^1[0,1]$.

Now we state the proposition:

(6) $(\otimes_{\mathbb{I}})(x, y) = x \cdot y$.

One can verify that $\otimes_{\mathbb{I}}$ is continuous.

Now we state the proposition:

(7) Let us consider points $a$, $b$ of $\mathbb{I}$ and a neighbourhood $N$ of $a \cdot b$. Then there exists a neighbourhood $N_1$ of $a$ and there exists a neighbourhood $N_2$ of $b$ such that for every points $x$, $y$ of $\mathbb{I}$ such that $x \in N_1$ and $y \in N_2$ holds $x \cdot y \in N$. The theorem is a consequence of (6).

Let $T$ be a non empty multiplicative magma and $F$, $G$ be functions from $\mathbb{I} \times \mathbb{I}$ into $T$. The functor $F * G$ yielding a function from $\mathbb{I} \times \mathbb{I}$ into $T$ is defined by

(Def. 7) Let us consider points $a$, $b$ of $\mathbb{I}$. Then $it(a, b) = F(a, b) \cdot G(a, b)$.

Now we state the proposition:

(8) Let us consider functions $F$, $G$ from $\mathbb{I} \times \mathbb{I}$ into $T$ and subsets $M$, $N$ of $\mathbb{I} \times \mathbb{I}$. Then $(F * G)^{\circ}(M \cap N) \subseteq F^{\circ}M \cdot G^{\circ}N$.

Let us consider $T$. Let $F$, $G$ be continuous functions from $\mathbb{I} \times \mathbb{I}$ into $T$. Observe that $F * G$ is continuous.

Now we state the propositions:

(9) Let us consider loops $f_1$, $f_2$, $g_1$, $g_2$ of $t$. Suppose

(i) $f_1$, $f_2$ are homotopic, and

(ii) $g_1$, $g_2$ are homotopic.

Then $f_1 \bullet g_1$, $f_2 \bullet g_2$ are homotopic.

(10) Let us consider loops $f_1$, $f_2$, $g_1$, $g_2$ of $t$, a homotopy $F$ between $f_1$ and $f_2$, and a homotopy $G$ between $g_1$ and $g_2$. Suppose

(i) $f_1$, $f_2$ are homotopic, and

(ii) $g_1$, $g_2$ are homotopic.

Then $F * G$ is a homotopy between $f_1 \bullet g_1$ and $f_2 \bullet g_2$. The theorem is a consequence of (9).

(11) $f + g = (f + c) \bullet (c + g)$.

(12) $f \bullet g$, $(f+c) \bullet (c+g)$ are homotopic. The theorem is a consequence of (9).

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Let $T$ be a semi topological group, $t$ be a point of $T$, and $f$, $g$ be loops of $t$. The functor HopfHomotopy$(f,g)$ yielding a function from $\mathbb{I}\times\mathbb{I}$ into $T$ is defined by

(Def. 8) Let us consider points $a$, $b$ of $\mathbb{I}$. Then $it(a,b) = (((f^{-1})(a\cdot b)\cdot f(a))\cdot g(a))\cdot f(a\cdot b)$.

Note that HopfHomotopy$(f,g)$ is continuous.

In the sequel $T$ denotes a topological group, $t$ denotes a unital point of $T$, and $f$, $g$ denote loops of $t$.

Now we state the proposition:

(13) $f\bullet g$, $g\bullet f$ are homotopic.

Let us consider $T$, $t$, $f$, and $g$. Let us note that the functor HopfHomotopy$(f,g)$ yields a homotopy between $f\bullet g$ and $g\bullet f$.

Now we are at the position where we can present the Main Theorem of the paper: $\pi_1(T,t)$ is commutative.

## References


[1] Grzegorz Bancerek. Monoids. *Formalized Mathematics*, 3(**2**):213–225, 1992.
[2] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[8] Agata Darmochwał and Yatsuka Nakamura. Metric spaces as topological spaces – fundamental concepts. *Formalized Mathematics*, 2(**4**):605–608, 1991.
[9] Adam Grabowski. Introduction to the homotopy theory. *Formalized Mathematics*, 6(**4**): 449–454, 1997.
[10] Adam Grabowski and Artur Korniłowicz. Algebraic properties of homotopies. *Formalized Mathematics*, 12(**3**):251–260, 2004.
[11] Allen Hatcher. *Algebraic Topology*. Cambridge University Press, 2002.
[12] Artur Korniłowicz. The fundamental group of convex subspaces of $\mathcal{E}^n_{\mathrm{T}}$. *Formalized Mathematics*, 12(**3**):295–299, 2004.
[13] Artur Korniłowicz. The definition and basic properties of topological groups. *Formalized Mathematics*, 7(**2**):217–225, 1998.
[14] Artur Korniłowicz and Yasunari Shidama. Some properties of circles on the plane. *Formalized Mathematics*, 13(**1**):117–124, 2005.
[15] Artur Korniłowicz, Yasunari Shidama, and Adam Grabowski. The fundamental group. *Formalized Mathematics*, 12(**3**):261–268, 2004.
[16] Beata Padlewska. Locally connected spaces. *Formalized Mathematics*, 2(**1**):93–96, 1991.
[17] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[18] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[19] Andrzej Trybulec. A Borsuk theorem on homotopy types. *Formalized Mathematics*, 2(**4**): 535–545, 1991.
[20] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.


Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

[21] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.
[22] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[23] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**): 855–864, 1990.
[24] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[25] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[26] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

*Received May 19, 2013*

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 133–143, 2013
DOI: 10.2478/forma-2013-0015

VERSITA
degruyter.com/view/j/forma

# Constructing Binary Huffman Tree[1]

Hiroyuki Okazaki[2]
Shinshu University
Nagano, Japan

Yuichi Futa
Japan Advanced Institute
of Science and Technology
Ishikawa, Japan

Yasunari Shidama[3]
Shinshu University
Nagano, Japan

**Summary.** Huffman coding is one of a most famous entropy encoding methods for lossless data compression [16]. JPEG and ZIP formats employ variants of Huffman encoding as lossless compression algorithms. Huffman coding is a bijective map from source letters into leaves of the Huffman tree constructed by the algorithm. In this article we formalize an algorithm constructing a binary code tree, Huffman tree.

MSC: 14G50 68P30 03B35

Keywords: formalization of Huffman coding tree; source coding

MML identifier: `HUFFMAN1`, version: `8.1.02 5.17.1181`

The notation and terminology used in this paper have been introduced in the following articles: [9], [1], [20], [8], [14], [11], [12], [23], [22], [2], [3], [18], [19], [17], [25], [26], [24], [4], [5], [6], [7], and [13].

## 1. Constructing Binary Decoded Trees

Let $D$ be a non empty set and $x$ be an element of $D$. Observe that the root tree of $x$ is binary as a decorated tree.

The functor $\mathbb{R}_{\mathbb{N}}$ yielding a set is defined by the term

[1]This research was presented during the 2013 International Conference on Foundations of Computer Science FCS'13 in Las Vegas, USA.
[2]This work was supported by JSPS KAKENHI 21240001.
[3]This work was supported by JSPS KAKENHI 22300285.

© 2013 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(Print), 1898-9934(Online)



Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(Def. 1) $\mathbb{N} \times \mathbb{R}$.

Note that $\mathbb{R}_{\mathbb{N}}$ is non empty.

Let $D$ be a non empty set. The binary finite trees of $D$ yielding a set of trees decorated with elements of $D$ is defined by

(Def. 2) Let us consider a tree $T$ decorated with elements of $D$. Then $\operatorname{dom} T$ is finite and $T$ is binary if and only if $T \in it$.

The Boolean binary finite trees of $D$ yielding a non empty subset of $2^{\text{the binary finite trees of } D}$ is defined by the term

(Def. 3) $\{x$, where $x$ is an element of $2^{\alpha} : x$ is finite and $x \neq \emptyset\}$, where $\alpha$ is the binary finite trees of $D$.

In this paper $\mathbb{S}$ denotes a non empty finite set, $p$ denotes a probability on the trivial $\sigma$-field of $\mathbb{S}$, $T_1$ denotes a finite sequence of elements of the Boolean binary finite trees of $\mathbb{R}_{\mathbb{N}}$, and $q$ denotes a finite sequence of elements of $\mathbb{N}$.

Let us consider $\mathbb{S}$ and $p$. The functor $\operatorname{InitTrees} p$ yielding a non empty finite subset of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$ is defined by the term

(Def. 4) $\{T$, where $T$ is an element of $\operatorname{FinTrees}(\mathbb{R}_{\mathbb{N}}) : T$ is a finite binary tree decorated with elements of $\mathbb{R}_{\mathbb{N}}$ and there exists an element $x$ of $\mathbb{S}$ such that $T =$ the root tree of $\langle (\operatorname{CFS}(\mathbb{S}))^{-1}(x), p(\{x\}) \rangle\}$.

Let $p$ be a tree decorated with elements of $\mathbb{R}_{\mathbb{N}}$. The value of root from right of $p$ yielding a real number is defined by the term

(Def. 5) $p(\emptyset)_{\mathbf{2}}$.

The value of root from left of $p$ yielding a natural number is defined by the term

(Def. 6) $p(\emptyset)_{\mathbf{1}}$.

Let $T$ be a finite binary tree decorated with elements of $\mathbb{R}_{\mathbb{N}}$ and $p$ be an element of $\operatorname{dom} T$. The value of tree of $p$ yielding a real number is defined by the term

(Def. 7) $T(p)_{\mathbf{2}}$.

Let $p$, $q$ be finite binary trees decorated with elements of $\mathbb{R}_{\mathbb{N}}$ and $k$ be a natural number. The functor $\operatorname{MakeTree}(p, q, k)$ yielding a finite binary tree decorated with elements of $\mathbb{R}_{\mathbb{N}}$ is defined by the term

(Def. 8) $\langle k$, (the value of root from right of $p$) $+$ (the value of root from right of $q$)$\rangle$-tree$(p, q)$.

Let $X$ be a non empty finite subset of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$. The maximal value of $X$ yielding a natural number is defined by

(Def. 9) There exists a non empty finite subset $L$ of $\mathbb{N}$ such that

(i) $L = \{$the value of root from left of $p$, where $p$ is an element of the binary finite trees of $\mathbb{R}_{\mathbb{N}} : p \in X\}$, and

(ii) $it = \max L$.

Now we state the propositions:

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(1) Let us consider a non empty finite subset $X$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$ and a finite binary tree $w$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. Suppose $X = \{w\}$. Then the maximal value of $X =$ the value of root from left of $w$. PROOF: Consider $L$ being a non empty finite subset of $\mathbb{N}$ such that $L = \{$the value of root from left of $p$, where $p$ is an element of the binary finite trees of $\mathbb{R}_{\mathbb{N}} : p \in X\}$ and the maximal value of $X = \max L$. For every element $n$ such that $n \in L$ holds $n =$ the value of root from left of $w$. For every element $n$ such that $n =$ the value of root from left of $w$ holds $n \in L$. □

(2) Let us consider non empty finite subsets $X$, $Y$, $Z$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$. Suppose $Z = X \cup Y$. Then the maximal value of $Z = \max($the maximal value of $X$, the maximal value of $Y)$.

