Contents

Formaliz. Math. 20 (**1**)

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 1–5, 2012
DOI: 10.2478/v10037-012-0001-5

VERSITA
versita.com/fm/

Elementary Introduction to Stochastic Finance in Discrete Time

Peter Jaeger
Ludwig Maximilians University of Munich
Germany

Summary. This article gives an elementary introduction to stochastic finance (in discrete time). A formalization of random variables is given and some elements of Borel sets are considered. Furthermore, special functions (for buying a present portfolio and the value of a portfolio in the future) and some statements about the relation between these functions are introduced. For details see: [8] (p. 185), [7] (pp. 12, 20), [6] (pp. 3–6).

MML identifier: FINANCE1, version: 7.12.01 4.167.1133

The notation and terminology used in this paper have been introduced in the following papers: [15], [2], [1], [3], [4], [11], [10], [9], [5], [14], [12], and [13].

We use the following convention: O_1, O_2 are non empty sets, S_1, F are σ-fields of subsets of O_1, and S_2, F_2 are σ-fields of subsets of O_2.

Let a, r be real numbers. We introduce the halfline finance of a and r as a synonym of $[a, r[$. Then the halfline finance of a and r is a subset of $\mathbb{R}$.

We now state two propositions:

(1) For every real number k holds $\mathbb{R} \setminus [k, +\infty[=]-\infty, k[$.

(2) For every real number k holds $\mathbb{R} \setminus]-\infty, k[= [k, +\infty[$.

Let a, b be real numbers. The half open sets of a and b yields a sequence of subsets of $\mathbb{R}$ and is defined by the conditions (Def. 1).

(Def. 1)(i) (The half open sets of a and b)(0) = the halfline finance of a and $b + 1$, and

(ii) for every element n of $\mathbb{N}$ holds (the half open sets of a and b)$(n+1)$ = the halfline finance of a and $b + \frac{1}{n+1}$.

A sequence of real numbers is said to be a price function if:

ISSN 1426–2630(p), 1898-9934(e)

(Def. 2) $\mathrm{It}(0) = 1$ and for every element n of $\mathbb{N}$ holds $\mathrm{it}(n) \geq 0$.

Let p_1, j_1 be sequences of real numbers. We introduce the elements of buy portfolio of p_1 and j_1 as a synonym of $p_1 \cdot j_1$. Then the elements of buy portfolio of p_1 and j_1 is a sequence of real numbers.

Let d be a natural number. The buy portfolio extension of p_1, j_1, and d yields an element of $\mathbb{R}$ and is defined as follows:

(Def. 3) The buy portfolio extension of p_1, j_1, and $d = (\sum_{\alpha=0}^{\kappa}(\text{the elements of buy portfolio of } p_1 \text{ and } j_1)(\alpha))_{\kappa\in\mathbb{N}}(d)$.

The buy portfolio of p_1, j_1, and d yielding an element of $\mathbb{R}$ is defined as follows:

(Def. 4) The buy portfolio of p_1, j_1, and $d = (\sum_{\alpha=0}^{\kappa}((\text{the elements of buy portfolio of } p_1 \text{ and } j_1) \uparrow 1)(\alpha))_{\kappa\in\mathbb{N}}(d-1)$.

Let O_1, O_2 be sets, let S_1 be a σ-field of subsets of O_1, let S_2 be a σ-field of subsets of O_2, and let X be a function. We say that X is random variable on S_1 and S_2 if and only if:

(Def. 5) For every element x of S_2 holds $\{y \in O_1 \colon X(y) \text{ is an element of } x\}$ is an element of S_1.

Let O_1, O_2 be sets, let F be a σ-field of subsets of O_1, and let F_2 be a σ-field of subsets of O_2. The set of random variables on F and F_2 is defined by:

(Def. 6) The set of random variables on F and $F_2 = \{f : O_1 \to O_2 \colon f \text{ is random variable on } F \text{ and } F_2\}$.

Let us consider O_1, O_2, F, F_2. One can check that the set of random variables on F and F_2 is non empty.