(3) Let us consider non empty finite subsets $X$, $Z$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$ and a set $Y$. Suppose $Z = X \setminus Y$. Then the maximal value of $Z \leqslant$ the maximal value of $X$. The theorem is a consequence of (2).

(4) Let us consider a non empty finite subset $X$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$ and an element $p$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$. Suppose $p \in X$. Then the value of root from left of $p \leqslant$ the maximal value of $X$.

Let $X$ be a non empty finite subset of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$. A minimal value tree of $X$ is a finite binary tree decorated with elements of $\mathbb{R}_{\mathbb{N}}$ and is defined by

(Def. 10) (i) *it* $\in X$, and

(ii) for every finite binary tree $q$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $q \in X$ holds the value of root from right of *it* $\leqslant$ the value of root from right of $q$.

Now we state the propositions:

(5) $\overline{\overline{\mathrm{InitTrees}\,p}} = \overline{\overline{\mathbb{S}}}$. PROOF: Reconsider $f_1 = (\mathrm{CFS}(\mathbb{S}))^{-1}$ as a function from $\mathbb{S}$ into $\mathrm{Seg}\,\overline{\overline{\mathbb{S}}}$. Define $\mathcal{P}[\text{element}, \text{element}] \equiv \$_2 =$ the root tree of $\langle f_1(\$_1), p(\{\$_1\})\rangle$. For every element $x$ such that $x \in \mathbb{S}$ there exists an element $y$ such that $y \in \mathrm{InitTrees}\,p$ and $\mathcal{P}[x, y]$ by [12, (5)], [13, (87)], [7, (3)]. Consider $f$ being a function from $\mathbb{S}$ into $\mathrm{InitTrees}\,p$ such that for every element $x$ such that $x \in \mathbb{S}$ holds $\mathcal{P}[x, f(x)]$ from [12, Sch. 1]. □

(6) Let us consider a non empty finite subset $X$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$ and finite binary trees $s$, $t$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. Then $\mathrm{MakeTree}(t, s, ((\text{the maximal value of } X) + 1)) \notin X$.

Let $X$ be a set. The set of leaves of $X$ yielding a subset of $2^{\mathbb{R}_{\mathbb{N}}}$ is defined by the term

(Def. 11) $\{\mathrm{Leaves}(p)$, where $p$ is an element of the binary finite trees of $\mathbb{R}_{\mathbb{N}} : p \in X\}$.

Now we state the propositions:

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(7) Let us consider a finite binary tree $X$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. Then the set of leaves of $\{X\} = \{\text{Leaves}(X)\}$. PROOF: For every element $x$, $x \in$ the set of leaves of $\{X\}$ iff $x \in \{\text{Leaves}(X)\}$. $\square$

(8) Let us consider sets $X$, $Y$. Then the set of leaves of $X \cup Y =$ (the set of leaves of $X$) $\cup$ (the set of leaves of $Y$). PROOF: For every element $x$, $x \in$ the set of leaves of $X \cup Y$ iff $x \in$ (the set of leaves of $X$) $\cup$ (the set of leaves of $Y$). $\square$

(9) Let us consider trees $s$, $t$. Then $\emptyset \notin \text{Leaves}(\overbrace{t, s})$. PROOF: For every element $p$, $p \in \overbrace{t, s}$ iff $p \in$ the elementary tree of 0 by [4, (19), (29)], [10, (130)]. $\square$

(10) Let us consider trees $s$, $t$. Then $\text{Leaves}(\overbrace{t, s}) = \{\langle 0 \rangle \frown p$, where $p$ is an element of $t : p \in \text{Leaves}(t)\} \cup \{\langle 1 \rangle \frown p$, where $p$ is an element of $s : p \in \text{Leaves}(s)\}$. The theorem is a consequence of (9). PROOF: Set $L = \{\langle 0 \rangle \frown p$, where $p$ is an element of $t : p \in \text{Leaves}(t)\}$. Set $R = \{\langle 1 \rangle \frown p$, where $p$ is an element of $s : p \in \text{Leaves}(s)\}$. Set $H = \text{Leaves}(\overbrace{t, s})$. For every element $x$, $x \in H$ iff $x \in L \cup R$ by [2, (23)], [9, (6)]. $\square$

Let us consider decorated trees $s$, $t$, an element $x$, and a finite sequence $q$ of elements of $\mathbb{N}$. Now we state the propositions:

(11) If $q \in \operatorname{dom} t$, then $(x\text{-tree}(t, s))(\langle 0 \rangle \frown q) = t(q)$.

(12) If $q \in \operatorname{dom} s$, then $(x\text{-tree}(t, s))(\langle 1 \rangle \frown q) = s(q)$.

Now we state the propositions:

(13) Let us consider decorated trees $s$, $t$ and an element $x$. Then $\text{Leaves}(x\text{-tree}(t, s)) = \text{Leaves}(t) \cup \text{Leaves}(s)$. The theorem is a consequence of (10), (11), and (12). PROOF: Set $L = \{\langle 0 \rangle \frown p$, where $p$ is an element of $\operatorname{dom} t : p \in \text{Leaves}(\operatorname{dom} t)\}$. Set $R = \{\langle 1 \rangle \frown p$, where $p$ is an element of $\operatorname{dom} s : p \in \text{Leaves}(\operatorname{dom} s)\}$. For every element $z$, $z \in (x\text{-tree}(t, s))^{\circ} L$ iff $z \in t^{\circ}(\text{Leaves}(\operatorname{dom} t))$. For every element $z$, $z \in (x\text{-tree}(t, s))^{\circ} R$ iff $z \in s^{\circ}(\text{Leaves}(\operatorname{dom} s))$. $\square$

(14) Let us consider a natural number $k$ and finite binary trees $s$, $t$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. Then $\bigcup$ the set of leaves of $\{s, t\} = \bigcup$ the set of leaves of $\{\text{MakeTree}(t, s, k)\}$. The theorem is a consequence of (8), (7), and (13).

(15) Leaves(the elementary tree of 0) $=$ the elementary tree of 0. PROOF: For every element $x$, $x \in$ Leaves(the elementary tree of 0) iff $x \in$ the elementary tree of 0 by [4, (29), (54)]. $\square$

(16) Let us consider an element $x$, a non empty set $D$, and a finite binary tree $T$ decorated with elements of $D$. Suppose $T =$ the root tree of $x$. Then $\text{Leaves}(T) = \{x\}$. The theorem is a consequence of (15).

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

## 2. Binary Huffman Tree

Let us consider $\mathbb{S}$, $p$, $T_1$, and $q$. We say that $T_1$, $q$, and $p$ are constructing binary Huffman tree if and only if

(Def. 12) (i) $T_1(1) = \mathrm{InitTrees}\, p$, and

(ii) $\mathrm{len}\, T_1 = \overline{\overline{\mathbb{S}}}$, and

(iii) for every natural number $i$ such that $1 \leqslant i < \mathrm{len}\, T_1$ there exist non empty finite subsets $X$, $Y$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$ and there exists a minimal value tree $s$ of $X$ and there exists a minimal value tree $t$ of $Y$ and there exists a finite binary tree $v$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $T_1(i) = X$ and $Y = X \setminus \{s\}$ and $v \in \{\mathrm{MakeTree}(t, s, ((\text{the maximal value of } X)+1)), \mathrm{MakeTree}(s, t, ((\text{the maximal value of } X) + 1))\}$ and $T_1(i+1) = (X \setminus \{t, s\}) \cup \{v\}$, and

(iv) there exists a finite binary tree $T$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $\{T\} = T_1(\mathrm{len}\, T_1)$, and

(v) $\mathrm{dom}\, q = \mathrm{Seg}\, \overline{\overline{\mathbb{S}}}$, and

(vi) for every natural number $k$ such that $k \in \mathrm{Seg}\, \overline{\overline{\mathbb{S}}}$ holds $q(k) = \overline{\overline{T_1(k)}}$ and $q(k) \neq 0$, and

(vii) for every natural number $k$ such that $k < \overline{\overline{\mathbb{S}}}$ holds $q(k+1) = q(1) - k$, and

(viii) for every natural number $k$ such that $1 \leqslant k < \overline{\overline{\mathbb{S}}}$ holds $2 \leqslant q(k)$.

Now we state the proposition:

(17) There exists $T_1$ and there exists $q$ such that $T_1$, $q$, and $p$ are constructing binary Huffman tree. The theorem is a consequence of (5) and (6). Proof: Define $\mathcal{A}[\text{natural number}, \text{set}, \text{set}] \equiv$ if there exist elements $u$, $v$ such that $u \neq v$ and $u$, $v \in \$_2$, then there exist non empty finite subsets $X$, $Y$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$ and there exists a minimal value tree $s$ of $X$ and there exists a minimal value tree $t$ of $Y$ and there exists a finite binary tree $w$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $\$_2 = X$ and $Y = X \setminus \{s\}$ and $w \in \{\mathrm{MakeTree}(t, s, ((\text{the maximal value of } X) + 1)), \mathrm{MakeTree}(s, t, ((\text{the maximal value of } X)+1))\}$ and $\$_3 = (X \setminus \{t, s\}) \cup \{w\}$. For every natural number $n$ such that $1 \leqslant n < \overline{\overline{\mathbb{S}}}$ for every element $x$ of the Boolean binary finite trees of $\mathbb{R}_{\mathbb{N}}$, there exists an element $y$ of the Boolean binary finite trees of $\mathbb{R}_{\mathbb{N}}$ such that $\mathcal{A}[n, x, y]$. Reconsider $I = \mathrm{InitTrees}\, p$ as an element of the Boolean binary finite trees of $\mathbb{R}_{\mathbb{N}}$. Consider $T_1$ being a finite sequence of elements of the Boolean binary finite trees of $\mathbb{R}_{\mathbb{N}}$ such that $\mathrm{len}\, T_1 = \overline{\overline{\mathbb{S}}}$ and $T_1(1) = I$ or $\overline{\overline{\mathbb{S}}} = 0$ and for every natural number $n$ such that $1 \leqslant n < \overline{\overline{\mathbb{S}}}$ holds $\mathcal{A}[n, T_1(n), T_1(n+1)]$ from [15, Sch. 4]. Define $\mathcal{B}[\text{element}, \text{element}] \equiv$ there exists a finite set $X$ such that

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

$T_1(\$_1) = X$ and $\$_2 = \overline{\overline{X}}$ and $\$_2 \neq 0$. For every natural number $k$ such that $k \in \operatorname{Seg} \overline{\overline{\mathbb{S}}}$ there exists an element $x$ of $\mathbb{N}$ such that $\mathcal{B}[k, x]$ by [11, (3)]. Consider $q$ being a finite sequence of elements of $\mathbb{N}$ such that $\operatorname{dom} q = \operatorname{Seg} \overline{\overline{\mathbb{S}}}$ and for every natural number $k$ such that $k \in \operatorname{Seg} \overline{\overline{\mathbb{S}}}$ holds $\mathcal{B}[k, q(k)]$ from [8, Sch. 5]. For every natural number $k$ such that $k \in \operatorname{Seg} \overline{\overline{\mathbb{S}}}$ holds $q(k) = \overline{\overline{T_1(k)}}$ and $q(k) \neq 0$. For every natural number $k$ such that $1 \leqslant k < \overline{\overline{\mathbb{S}}}$ holds if $2 \leqslant q(k)$, then $q(k+1) = q(k) - 1$ by [8, (1)], [2, (11), (13)]. Define $\mathcal{C}[\text{natural number}] \equiv$ if $\$_1 < \overline{\overline{\mathbb{S}}}$, then $q(\$_1 + 1) = q(1) - \$_1$. For every natural number $n$ such that $\mathcal{C}[n]$ holds $\mathcal{C}[n + 1]$ by [2, (11)], [8, (1)], [2, (14), (13)]. For every natural number $n$, $\mathcal{C}[n]$ from [2, Sch. 2]. For every natural number $n$ such that $1 \leqslant n < \overline{\overline{\mathbb{S}}}$ holds $2 \leqslant q(n)$ by [2, (21), (13)]. For every natural number $k$ such that $1 \leqslant k < \operatorname{len} T_1$ there exist non empty finite subsets $X$, $Y$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$ and there exists a minimal value tree $s$ of $X$ and there exists a minimal value tree $t$ of $Y$ and there exists a finite binary tree $w$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $T_1(k) = X$ and $Y = X \setminus \{s\}$ and $w \in \{\text{MakeTree}(t, s, ((\text{the maximal value of } X) + 1)), \text{MakeTree}(s, t, ((\text{the maximal value of } X) + 1))\}$ and $T_1(k + 1) = (X \setminus \{t, s\}) \cup \{w\}$ by [8, (1)]. Consider $T_2$ being a finite set such that $T_1(\overline{\overline{\mathbb{S}}}) = T_2$ and $q(\overline{\overline{\mathbb{S}}}) = \overline{\overline{T_2}}$ and $q(\overline{\overline{\mathbb{S}}}) \neq 0$. Consider $u$ being an element such that $T_2 = \{u\}$. $\square$

Let us consider $\mathbb{S}$ and $p$. A binary Huffman tree of $p$ is a finite binary tree decorated with elements of $\mathbb{R}_{\mathbb{N}}$ and is defined by

(Def. 13) There exists a finite sequence $T_1$ of elements of the Boolean binary finite trees of $\mathbb{R}_{\mathbb{N}}$ and there exists a finite sequence $q$ of elements of $\mathbb{N}$ such that $T_1$, $q$, and $p$ are constructing binary Huffman tree and $\{it\} = T_1(\operatorname{len} T_1)$.

In this paper $T$ denotes a binary Huffman tree of $p$.

Now we state the propositions:

(18) $\bigcup$ the set of leaves of $\operatorname{InitTrees} p = \{z,$ where $z$ is an element of $\mathbb{N} \times \mathbb{R}$ : there exists an element $x$ of $\mathbb{S}$ such that $z = \langle (\text{CFS}(\mathbb{S}))^{-1}(x), p(\{x\}) \rangle\}$. The theorem is a consequence of (16). Proof: Set $L = \bigcup$ the set of leaves of $\operatorname{InitTrees} p$. Set $R = \{z,$ where $z$ is an element of $\mathbb{N} \times \mathbb{R}$ : there exists an element $x$ of $\mathbb{S}$ such that $z = \langle (\text{CFS}(\mathbb{S}))^{-1}(x), p(\{x\}) \rangle\}$. For every element $x$, $x \in L$ iff $x \in R$ by [13, (87)], [7, (3)]. $\square$

(19) Suppose $T_1$, $q$, and $p$ are constructing binary Huffman tree. Let us consider a natural number $i$. Suppose $1 \leqslant i \leqslant \operatorname{len} T_1$. Then $\bigcup$ the set of leaves of $T_1(i) = \{z,$ where $z$ is an element of $\mathbb{N} \times \mathbb{R}$ : there exists an element $x$ of $\mathbb{S}$ such that $z = \langle (\text{CFS}(\mathbb{S}))^{-1}(x), p(\{x\}) \rangle\}$. The theorem is a consequence of (18), (8), and (14). Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 < \operatorname{len} T_1$, then $\bigcup$ the set of leaves of $T_1(\$_1 + 1) = \{z,$ where $z$ is an element of $\mathbb{N} \times \mathbb{R}$ : there exists an element $x$ of $\mathbb{S}$ such that $z = \langle (\text{CFS}(\mathbb{S}))^{-1}(x),$

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

$p(\{x\})\rangle\!\rangle\}$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [2, (11)], [13, (78), (32)]. For every natural number $k$, $\mathcal{P}[k]$ from [2, Sch. 2]. $\square$

(20) $\mathrm{Leaves}(T) = \{z,$ where $z$ is an element of $\mathbb{N}\times\mathbb{R}$ : there exists an element $x$ of $\mathbb{S}$ such that $z = \langle\!\langle(\mathrm{CFS}(\mathbb{S}))^{-1}(x), p(\{x\})\rangle\!\rangle\}$. The theorem is a consequence of (19) and (7).

(21) Suppose $T_1$, $q$, and $p$ are constructing binary Huffman tree. Let us consider a natural number $i$, a finite binary tree $T$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$, and elements $t$, $s$, $r$ of $\mathrm{dom}\,T$. Suppose

(i) $T \in T_1(i)$, and

(ii) $t \in \mathrm{dom}\,T \setminus \mathrm{Leaves}(\mathrm{dom}\,T)$, and

(iii) $s = t \frown \langle 0\rangle$, and

(iv) $r = t \frown \langle 1\rangle$.

Then the value of tree of $t =$ (the value of tree of $s$) + (the value of tree of $r$). The theorem is a consequence of (15), (11), and (12). Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if $1 \leqslant \$_1 \leqslant \mathrm{len}\,T_1$, then for every finite binary tree $T$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ and for every elements $a$, $b$, $c$ of $\mathrm{dom}\,T$ such that $T \in T_1(\$_1)$ and $a \in \mathrm{dom}\,T \setminus \mathrm{Leaves}(\mathrm{dom}\,T)$ and $b = a \frown \langle 0\rangle$ and $c = a \frown \langle 1\rangle$ holds the value of tree of $a =$ (the value of tree of $b$)+(the value of tree of $c$). For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [2, (16), (14)], [8, (44)]. For every natural number $i$, $\mathcal{P}[i]$ from [2, Sch. 2]. $\square$

(22) Let us consider elements $t$, $s$, $r$ of $\mathrm{dom}\,T$. Suppose

(i) $t \in \mathrm{dom}\,T \setminus \mathrm{Leaves}(\mathrm{dom}\,T)$, and

(ii) $s = t \frown \langle 0\rangle$, and

(iii) $r = t \frown \langle 1\rangle$.

Then the value of tree of $t =$ (the value of tree of $s$) + (the value of tree of $r$). The theorem is a consequence of (21).

(23) Let us consider a non empty finite subset $X$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$. Suppose a finite binary tree $T$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. Suppose $T \in X$. Let us consider an element $p$ of $\mathrm{dom}\,T$ and an element $r$ of $\mathbb{N}$. Suppose $r = T(p)_{\mathbf{1}}$. Then $r \leqslant$ the maximal value of $X$. Let us consider finite binary trees $s$, $t$, $w$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. Suppose

(i) $s, t \in X$, and

(ii) $w = \mathrm{MakeTree}(t, s, ((\text{the maximal value of } X) + 1))$.

Let us consider an element $p$ of $\mathrm{dom}\,w$ and an element $r$ of $\mathbb{N}$. Suppose $r = w(p)_{\mathbf{1}}$. Then $r \leqslant$ (the maximal value of $X$) + 1. The theorem is a consequence of (11) and (12). Proof: For every element $a$ such that

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

$a \in \operatorname{dom} d$ holds $a = \emptyset$ or there exists an element $f$ of $\operatorname{dom} t$ such that $a = \langle 0 \rangle \frown f$ or there exists an element $f$ of $\operatorname{dom} s$ such that $a = \langle 1 \rangle \frown f$ by [2, (23)]. □

(24) Suppose $T_1$, $q$, and $p$ are constructing binary Huffman tree. Let us consider a natural number $i$. Suppose $1 \leqslant i < \operatorname{len} T_1$. Let us consider non empty finite subsets $X$, $Y$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$. Suppose

(i) $X = T_1(i)$, and

(ii) $Y = T_1(i+1)$.

Then the maximal value of $Y =$ (the maximal value of $X) + 1$. PROOF: Consider $X$, $Y$ being non empty finite subsets of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$, $s$ being a minimal value tree of $X$, $t$ being a minimal value tree of $Y$, $v$ being a finite binary tree decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $T_1(i) = X$ and $Y = X \setminus \{s\}$ and $v \in \{\mathrm{MakeTree}(t, s, ((\text{the maximal value of } X) + 1)), \mathrm{MakeTree}(s, t, ((\text{the maximal value of } X) + 1))\}$ and $T_1(i+1) = (X \setminus \{t, s\}) \cup \{v\}$. Consider $L_1$ being a non empty finite subset of $\mathbb{N}$ such that $L_1 = \{$the value of root from left of $p$, where $p$ is an element of the binary finite trees of $\mathbb{R}_{\mathbb{N}} : p \in X0\}$ and the maximal value of $X0 = \max L_1$. Consider $L_4$ being a non empty finite subset of $\mathbb{N}$ such that $L_4 = \{$the value of root from left of $p$, where $p$ is an element of the binary finite trees of $\mathbb{R}_{\mathbb{N}} : p \in Y0\}$ and the maximal value of $Y0 = \max L_4$. Reconsider $p_1 = v$ as an element of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$. For every extended real $x$ such that $x \in L_4$ holds $x \leqslant$ the value of root from left of $p_1$ by [2, (16)]. □

Let us consider a natural number $i$, a non empty finite subset $X$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$, a finite binary tree $T$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$, an element $p$ of $\operatorname{dom} T$, and an element $r$ of $\mathbb{N}$. Now we state the propositions:

(25) Suppose $T_1$, $q$, and $p$ are constructing binary Huffman tree. Then if $X = T_1(i)$, then if $T \in X$, then if $r = T(p)_{\mathbf{1}}$, then $r \leqslant$ the maximal value of $X$.

(26) Suppose $T_1$, $q$, and $p$ are constructing binary Huffman tree. Then if $X = T_1(i)$, then if $T \in X$, then if $r = T(p)_{\mathbf{1}}$, then $r \leqslant$ the maximal value of $X$.

Now we state the proposition:

(27) Suppose $T_1$, $q$, and $p$ are constructing binary Huffman tree. Let us consider a natural number $i$, finite binary trees $s$, $t$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$, and a non empty finite subset $X$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$. Suppose

(i) $X = T_1(i)$, and

(ii) $s, t \in X$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Let us consider a finite binary tree $z$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. Suppose $z \in X$. Then $\langle$(the maximal value of $X$) + 1, (the value of root from right of $t$) + (the value of root from right of $s$)$\rangle \notin \operatorname{rng} z$. The theorem is a consequence of (26).