Let O_1, O_2 be non empty sets, let F be a σ-field of subsets of O_1, let F_2 be a σ-field of subsets of O_2, and let X be a set. Let us assume that $X =$ the set of random variables on F and F_2. Let k be an element of X. The change element to function F, F_2, and k yielding a function from O_1 into O_2 is defined by:

(Def. 7) The change element to function F, F_2, and $k = k$.

Let O_1 be a non empty set, let F be a σ-field of subsets of O_1, let X be a non empty set, and let k be an element of X. The random variables for future elements of portfolio value of F and k yields a function from O_1 into $\mathbb{R}$ and is defined by the condition (Def. 8).

(Def. 8) Let w be an element of O_1. Then (the random variables for future elements of portfolio value of F and $k)(w) =$ (the change element to function F, the Borel sets, and $k)(w)$.

Let p be a natural number, let O_1, O_2 be non empty sets, let F be a σ-field of subsets of O_1, let F_2 be a σ-field of subsets of O_2, and let X be a set. Let us assume that $X =$ the set of random variables on F and F_2. Let G be a function from $\mathbb{N}$ into X. The element of F, F_2, G, and p yields a function from O_1 into O_2 and is defined as follows:

(Def. 9) The element of F, F_2, G, and $p = G(p)$.

Let r be a real number, let O_1 be a non empty set, let F be a σ-field of subsets of O_1, let X be a non empty set, let w be an element of O_1, let G be a function from $\mathbb{N}$ into X, and let p_1 be a sequence of real numbers. The future elements of portfolio value of r, p_1, F, w, and G yields a sequence of real numbers and is defined by the condition (Def. 10).

(Def. 10) Let n be an element of $\mathbb{N}$. Then (the future elements of portfolio value of r, p_1, F, w, and $G)(n) =$ (the random variables for future elements of portfolio value of F and $G(n))(w) \cdot p_1(n)$.

Let r be a real number, let d be a natural number, let p_1 be a sequence of real numbers, let O_1 be a non empty set, let F be a σ-field of subsets of O_1, let X be a non empty set, let G be a function from $\mathbb{N}$ into X, and let w be an element of O_1. The future portfolio value extension of r, d, p_1, F, G, and w yields an element of $\mathbb{R}$ and is defined by the condition (Def. 11).

(Def. 11) The future portfolio value extension of r, d, p_1, F, G, and $w =$ $(\sum_{\alpha=0}^{\kappa}$ (the future elements of portfolio value of r, p_1, F, w, and $G)(\alpha))_{\kappa\in\mathbb{N}}(d)$.

The future portfolio value of r, d, p_1, F, G, and w yields an element of $\mathbb{R}$ and is defined by the condition (Def. 12).

(Def. 12) The future portfolio value of r, d, p_1, F, G, and $w = (\sum_{\alpha=0}^{\kappa}$((the future elements of portfolio value of r, p_1, F, w, and $G) \upharpoonright 1)(\alpha))_{\kappa\in\mathbb{N}}(d-1)$.

Let us observe that there exists an element of the Borel sets which is non empty.

One can prove the following propositions:

(3) For every real number k holds $[k, +\infty[$ is an element of the Borel sets and $]-\infty, k[$ is an element of the Borel sets.

(4) For all real numbers k_1, k_2 holds $[k_2, k_1[$ is an element of the Borel sets.

(5) For all real numbers a, b holds Intersection (the half open sets of a and b) is an element of the Borel sets.

(6) For all real numbers a, b holds Intersection (the half open sets of a and $b) = [a, b]$.

(7) Let a, b be real numbers and n be a natural number. Then (the partial intersections of the half open sets of a and $b)(n)$ is an element of the Borel sets.

(8) For all real numbers k_1, k_2 holds $[k_2, k_1]$ is an element of the Borel sets.