Let $x$ be an element. Note that the root tree of $x$ is one-to-one.

Now we state the propositions:

(28) Let us consider a non empty finite subset $X$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$ and finite binary trees $s$, $t$, $w$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. Suppose

- (i) for every finite binary tree $T$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $T \in X$ for every element $p$ of $\operatorname{dom} T$ for every element $r$ of $\mathbb{N}$ such that $r = T(p)_{\mathbf{1}}$ holds $r \leqslant$ the maximal value of $X$, and
- (ii) for every finite binary trees $p$, $q$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $p$, $q \in X$ and $p \neq q$ holds $\operatorname{rng} p \cap \operatorname{rng} q = \emptyset$, and
- (iii) $s$, $t \in X$, and
- (iv) $s \neq t$, and
- (v) $w \in X \setminus \{s, t\}$.

Then $\operatorname{rng} \operatorname{MakeTree}(t, s, ((\text{the maximal value of } X) + 1)) \cap \operatorname{rng} w = \emptyset$. The theorem is a consequence of (11) and (12). Proof: Set $d = \operatorname{MakeTree}(t, s, ((\text{the maximal value of } X) + 1))$. For every element $a$ such that $a \in \operatorname{dom} d$ holds $a = \emptyset$ or there exists an element $f$ of $\operatorname{dom} t$ such that $a = \langle 0 \rangle \frown f$ or there exists an element $f$ of $\operatorname{dom} s$ such that $a = \langle 1 \rangle \frown f$ by [2, (23)]. Consider $n_2$ being an element such that $n_2 \in \operatorname{rng} d \cap \operatorname{rng} w$. Consider $a_1$ being an element such that $a_1 \in \operatorname{dom} d$ and $n_2 = d(a_1)$. Consider $b_1$ being an element such that $b_1 \in \operatorname{dom} w$ and $n_2 = w(b_1)$. $w \in X$ and $w \neq s$ and $w \neq t$. $\square$

(29) Suppose $T_1$, $q$, and $p$ are constructing binary Huffman tree. Let us consider a natural number $i$ and finite binary trees $T$, $S$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. Suppose

- (i) $T$, $S \in T_1(i)$, and
- (ii) $T \neq S$.

Then $\operatorname{rng} T \cap \operatorname{rng} S = \emptyset$. The theorem is a consequence of (26) and (28). Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if $1 \leqslant \$_1 \leqslant \operatorname{len} T_1$, then for every finite binary trees $T$, $S$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $T$, $S \in T_1(\$_1)$ and $T \neq S$ holds $\operatorname{rng} T \cap \operatorname{rng} S = \emptyset$. For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [21, (8)], [2, (16), (14)]. For every natural number $i$, $\mathcal{P}[i]$ from [2, Sch. 2]. $\square$

(30) Let us consider a non empty finite subset $X$ of the binary finite trees of $\mathbb{R}_{\mathbb{N}}$ and finite binary trees $s$, $t$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. Suppose

- (i) $s$ is one-to-one, and

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(ii) $t$ is one-to-one, and
(iii) $t$, $s \in X$, and
(iv) $\operatorname{rng} s \cap \operatorname{rng} t = \emptyset$, and
(v) for every finite binary tree $z$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $z \in X$ holds $\langle$(the maximal value of $X$) + 1, (the value of root from right of $t$) + (the value of root from right of $s$)$\rangle \notin \operatorname{rng} z$.

Then MakeTree($t, s$, ((the maximal value of $X$) + 1)) is one-to-one. The theorem is a consequence of (11) and (12). Proof: Set $d$ = MakeTree($t, s$, ((the maximal value of $X$) + 1)). For every element $a$ such that $a \in \operatorname{dom} d$ holds $a = \emptyset$ or there exists an element $f$ of $\operatorname{dom} t$ such that $a = \langle 0 \rangle \frown f$ or there exists an element $f$ of $\operatorname{dom} s$ such that $a = \langle 1 \rangle \frown f$ by [2, (23)]. For every element $x$ such that $x \in \operatorname{dom} d$ and $x \neq \emptyset$ holds $d(x) \neq d(\emptyset)$ by [11, (3)]. For every elements $x_1$, $x_2$ such that $x_1$, $x_2 \in \operatorname{dom} d$ and $d(x_1) = d(x_2)$ holds it is not true that there exists an element $f$ of $\operatorname{dom} s$ such that $x_1 = \langle 1 \rangle \frown f$ and there exists an element $f$ of $\operatorname{dom} t$ such that $x_2 = \langle 0 \rangle \frown f$ by [11, (3)]. For every elements $x_1, x_2$ such that $x_1, x_2 \in \operatorname{dom} d$ and $d(x_1) = d(x_2)$ holds $x_1 = x_2$. □

(31) Suppose $T_1$, $q$, and $p$ are constructing binary Huffman tree. Let us consider a natural number $i$ and a finite binary tree $T$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$. If $T \in T_1(i)$, then $T$ is one-to-one. The theorem is a consequence of (27), (29), and (30). Proof: Define $\mathcal{P}$[natural number] $\equiv$ if $1 \leqslant \$_1 \leqslant \operatorname{len} T_1$, then for every finite binary tree $T$ decorated with elements of $\mathbb{R}_{\mathbb{N}}$ such that $T \in T_1(\$_1)$ holds $T$ is one-to-one. For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [2, (16), (14)]. For every natural number $i$, $\mathcal{P}[i]$ from [2, Sch. 2]. □

Let us consider $p$.

Now we are at the position where we can present the Main Theorem of the paper: Every binary Huffman tree of $p$ is one-to-one.

## References


[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek. Introduction to trees. *Formalized Mathematics*, 1(**2**):421–427, 1990.
[5] Grzegorz Bancerek. König's lemma. *Formalized Mathematics*, 2(**3**):397–402, 1991.
[6] Grzegorz Bancerek. Sets and functions of trees and joining operations of trees. *Formalized Mathematics*, 3(**2**):195–204, 1992.
[7] Grzegorz Bancerek. Joining of decorated trees. *Formalized Mathematics*, 4(**1**):77–82, 1993.
[8] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[9] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on binary trees. *Formalized Mathematics*, 5(**1**):9–13, 1996.


Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

[10] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[11] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[12] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[13] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[14] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[15] Krzysztof Hryniewiecki. Recursive definitions. *Formalized Mathematics*, 1(**2**):321–328, 1990.
[16] D. A. Huffman. *A method for the construction of minimum-redundancy codes*. Proceedings of the I.R.E, 1952.
[17] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.
[18] Andrzej Nędzusiak. $\sigma$-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.
[19] Hiroyuki Okazaki and Yasunari Shidama. Probability on finite set and real-valued random variables. *Formalized Mathematics*, 17(**2**):129–136, 2009. doi:10.2478/v10037-009-0014-x.
[20] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.
[21] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.
[22] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.
[23] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[24] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[25] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[26] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

*Received June 18, 2013*

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 145–152, 2013
DOI: 10.2478/forma-2013-0016

VERSITA
degruyter.com/view/j/forma

# Riemann Integral of Functions from $\mathbb{R}$ into Real Banach Space[1]

Keiko Narita
Hirosaki-city
Aomori, Japan

Noboru Endou
Gifu National College of Technology
Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

**Summary.** In this article we deal with the Riemann integral of functions from $\mathbb{R}$ into a real Banach space. The last theorem establishes the integrability of continuous functions on the closed interval of reals. To prove the integrability we defined uniform continuity for functions from $\mathbb{R}$ into a real normed space, and proved related theorems. We also stated some properties of finite sequences of elements of a real normed space and finite sequences of real numbers.

In addition we proved some theorems about the convergence of sequences. We applied definitions introduced in the previous article [21] to the proof of integrability.

MSC: 26A42 03B35

Keywords: formalization of Riemann integral

MML identifier: INTEGR20, version: 8.1.02 5.17.1181

The notation and terminology used in this paper have been introduced in the following articles: [6], [1], [7], [22], [4], [8], [14], [9], [10], [21], [15], [16], [17], [18], [28], [26], [5], [27], [2], [23], [24], [3], [11], [19], [25], [32], [33], [30], [12], [20], [31], and [13].

## 1. Some Properties of Continuous Functions

In this paper $s_1$, $s_2$, $q_1$ denote sequences of real numbers.

Let $X$ be a real normed space and $f$ be a partial function from $\mathbb{R}$ to the carrier of $X$. We say that $f$ is uniformly continuous if and only if

[1]This work was supported by JSPS KAKENHI 22300285 and 23500029.

© 2013 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(Print), 1898-9934(Online)



Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(Def. 1) Let us consider a real number $r$. Suppose $0 < r$. Then there exists a real number $s$ such that

(i) $0 < s$, and

(ii) for every real numbers $x_1$, $x_2$ such that $x_1, x_2 \in \operatorname{dom} f$ and $|x_1 - x_2| < s$ holds $\|f_{x_1} - f_{x_2}\| < r$.

Now we state the propositions:

(1) Let us consider a set $X$, a real normed space $Y$, and a partial function $f$ from $\mathbb{R}$ to the carrier of $Y$. Then $f \restriction X$ is uniformly continuous if and only if for every real number $r$ such that $0 < r$ there exists a real number $s$ such that $0 < s$ and for every real numbers $x_1$, $x_2$ such that $x_1, x_2 \in \operatorname{dom}(f \restriction X)$ and $|x_1 - x_2| < s$ holds $\|f_{x_1} - f_{x_2}\| < r$. PROOF: If $f \restriction X$ is uniformly continuous, then for every real number $r$ such that $0 < r$ there exists a real number $s$ such that $0 < s$ and for every real numbers $x_1$, $x_2$ such that $x_1, x_2 \in \operatorname{dom}(f \restriction X)$ and $|x_1 - x_2| < s$ holds $\|f_{x_1} - f_{x_2}\| < r$ by [11, (80)]. Consider $s$ being a real number such that $0 < s$ and for every real numbers $x_1$, $x_2$ such that $x_1, x_2 \in \operatorname{dom}(f \restriction X)$ and $|x_1 - x_2| < s$ holds $\|f_{x_1} - f_{x_2}\| < r$. $\square$

(2) Let us consider sets $X$, $X_1$, a real normed space $Y$, and a partial function $f$ from $\mathbb{R}$ to the carrier of $Y$. Suppose

(i) $f \restriction X$ is uniformly continuous, and

(ii) $X_1 \subseteq X$.

Then $f \restriction X_1$ is uniformly continuous. The theorem is a consequence of (1).

(3) Let us consider a real normed space $X$, a partial function $f$ from $\mathbb{R}$ to the carrier of $X$, and a subset $Z$ of $\mathbb{R}$. Suppose

(i) $Z \subseteq \operatorname{dom} f$, and

(ii) $Z$ is compact, and

(iii) $f \restriction Z$ is continuous.

Then $f \restriction Z$ is uniformly continuous. The theorem is a consequence of (1).

## 2. Some Properties of Sequences

Now we state the proposition:

(4) Let us consider a real normed space $X$, natural numbers $n$, $m$, a function $a$ from $\operatorname{Seg} n \times \operatorname{Seg} m$ into $X$, and finite sequences $p$, $q$ of elements of $X$. Suppose

(i) $\operatorname{dom} p = \operatorname{Seg} n$, and

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(ii) for every natural number $i$ such that $i \in \operatorname{dom} p$ there exists a finite sequence $r$ of elements of $X$ such that $\operatorname{dom} r = \operatorname{Seg} m$ and $p(i) = \sum r$ and for every natural number $j$ such that $j \in \operatorname{dom} r$ holds $r(j) = a(i, j)$, and

(iii) $\operatorname{dom} q = \operatorname{Seg} m$, and

(iv) for every natural number $j$ such that $j \in \operatorname{dom} q$ there exists a finite sequence $s$ of elements of $X$ such that $\operatorname{dom} s = \operatorname{Seg} n$ and $q(j) = \sum s$ and for every natural number $i$ such that $i \in \operatorname{dom} s$ holds $s(i) = a(i, j)$.

Then $\sum p = \sum q$. PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every natural number $m$ for every function $a$ from $\operatorname{Seg} \$_1 \times \operatorname{Seg} m$ into $X$ for every finite sequences $p$, $q$ of elements of $X$ such that $\operatorname{dom} p = \operatorname{Seg} \$_1$ and for every natural number $i$ such that $i \in \operatorname{dom} p$ there exists a finite sequence $r$ of elements of $X$ such that $\operatorname{dom} r = \operatorname{Seg} m$ and $p(i) = \sum r$ and for every natural number $j$ such that $j \in \operatorname{dom} r$ holds $r(j) = a(i, j)$ and $\operatorname{dom} q = \operatorname{Seg} m$ and for every natural number $j$ such that $j \in \operatorname{dom} q$ there exists a finite sequence $s$ of elements of $X$ such that $\operatorname{dom} s = \operatorname{Seg} \$_1$ and $q(j) = \sum s$ and for every natural number $i$ such that $i \in \operatorname{dom} s$ holds $s(i) = a(i, j)$ holds $\sum p = \sum q$. For every natural number $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$ by [4, (5)], [2, (11)], [13, (95)]. For every natural number $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. □

Let $A$ be a subset of $\mathbb{R}$. The extension of $\operatorname{vol}(A)$ yielding a real number is defined by the term

(Def. 2) $\begin{cases} 0, & \textbf{if } A \text{ is empty}, \\ \operatorname{vol}(A), & \textbf{otherwise}. \end{cases}$

In the sequel $n$ denotes an element of $\mathbb{N}$ and $a$, $b$ denote real numbers.

Now we state the propositions:

(5) Let us consider a real bounded subset $A$ of $\mathbb{R}$. Then $0 \leqslant$ the extension of $\operatorname{vol}(A)$.

(6) Let us consider a non empty closed interval subset $A$ of $\mathbb{R}$, a Division $D$ of $A$, and a finite sequence $q$ of elements of $\mathbb{R}$. Suppose

(i) $\operatorname{dom} q = \operatorname{Seg} \operatorname{len} D$, and

(ii) for every natural number $i$ such that $i \in \operatorname{Seg} \operatorname{len} D$ holds $q(i) = \operatorname{vol}(\operatorname{divset}(D, i))$.

Then $\sum q = \operatorname{vol}(A)$. PROOF: Set $p = \text{lower\_volume}(\chi_{A,A}, D)$. For every natural number $k$ such that $k \in \operatorname{dom} q$ holds $q(k) = p(k)$ by [15, (19)]. □

(7) Let us consider a real normed space $Y$, a point $E$ of $Y$, a finite sequence $q$ of elements of $\mathbb{R}$, and a finite sequence $S$ of elements of $Y$. Suppose

(i) $\operatorname{len} S = \operatorname{len} q$, and

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(ii) for every natural number $i$ such that $i \in \operatorname{dom} S$ there exists a real number $r$ such that $r = q(i)$ and $S(i) = r \cdot E$.

Then $\sum S = \sum q \cdot E$. PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence $q$ of elements of $\mathbb{R}$ for every finite sequence $S$ of elements of $Y$ such that $\$_1 = \operatorname{len} S$ and $\operatorname{len} S = \operatorname{len} q$ and for every natural number $i$ such that $i \in \operatorname{dom} S$ there exists a real number $r$ such that $r = q(i)$ and $S(i) = r \cdot E$ holds $\sum S = \sum q \cdot E$. $\mathcal{P}[0]$ by [30, (10)], [12, (72)], [30, (43)]. For every natural number $i$, $\mathcal{P}[i]$ from [2, Sch. 2]. $\square$

(8) Let us consider a non empty closed interval subset $A$ of $\mathbb{R}$, a Division $D$ of $A$, a non empty closed interval subset $B$ of $\mathbb{R}$, and a finite sequence $v$ of elements of $\mathbb{R}$. Suppose

(i) $B \subseteq A$, and

(ii) $\operatorname{len} D = \operatorname{len} v$, and

(iii) for every natural number $i$ such that $i \in \operatorname{dom} v$ holds $v(i) =$ the extension of $\operatorname{vol}(B \cap \operatorname{divset}(D, i))$.

Then $\sum v = \operatorname{vol}(B)$. The theorem is a consequence of (5). PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non empty closed interval subset $A$ of $\mathbb{R}$ for every Division $D$ of $A$ for every non empty closed interval subset $B$ of $\mathbb{R}$ for every finite sequence $v$ of elements of $\mathbb{R}$ such that $\$_1 = \operatorname{len} D$ and $B \subseteq A$ and $\operatorname{len} D = \operatorname{len} v$ and for every natural number $k$ such that $k \in \operatorname{dom} v$ holds $v(k) =$ the extension of $\operatorname{vol}(B \cap \operatorname{divset}(D, k))$ holds $\sum v = \operatorname{vol}(B)$. For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [29, (29)], [4, (4)], [2, (11)]. For every natural number $i$, $\mathcal{P}[i]$ from [2, Sch. 2]. $\square$

(9) Let us consider a real normed space $Y$, a finite sequence $x_3$ of elements of $Y$, and a finite sequence $y$ of elements of $\mathbb{R}$. Suppose

(i) $\operatorname{len} x_3 = \operatorname{len} y$, and

(ii) for every element $i$ of $\mathbb{N}$ such that $i \in \operatorname{dom} x_3$ there exists a point $v$ of $Y$ such that $v = x_{3i}$ and $y(i) = \|v\|$.

Then $\|\sum x_3\| \leqslant \sum y$. PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence $x_3$ of elements of $Y$ for every finite sequence $y$ of elements of $\mathbb{R}$ such that $\$_1 = \operatorname{len} x_3$ and $\operatorname{len} x_3 = \operatorname{len} y$ and for every element $i$ of $\mathbb{N}$ such that $i \in \operatorname{dom} x_3$ there exists a point $v$ of $Y$ such that $v = x_{3i}$ and $y(i) = \|v\|$ holds $\|\sum x_3\| \leqslant \sum y$. $\mathcal{P}[0]$ by [30, (43)], [12, (72)]. For every natural number $i$, $\mathcal{P}[i]$ from [2, Sch. 2]. $\square$

(10) Let us consider a real normed space $Y$, a finite sequence $p$ of elements of $Y$, and a finite sequence $q$ of elements of $\mathbb{R}$. Suppose

(i) $\operatorname{len} p = \operatorname{len} q$, and

(ii) for every natural number $j$ such that $j \in \operatorname{dom} p$ holds $\|p_j\| \leqslant q(j)$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Then $\|\sum p\| \leqslant \sum q$. The theorem is a consequence of (9). PROOF: Define $\mathcal{Q}[\text{natural number}, \text{set}] \equiv$ there exists a point $v$ of $Y$ such that $v = p_{\$_1}$ and $\$_2 = \|v\|$. For every natural number $i$ such that $i \in \operatorname{Seg} \operatorname{len} p$ there exists an element $x$ of $\mathbb{R}$ such that $\mathcal{Q}[i, x]$. Consider $u$ being a finite sequence of elements of $\mathbb{R}$ such that $\operatorname{dom} u = \operatorname{Seg} \operatorname{len} p$ and for every natural number $i$ such that $i \in \operatorname{Seg} \operatorname{len} p$ holds $\mathcal{Q}[i, u(i)]$ from [4, Sch. 5]. For every element $i$ of $\mathbb{N}$ such that $i \in \operatorname{dom} p$ there exists a point $v$ of $Y$ such that $v = p_i$ and $u(i) = \|v\|$. $\square$

(11) Let us consider an element $j$ of $\mathbb{N}$, a non empty closed interval subset $A$ of $\mathbb{R}$, and a Division $D_1$ of $A$. Suppose $j \in \operatorname{dom} D_1$. Then $\operatorname{vol}(\operatorname{divset}(D_1, j)) \leqslant \delta_{D_1}$.

(12) Let us consider a non empty closed interval subset $A$ of $\mathbb{R}$, a Division $D$ of $A$, and a real number $r$. Suppose $\delta_D < r$. Let us consider a natural number $i$ and real numbers $s$, $t$. If $i \in \operatorname{dom} D$ and $s, t \in \operatorname{divset}(D, i)$, then $|s - t| < r$. The theorem is a consequence of (11).

(13) Let us consider a real Banach space $X$, a non empty closed interval subset $A$ of $\mathbb{R}$, and a function $h$ from $A$ into the carrier of $X$. Suppose a real number $r$. Suppose $0 < r$. Then there exists a real number $s$ such that

(i) $0 < s$, and

(ii) for every real numbers $x_1, x_2$ such that $x_1, x_2 \in \operatorname{dom} h$ and $|x_1 - x_2| < s$ holds $\|h_{x_1} - h_{x_2}\| < r$.

Let us consider a division sequence $T$ of $A$ and a middle volume sequence $S$ of $h$ and $T$. Suppose

(iii) $\delta_T$ is convergent, and

(iv) $\lim \delta_T = 0$.

Then middle $\operatorname{sum}(h, S)$ is convergent. The theorem is a consequence of (8), (7), (4), (12), (5), (10), and (6). PROOF: For every division sequence $T$ of $A$ and for every middle volume sequence $S$ of $h$ and $T$ such that $\delta_T$ is convergent and $\lim \delta_T = 0$ holds middle $\operatorname{sum}(h, S)$ is convergent by [32, (57)], [15, (9)], [17, (9)]. $\square$

The scheme *ExRealSeq2X* deals with a non empty set $\mathcal{D}$ and a unary functor $\mathcal{F}$, $\mathcal{G}$ yielding an element of $\mathcal{D}$ and states that

(Sch. 1) There exists a sequence $s$ of $\mathcal{D}$ such that for every natural number $n$, $s(2 \cdot n) = \mathcal{F}(n)$ and $s(2 \cdot n + 1) = \mathcal{G}(n)$.

Now we state the propositions:

(14) Let us consider a natural number $n$. Then there exists a natural number $k$ such that $n = 2 \cdot k$ or $n = 2 \cdot k + 1$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(15) Let us consider a non empty closed interval subset $A$ of $\mathbb{R}$ and division sequences $T_2$, $T$ of $A$. Then there exists a division sequence $T_1$ of $A$ such that for every natural number $i$, $T_1(2 \cdot i) = T_2(i)$ and $T_1(2 \cdot i + 1) = T(i)$. The theorem is a consequence of (14).

(16) Let us consider a non empty closed interval subset $A$ of $\mathbb{R}$ and division sequences $T_2$, $T$, $T_1$ of $A$. Suppose

(i) $\delta_{T_2}$ is convergent, and

(ii) $\lim \delta_{T_2} = 0$, and

(iii) $\delta_T$ is convergent, and

(iv) $\lim \delta_T = 0$, and

(v) for every natural number $i$, $T_1(2 \cdot i) = T_2(i)$ and $T_1(2 \cdot i + 1) = T(i)$.

Then

(vi) $\delta_{T_1}$ is convergent, and

(vii) $\lim \delta_{T_1} = 0$.

The theorem is a consequence of (14).

(17) Let us consider a real normed space $X$, a non empty closed interval subset $A$ of $\mathbb{R}$, a function $h$ from $A$ into the carrier of $X$, division sequences $T_2$, $T$, $T_1$ of $A$, a middle volume sequence $S_7$ of $h$ and $T_2$, and a middle volume sequence $S$ of $h$ and $T$. Suppose a natural number $i$. Then

(i) $T_1(2 \cdot i) = T_2(i)$, and

(ii) $T_1(2 \cdot i + 1) = T(i)$.

Then there exists a middle volume sequence $S_1$ of $h$ and $T_1$ such that for every natural number $i$, $S_1(2 \cdot i) = S_7(i)$ and $S_1(2 \cdot i + 1) = S(i)$. The theorem is a consequence of (14). PROOF: Reconsider $S_2 = S_7$, $S_3 = S$ as a sequence of (the carrier of $X)^*$. Define $\mathcal{F}$(natural number) $=$ $S_{2\$_1}$. Define $\mathcal{G}$(natural number) $= S_{3\$_1}$. Consider $S_1$ being a sequence of (the carrier of $X)^*$ such that for every natural number $n$, $S_1(2 \cdot n) = \mathcal{F}(n)$ and $S_1(2 \cdot n+1) = \mathcal{G}(n)$ from *ExRealSeq2X*. For every element $i$ of $\mathbb{N}$, $S_1(i)$ is a middle volume of $h$ and $T_1(i)$. $\square$

(18) Let us consider a real normed space $X$ and sequences $S_4$, $S_6$, $S_5$ of $X$. Suppose

(i) $S_5$ is convergent, and

(ii) for every natural number $i$, $S_5(2 \cdot i) = S_4(i)$ and $S_5(2 \cdot i + 1) = S_6(i)$.

Then

(iii) $S_4$ is convergent, and

(iv) $\lim S_4 = \lim S_5$, and

(v) $S_6$ is convergent, and

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(vi) $\lim S_6 = \lim S_5$.

The theorem is a consequence of (14). Proof: For every real number $r$ such that $0 < r$ there exists a natural number $m_1$ such that for every natural number $i$ such that $m_1 \leqslant i$ holds $\|S_4(i) - \lim S_5\| < r$ by [2, (11)]. For every real number $r$ such that $0 < r$ there exists a natural number $m_1$ such that for every natural number $i$ such that $m_1 \leqslant i$ holds $\|S_6(i) - \lim S_5\| < r$ by [2, (11)]. □

(19) Let us consider a real Banach space $X$ and a continuous partial function $f$ from $\mathbb{R}$ to the carrier of $X$. If $a \leqslant b$ and $[a, b] \subseteq \operatorname{dom} f$, then $f$ is integrable on $[a, b]$. The theorem is a consequence of (3), (13), (15), (17), (16), and (18). Proof: Set $A = [a, b]$. Reconsider $h = f \restriction A$ as a function from $A$ into the carrier of $X$. Consider $T_2$ being a division sequence of $A$ such that $\delta_{T_2}$ is convergent and $\lim \delta_{T_2} = 0$. Set $S_7 =$ the middle volume sequence of $h$ and $T_2$. Set $I = \lim \text{middle sum}(h, S_7)$. For every division sequence $T$ of $A$ and for every middle volume sequence $S$ of $h$ and $T$ such that $\delta_T$ is convergent and $\lim \delta_T = 0$ holds middle sum$(h, S)$ is convergent and $\lim \text{middle sum}(h, S) = I$. □

## References


[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[5] Józef Białas. Properties of the intervals of real numbers. *Formalized Mathematics*, 3(**2**):263–269, 1992.

[6] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[7] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[8] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[9] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[10] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[11] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[12] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[13] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[14] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[15] Noboru Endou and Artur Korniłowicz. The definition of the Riemann definite integral and some related lemmas. *Formalized Mathematics*, 8(**1**):93–102, 1999.

[16] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Scalar multiple of Riemann definite integral. *Formalized Mathematics*, 9(**1**):191–196, 2001.

[17] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Darboux's theorem. *Formalized Mathematics*, 9(**1**):197–200, 2001.

[18] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definition of integrability for


Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

partial functions from $\mathbb{R}$ to $\mathbb{R}$ and integrability for continuous functions. *Formalized Mathematics*, 9(**2**):281–284, 2001.

[19] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[20] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.

[21] Keiichi Miyajima, Takahiro Kato, and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into real normed space. *Formalized Mathematics*, 19(**1**):17–22, 2011. doi:10.2478/v10037-011-0003-8.

[22] Adam Naumowicz. Conjugate sequences, bounded complex sequences and convergent complex sequences. *Formalized Mathematics*, 6(**2**):265–268, 1997.

[23] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. More on continuous functions on normed linear spaces. *Formalized Mathematics*, 19(**1**):45–49, 2011. doi:10.2478/v10037-011-0008-3.

[24] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.

[25] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.

[26] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.

[27] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[28] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[29] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[30] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[33] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

*Received June 18, 2013*

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 153–162, 2013
DOI: 10.2478/forma-2013-0017

VERSITA
degruyter.com/view/j/forma

# On Square-Free Numbers

Adam Grabowski
Institute of Informatics
University of Białystok
Akademicka 2, 15-267 Białystok
Poland

**Summary.** In the article the formal characterization of square-free numbers is shown; in this manner the paper is the continuation of [19]. Essentially, we prepared some lemmas for convenient work with numbers (including the proof that the sequence of prime reciprocals diverges [1]) according to [18] which were absent in the Mizar Mathematical Library. Some of them were expressed in terms of clusters' registrations, enabling automatization machinery available in the Mizar system. Our main result of the article is in the final section; we proved that the lattice of positive divisors of a positive integer $n$ is Boolean if and only if $n$ is square-free.

MSC: 11A51 03B35

Keywords: square-free numbers; prime reciprocals; lattice of natural divisors

MML identifier: `MOEBIUS2`, version: `8.1.02 5.18.1182`

The notation and terminology used in this paper have been introduced in the following articles: [8], [2], [3], [30], [34], [6], [9], [16], [10], [11], [39], [27], [31], [42], [36], [19], [4], [23], [15], [26], [5], [12], [22], [37], [17], [20], [7], [41], [13], [25], [33], [32], [38], [40], [21], and [14].

## 1. Preliminaries

Let $a$, $b$ be non zero natural numbers. Let us observe that $\gcd(a,b)$ is non zero and $\mathrm{lcm}(a,b)$ is non zero.

Let $n$ be a natural number. Note that $0 -' n$ reduces to 0.

Now we state the propositions:

(1) Let us consider natural numbers $n$, $i$. If $n \geqslant 2^{2 \cdot i+2}$, then $\frac{n}{2} \geqslant 2^i \cdot \sqrt{n}$.

(2) Let us consider a natural number $n$. Then support $\mathrm{PFExp}(n) \subseteq \mathbb{P}$.

© 2013 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(Print), 1898-9934(Online)



Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

Let us consider a non zero natural number $n$. Now we state the propositions:

(3) $n - (n \operatorname{div} 2) \cdot 2 \leqslant 1$.

(4) $(n \operatorname{div} 2) \cdot 2 \leqslant n$.

Now we state the propositions:

(5) Let us consider non zero natural numbers $a$, $b$. Suppose $a$ and $b$ are not relatively prime. Then there exists a non zero natural number $k$ such that

- (i) $k \neq 1$, and
- (ii) $k \mid a$, and
- (iii) $k \mid b$.

(6) Let us consider non zero natural numbers $n$, $a$. If $a \mid n$, then $n \operatorname{div} a \neq 0$.

(7) Let us consider natural numbers $i$, $j$. If $i$ and $j$ are relatively prime, then $\operatorname{lcm}(i, j) = i \cdot j$.

Let $f$ be a natural-valued finite sequence. Let us note that $\prod f$ is natural.

## 2. Prime Numbers

Now we state the propositions:

(8) $\operatorname{pr}(0) = 2$.

(9) $\mathbb{P}(3) = \{2\}$. Proof: For every natural number $q$, $q \in \{2\}$ iff $q < 3$ and $q$ is prime by [27, (28)], [4, (13)]. $\square$

(10) $\operatorname{pr}(1) = 3$. The theorem is a consequence of (9).

(11) $\mathbb{P}(5) = \{2, 3\}$. Proof: For every natural number $q$, $q \in \{2, 3\}$ iff $q < 5$ and $q$ is prime by [27, (28)], [17, (41)], [4, (13)]. $\square$

(12) $\operatorname{pr}(2) = 5$. The theorem is a consequence of (11).

(13) $\mathbb{P}(6) = \{2, 3, 5\}$. Proof: $\{2, 3, 5\} \subseteq \mathbb{N}$. For every natural number $q$, $q \in \{2, 3, 5\}$ iff $q < 6$ and $q$ is prime by [27, (28)], [17, (41), (59)]. $\square$

(14) $\mathbb{P}(7) = \{2, 3, 5\}$. Proof: $\{2, 3, 5\} \subseteq \mathbb{N}$. For every natural number $q$, $q \in \{2, 3, 5\}$ iff $q < 7$ and $q$ is prime by [27, (28)], [17, (41), (59)]. $\square$

(15) $\operatorname{pr}(3) = 7$. The theorem is a consequence of (14).

(16) $\mathbb{P}(11) = \{2, 3, 5, 7\}$. Proof: $\{2, 3, 5, 7\} \subseteq \mathbb{N}$. For every natural number $q$, $q \in \{2, 3, 5, 7\}$ iff $q < 11$ and $q$ is prime by [27, (28)], [17, (41), (59)]. $\square$

(17) $\operatorname{pr}(4) = 11$. The theorem is a consequence of (16).

(18) $\mathbb{P}(13) = \{2, 3, 5, 7, 11\}$. Proof: $\{2, 3, 5, 7, 11\} \subseteq \mathbb{N}$. For every natural number $q$, $q \in \{2, 3, 5, 7, 11\}$ iff $q < 13$ and $q$ is prime by [27, (28)], [17, (41), (59)]. $\square$

(19) $\operatorname{pr}(5) = 13$.

(20) Let us consider natural numbers $m$, $n$. Then

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(i) $\mathbb{P}(m) \subseteq \mathbb{P}(n)$, or

(ii) $\mathbb{P}(n) \subseteq \mathbb{P}(m)$.

(21) Let us consider natural numbers $n$, $m$. Then $n < m$ if and only if $\mathrm{pr}(n) < \mathrm{pr}(m)$. PROOF: For every natural numbers $n$, $m$ such that $n < m$ holds $\mathrm{pr}(n) < \mathrm{pr}(m)$ by [2, (11)], [26, (69)], [4, (39)]. □

## 3. PRIME RECIPROCALS

In this paper $n$, $i$ denote natural numbers.

The functor $\mathrm{inv}_{\mathbb{P}}$ yielding a sequence of real numbers is defined by

(Def. 1) Let us consider a natural number $i$. Then $it(i) = \frac{1}{\mathrm{pr}(i)}$.

Let $f$ be a sequence of real numbers. We introduce $f$ is divergent as an antonym for $f$ is convergent.

Let us note that $\mathrm{inv}_{\mathbb{P}}$ is decreasing and lower bounded and $\mathrm{inv}_{\mathbb{P}}$ is convergent.

The functor $\mathrm{inv}_{\mathbb{N}}$ yielding a sequence of real numbers is defined by

(Def. 2) Let us consider a natural number $i$. Then $it(i) = \frac{1}{i}$.

Let us note that $\mathrm{inv}_{\mathbb{N}}$ is non-negative yielding and $\mathrm{inv}_{\mathbb{N}}$ is convergent.

Now we state the propositions:

(22) $\lim \mathrm{inv}_{\mathbb{N}} = 0$.

(23) $\mathrm{inv}_{\mathbb{P}}$ is a subsequence of $\mathrm{inv}_{\mathbb{N}}$. The theorem is a consequence of (21). PROOF: Define $\mathcal{F}(\text{natural number}) = \mathrm{pr}(\$_1)$. Consider $f$ being a sequence of real numbers such that for every natural number $i$, $f(i) = \mathcal{F}(i)$ from [24, Sch. 1]. For every natural number $n$, $f(n)$ is an element of $\mathbb{N}$. For every natural numbers $n$, $m$ such that $n < m$ holds $f(n) < f(m)$. $\mathrm{inv}_{\mathbb{P}} = \mathrm{inv}_{\mathbb{N}} \cdot f$ by [10, (13)]. □

Let $f$ be a non-negative yielding sequence of real numbers. One can verify that every subsequence of $f$ is non-negative yielding and $\mathrm{inv}_{\mathbb{P}}$ is non-negative yielding.

Now we state the proposition:

(24) $\lim \mathrm{inv}_{\mathbb{P}} = 0$.

Observe that $(\sum_{\alpha=0}^{\kappa}(\mathrm{inv}_{\mathbb{P}})(\alpha))_{\kappa\in\mathbb{N}}$ is non-decreasing as a sequence of real numbers.

Now we state the proposition:

(25) Let us consider a non-negative yielding sequence $f$ of real numbers. Suppose $f$ is summable. Let us consider a real number $p$. Suppose $p > 0$. Then there exists an element $i$ of $\mathbb{N}$ such that $\sum(f \uparrow i) < p$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

## 4. Square Factors

Let $n$ be a non zero natural number. The functor $\mathrm{SqFactors}\, n$ yielding a many sorted set indexed by $\mathbb{P}$ is defined by

(Def. 3) (i) support $it$ = support $\mathrm{PFExp}(n)$, and

(ii) for every natural number $p$ such that $p \in \mathrm{support}\, \mathrm{PFExp}(n)$ holds $it(p) = p^{(p\text{-count}(n)) \operatorname{div} 2}$.

Let us observe that $\mathrm{SqFactors}\, n$ is finite-support and natural-valued.

Note that every element of support $\mathrm{SqFactors}\, n$ is natural.

The functor $\mathrm{SqF}\, n$ yielding a natural number is defined by the term

(Def. 4) $\prod \mathrm{SqFactors}\, n$.

Now we state the proposition:

(26) Let us consider a bag $f$ of $\mathbb{P}$. Then $\prod f \neq 0$.

Let $n$ be a non zero natural number. Let us observe that $\mathrm{SqF}\, n$ is non zero.

Let $p$ be a prime number. The functor $\mathrm{SqFDiv}\, p$ yielding a subset of $\mathbb{N}$ is defined by

(Def. 5) Let us consider a natural number $n$. Then $n \in it$ if and only if $n$ is square-free and for every prime number $i$ such that $i \mid n$ holds $i \leqslant p$.

In the sequel $p$ denotes a prime number.

Now we state the propositions:

(27) $1 \in \mathrm{SqFDiv}\, p$. Proof: For every prime number $i$ such that $i \mid 1$ holds $i \leqslant p$ by [21, (15)]. □

(28) $0 \notin \mathrm{SqFDiv}\, p$.

Let us note that there exists a natural number which is square-free and non zero.

Let us consider $p$. One can verify that there exists a bag of $\mathrm{Seg}\, p$ which is positive yielding.

Now we state the propositions:

(29) Let us consider a positive yielding bag $f$ of $\mathrm{Seg}\, p$. Then $\mathrm{dom}\, f = \mathrm{support}\, f$. Proof: $\mathrm{Seg}\, p \subseteq \mathrm{support}\, f$ by [10, (3)]. □

(30) $\mathrm{dom}\, \mathrm{CFS}(\mathrm{Seg}\, p) = \mathrm{Seg}\, p$.

(31) Let us consider a finite set $A$. Then $\mathrm{dom}\, \mathrm{CFS}(A) = \mathrm{Seg}\, \overline{\overline{A}}$.

(32) Let us consider a positive yielding bag $g$ of $\mathrm{Seg}\, p$. If $g = p \longmapsto p$, then $g = g \cdot \mathrm{CFS}(\mathrm{support}\, g)$. The theorem is a consequence of (29) and (30). Proof: Set $g = f \cdot \mathrm{CFS}(\mathrm{Seg}\, p)$. For every element $x$ such that $x \in \mathrm{dom}\, g$ holds $g(x) = p \longmapsto p(x)$ by [10, (12)], [35, (7)], [10, (3)]. □

(33) Let us consider a positive yielding bag $f$ of $\mathrm{Seg}\, p$. If $f = p \longmapsto p$, then $\prod f = p^p$. The theorem is a consequence of (32).

Let us consider a non zero natural number $n$. Now we state the propositions:

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(34) If $n \in \mathrm{SqFDiv}\, p$, then $\underline{\mathrm{support\,PFExp}(n)} \subseteq \mathrm{Seg}\, p$.

(35) If $n \in \mathrm{SqFDiv}\, p$, then $\overline{\overline{\mathrm{support\,PFExp}(n)}} \leqslant p$.

Now we state the propositions:

(36) Let us consider a square-free non zero natural number $n$. Then $\mathrm{rng\,PFExp}(n) \subseteq \{0,1\}$.

(37) Let us consider non zero natural numbers $m$, $n$. If $\mathrm{PFExp}(m) = \mathrm{PFExp}(n)$, then $m = n$. Proof: For every element $x$ such that $x \in \mathrm{dom\,PPF}(m)$ holds $(\mathrm{PPF}(m))(x) = (\mathrm{PPF}(n))(x)$ by [23, (33)]. □

Let $p$ be a prime number. Observe that $\mathrm{SqFDiv}\, p$ is non empty.

Note that every element of $\mathrm{SqFDiv}\, p$ is non empty.

The functor $2^{\mathbb{P}}(p)$ yielding a set is defined by the term

(Def. 6) $2^{\mathrm{Seg}\, p \cap \mathbb{P}}$.

Let us note that $2^{\mathbb{P}}(p)$ is finite.

The functor $\mathrm{Hom}_{\mathbb{P}}(p)$ yielding a function from $\mathrm{SqFDiv}\, p$ into $2^{\mathbb{P}}(p)$ is defined by

(Def. 7) Let us consider an element $x$ of $\mathrm{SqFDiv}\, p$. Then $it(x) = \mathrm{PFExp}(x) \restriction (\mathrm{Seg}\, p \cap \mathbb{P})$.

Observe that $\mathrm{Hom}_{\mathbb{P}}(p)$ is one-to-one.

Now we state the proposition:

(38) $\overline{\overline{\mathrm{SqFDiv}\, p}} \subseteq \overline{\overline{2^{\mathbb{P}}(p)}}$.

Let $p$ be a prime number. One can verify that $\mathrm{SqFDiv}\, p$ is finite.

Now we state the propositions:

(39) $\overline{\overline{\mathrm{SqFDiv}\, p}} \leqslant 2^p$.

(40) If $n \neq 0$ and $p^i \mid n$, then $i \leqslant p\text{-count}(n)$.

(41) If $n \neq 0$ and for every prime number $p$, $p\text{-count}(n) \leqslant 1$, then $n$ is square-free. The theorem is a consequence of (40).

(42) Let us consider a prime number $p$ and a non zero natural number $n$. If $p\text{-count}(n) = 0$, then $(\mathrm{SqFactors}\, n)(p) = 0$.

(43) Let us consider a non zero natural number $n$ and a prime number $p$. Suppose $p\text{-count}(n) \neq 0$. Then $(\mathrm{SqFactors}\, n)(p) = p^{(p\text{-count}(n)) \operatorname{div} 2}$.

(44) Let us consider non zero natural numbers $m$, $n$. Suppose $m$ and $n$ are relatively prime. Then $\mathrm{SqFactors}(m \cdot n) = \mathrm{SqFactors}\, m + \mathrm{SqFactors}\, n$. The theorem is a consequence of (42) and (43).

(45) Let us consider a non zero natural number $n$. Then $\mathrm{SqF}\, n \mid n$. The theorem is a consequence of (44). Proof: Define $\mathcal{F}(\text{non zero natural number}) = \prod \mathrm{SqFactors}\, \$_1$. Define $\mathcal{G}(\text{non zero natural number}) = \mathrm{SqFactors}\, \$_1$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every non zero natural number $n$ such that $\mathrm{support}\, \mathcal{G}(n) \subseteq \mathrm{Seg}\, \$_1$ holds $\mathcal{F}(n) \mid n$. For every natural number

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

$k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (1)], [4, (13)], [23, (34), (42)]. $\mathcal{P}[0]$ by [23, (20)]. For every natural number $k$, $\mathcal{P}[k]$ from [4, Sch. 2]. $\square$

Let $n$ be a non zero natural number. One can check that PFactors $n$ is prime-factorization-like.

Let us consider a bag $f$ of $\mathbb{P}$. Now we state the propositions:

(46) There exists a finite sequence $g$ of elements of $\mathbb{N}$ such that

(i) $\prod f = \prod g$, and

(ii) $g = f \cdot \mathrm{CFS}(\mathrm{support}\, f)$.

(47) If $f(p) = p^n$, then $p^n \mid \prod f$.

(48) If $f(p) = p^n$, then $p$-count$(\prod f) \geqslant n$.

## 5. Extracting Square-containing and Square-free Part of a Number

Let $n$ be a non zero natural number. The functor TSqFactors $n$ yielding a many sorted set indexed by $\mathbb{P}$ is defined by

(Def. 8) (i) support $it$ = support PFExp$(n)$, and

(ii) for every natural number $p$ such that $p \in$ support PFExp$(n)$ holds $it(p) = p^{2 \cdot ((p\text{-count}(n)) \,\mathrm{div}\, 2)}$.

Now we state the proposition:

(49) Let us consider a non zero natural number $n$. Then TSqFactors $n$ = (SqFactors $n)^2$. Proof: For every element $x$ such that $x \in$ dom TSqFactors $n$ holds (TSqFactors $n)(x)$ = (SqFactors $n)^2(x)$ by [26, (9), (11)]. $\square$

Let $n$ be a non zero natural number. Let us observe that TSqFactors $n$ is finite-support and natural-valued.

The functor TSqF $n$ yielding a natural number is defined by the term

(Def. 9) $\prod$ TSqFactors $n$.

Observe that TSqF $n$ is non zero.

Now we state the propositions:

(50) Let us consider a prime number $p$ and a non zero natural number $n$. If $p$-count$(n) = 0$, then (TSqFactors $n)(p) = 0$.

(51) Let us consider a non zero natural number $n$ and a prime number $p$. Suppose $p$-count$(n) \neq 0$. Then (TSqFactors $n)(p) = p^{2 \cdot ((p\text{-count}(n)) \,\mathrm{div}\, 2)}$.

(52) Let us consider non zero natural numbers $m$, $n$. Suppose $m$ and $n$ are relatively prime. Then TSqFactors$(m \cdot n)$ = TSqFactors $m$ + TSqFactors $n$. The theorem is a consequence of (50) and (51).

Let $n$ be a non zero natural number. One can check that support TSqFactors $n$ is natural-membered.

Now we state the proposition:

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(53) Let us consider a non zero natural number $n$. Then $\mathrm{TSqF}\,n \mid n$. The theorem is a consequence of (4) and (52). Proof: Define $\mathcal{F}$(non zero natural number) $= \prod \mathrm{TSqFactors}\,\$_1$. Define $\mathcal{G}$(non zero natural number) $=$ TSqFactors $\$_1$. Define $\mathcal{P}$[natural number] $\equiv$ for every non zero natural number $n$ such that support $\mathcal{G}(n) \subseteq \mathrm{Seg}\,\$_1$ holds $\mathcal{F}(n) \mid n$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (1)], [4, (13)], [23, (34), (42)]. $\mathcal{P}[0]$ by [23, (20)]. For every natural number $k$, $\mathcal{P}[k]$ from [4, Sch. 2]. $\square$

Let $n$ be a non zero natural number. Let us note that $n \,\mathrm{div}\, \mathrm{TSqF}\,n$ is square-free as a natural number.

Now we state the propositions:

(54) Let us consider non zero natural numbers $n$, $k$. If $k \neq 1$ and $k^{\mathbf{2}} \mid n$, then $n$ is square-containing.

(55) Let us consider a square-free non zero natural number $n$ and a non zero natural number $a$. If $a \mid n$, then $a$ and $n \,\mathrm{div}\, a$ are relatively prime. The theorem is a consequence of (5) and (54). Proof: $n \,\mathrm{div}\, a \neq 0$ by [29, (12)]. Consider $k$ being a non zero natural number such that $k \neq 1$ and $k \mid a$ and $k \mid n \,\mathrm{div}\, a$. $\square$

## 6. Binary Operations

Now we state the propositions:

(56) Let us consider non empty sets $A$, $C$, a commutative binary operation $L$ on $A$, and a binary operation $L_1$ on $C$. If $C \subseteq A$ and $L_1 = L \restriction C$, then $L_1$ is commutative. Proof: For every elements $a$, $b$ of $C$, $L_1(a, b) = L_1(b, a)$ by [14, (87)], [10, (49)]. $\square$

(57) Let us consider non empty sets $A$, $C$, an associative binary operation $L$ on $A$, and a binary operation $L_1$ on $C$. If $C \subseteq A$ and $L_1 = L \restriction C$, then $L_1$ is associative. Proof: For every elements $a$, $b$, $c$ of $C$, $L_1(a, L_1(b, c)) = L_1(L_1(a, b), c)$ by [14, (87)], [10, (49), (47)]. $\square$

Let $C$ be a non empty set, $L$ be a commutative binary operation on $C$, and $M$ be a binary operation on $C$. Note that $\langle C, L, M \rangle$ is join-commutative.

Let $L$ be a binary operation on $C$ and $M$ be a commutative binary operation on $C$. Let us observe that $\langle C, L, M \rangle$ is meet-commutative.

Let $L$ be an associative binary operation on $C$ and $M$ be a binary operation on $C$. Note that $\langle C, L, M \rangle$ is join-associative.

Let $L$ be a binary operation on $C$ and $M$ be an associative binary operation on $C$. Let us observe that $\langle C, L, M \rangle$ is meet-associative.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

## 7. On the Natural Divisors

Now we state the proposition:

(58) Let us consider a non zero natural number $n$. Then the set of positive divisors of $n \subseteq \mathbb{N}^+$.

Let us consider a non zero natural number $n$ and natural numbers $x$, $y$. Now we state the propositions:

(59) Suppose $x, y \in$ the set of positive divisors of $n$. Then $\mathrm{lcm}(x, y) \in$ the set of positive divisors of $n$.

(60) Suppose $x, y \in$ the set of positive divisors of $n$. Then $\gcd(x, y) \in$ the set of positive divisors of $n$.

Let $n$ be a non zero natural number. Note that the set of positive divisors of $n$ is non empty and $\gcd_{\mathbb{N}}$ is commutative and associative and $\mathrm{lcm}_{\mathbb{N}}$ is commutative and associative.

Now we state the propositions:

(61) $\gcd_{\mathbb{N}^+} = \gcd_{\mathbb{N}} \restriction \mathbb{N}^+$. Proof: Set $h_1 = \gcd_{\mathbb{N}^+}$. Set $h = \gcd_{\mathbb{N}}$. Set $N = \mathbb{N}^+$. $h_1 = h \restriction (N \times N)$ by [41, (62)], [10, (49), (2)]. $\square$

(62) $\mathrm{lcm}_{\mathbb{N}^+} = \mathrm{lcm}_{\mathbb{N}} \restriction \mathbb{N}^+$. Proof: Set $h_1 = \mathrm{lcm}_{\mathbb{N}^+}$. Set $h = \mathrm{lcm}_{\mathbb{N}}$. Set $N = \mathbb{N}^+$. $h_1 = h \restriction (N \times N)$ by [41, (62)], [10, (49), (2)]. $\square$

Let us observe that $\gcd_{\mathbb{N}^+}$ is commutative and $\mathrm{lcm}_{\mathbb{N}^+}$ is commutative and $\gcd_{\mathbb{N}^+}$ is associative and $\mathrm{lcm}_{\mathbb{N}^+}$ is associative.

## 8. The Lattice of Natural Divisors

Let $n$ be a non zero natural number. The lattice of positive divisors of $n$ yielding a strict sublattice of $\mathbb{L}_{\mathbb{N}^+}$ is defined by

(Def. 10) The carrier of $it =$ the set of positive divisors of $n$.

One can check that the carrier of the lattice of positive divisors of $n$ is natural-membered.

Now we state the proposition:

(63) Let us consider a non zero natural number $n$ and elements $a$, $b$ of the lattice of positive divisors of $n$. Then

(i) $a \sqcup b = \mathrm{lcm}(a, b)$, and

(ii) $a \sqcap b = \gcd(a, b)$.

Let $n$ be a non zero natural number and $p$, $q$ be elements of the lattice of positive divisors of $n$. We identify $\mathrm{lcm}(p, q)$ with $p \sqcup q$. We identify $\gcd(p, q)$ with $p \sqcap q$. Let us note that the lattice of positive divisors of $n$ is non empty.

Note that the lattice of positive divisors of $n$ is distributive and bounded.

Now we state the proposition:

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

(64) Let us consider a non zero natural number $n$. Then

(i) $\top_\alpha = n$, and

(ii) $\bot_\alpha = 1$,

where $\alpha$ is the lattice of positive divisors of $n$. PROOF: Set $L =$ the lattice of positive divisors of $n$. Reconsider $T = n$ as an element of $L$. For every element $a$ of $L$, $T \sqcup a = T$ and $a \sqcup T = T$ by [26, (44)], [19, (39)]. □

Let $n$ be a square-free non zero natural number. One can verify that the lattice of positive divisors of $n$ is Boolean.

Let $n$ be a non zero natural number. One can verify that every element of the lattice of positive divisors of $n$ is non zero.

Now we state the proposition:

(65) Let us consider a non zero natural number $n$. Then the lattice of positive divisors of $n$ is Boolean if and only if $n$ is square-free. The theorem is a consequence of (64) and (7). PROOF: Set $L =$ the lattice of positive divisors of $n$. If $L$ is Boolean, then $n$ is square-free by [26, (81)], [19, (39)], [28, (7)]. □

## REFERENCES


[1] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK*. Springer-Verlag, Berlin Heidelberg New York, 2004.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

[4] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[5] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[7] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

[8] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[9] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[10] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[11] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[12] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[13] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[14] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[15] Marek Chmur. The lattice of natural numbers and the sublattice of it. The set of prime numbers. *Formalized Mathematics*, 2(**4**):453–459, 1991.

[16] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[17] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.

[18] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1980.


Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM

[19] Magdalena Jastrzębska and Adam Grabowski. On the properties of the Möbius function. *Formalized Mathematics*, 14(**1**):29–36, 2006. doi:10.2478/v10037-006-0005-0.

[20] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[21] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**): 573–577, 1997.

[22] Artur Korniłowicz. On the real valued functions. *Formalized Mathematics*, 13(**1**):181–187, 2005.

[23] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.

[24] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[25] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.

[26] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[27] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[28] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(**4**):181–187, 2007. doi:10.2478/v10037-007-0022-7.

[29] Robert Milewski. Natural numbers. *Formalized Mathematics*, 7(**1**):19–22, 1998.

[30] Adam Naumowicz. Conjugate sequences, bounded complex sequences and convergent complex sequences. *Formalized Mathematics*, 6(**2**):265–268, 1997.

[31] Hiroyuki Okazaki and Yasunari Shidama. Uniqueness of factoring an integer and multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$. *Formalized Mathematics*, 16(**2**):103–107, 2008. doi:10.2478/v10037-008-0015-1.

[32] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[33] Konrad Raczkowski and Andrzej Nędzusiak. Series. *Formalized Mathematics*, 2(**4**):449–452, 1991.

[34] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[35] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[36] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[37] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.

[38] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[39] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[40] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[41] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[42] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

*Received July 12, 2013*

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated | 212.33.72.148
Download Date | 2/27/14 10:42 AM