(9) Let X be a function from O_1 into $\mathbb{R}$. Suppose X is random variable on S_1 and the Borel sets. Then for every real number k holds $\{w \in O_1$: $X(w) \geq k\}$ is an element of S_1 and $\{w \in O_1$: $X(w) < k\}$ is an element of S_1 and for all real numbers k_1, k_2 such that $k_1 < k_2$ holds $\{w \in O_1$: $k_1 \leq X(w) \ \wedge \ X(w) < k_2\}$ is an element of S_1 and for all real numbers k_1, k_2 such that $k_1 \leq k_2$ holds $\{w \in O_1$: $k_1 \leq X(w) \ \wedge \ X(w) \leq k_2\}$ is an

element of S_1 and for every real number r holds LE-dom$(X, r) = \{w \in O_1$: $X(w) < r\}$ and for every real number r holds GTE-dom$(X, r) = \{w \in O_1$: $X(w) \geq r\}$ and for every real number r holds EQ-dom$(X, r) = \{w \in O_1$: $X(w) = r\}$ and for every real number r holds EQ-dom(X, r) is an element of S_1.

(10) For every real number s holds $O_1 \longmapsto s$ is random variable on S_1 and the Borel sets.

(11) Let p_1 be a sequence of real numbers, j_1 be a price function, and d be a natural number. Suppose $d > 0$. Then the buy portfolio extension of p_1, j_1, and $d = p_1(0) +$ the buy portfolio of p_1, j_1, and d.

(12) Let d be a natural number. Suppose $d > 0$. Let r be a real number, p_1 be a sequence of real numbers, and G be a function from $\mathbb{N}$ into the set of random variables on F and the Borel sets. Suppose the element of F, the Borel sets, G, and $0 = O_1 \longmapsto 1 + r$. Let w be an element of O_1. Then the future portfolio value extension of r, d, p_1, F, G, and $w = (1+r) \cdot p_1(0) +$the future portfolio value of r, d, p_1, F, G, and w.

(13) Let d be a natural number. Suppose $d > 0$. Let r be a real number. Suppose $r > -1$. Let p_1 be a sequence of real numbers, j_1 be a price function, and G be a function from $\mathbb{N}$ into the set of random variables on F and the Borel sets. Suppose the element of F, the Borel sets, G, and $0 = O_1 \longmapsto 1 + r$. Let w be an element of O_1. Suppose the buy portfolio extension of p_1, j_1, and $d \leq 0$. Then the future portfolio value extension of r, d, p_1, F, G, and $w \leq$ (the future portfolio value of r, d, p_1, F, G, and $w) - (1 + r) \cdot$ the buy portfolio of p_1, j_1, and d.

(14) Let d be a natural number. Suppose $d > 0$. Let r be a real number. Suppose $r > -1$. Let p_1 be a sequence of real numbers, j_1 be a price function, and G be a function from $\mathbb{N}$ into the set of random variables on F and the Borel sets. Suppose the element of F, the Borel sets, G, and $0 = O_1 \longmapsto 1 + r$. Suppose the buy portfolio extension of p_1, j_1, and $d \leq 0$. Then

(i) $\{w \in O_1$: the future portfolio value extension of r, d, p_1, F, G, and $w \geq 0\} \subseteq \{w \in O_1$: the future portfolio value of r, d, p_1, F, G, and $w \geq (1 + r) \cdot$ the buy portfolio of p_1, j_1, and $d\}$, and

(ii) $\{w \in O_1$: the future portfolio value extension of r, d, p_1, F, G, and $w > 0\} \subseteq \{w \in O_1$: the future portfolio value of r, d, p_1, F, G, and $w > (1 + r) \cdot$ the buy portfolio of p_1, j_1, and $d\}$.

(15) Let f be a function from O_1 into $\mathbb{R}$. Suppose f is random variable on S_1 and the Borel sets. Then f is measurable on $\Omega_{(S_1)}$ and f is a real-valued random variable on S_1.

(16) The set of random variables on S_1 and the Borel sets $\subseteq$ the real-valued random variables set on S_1.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[5] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.
[6] Hans Föllmer and Alexander Schied. *Stochastic Finance: An Introduction in Discrete Time*, volume 27 of *Studies in Mathematics*. de Gruyter, Berlin, 2nd edition, 2004.
[7] Hans-Otto Georgii. *Stochastik, Einführung in die Wahrscheinlichkeitstheorie und Statistik*. deGruyter, Berlin, 2 edition, 2004.
[8] Achim Klenke. *Wahrscheinlichkeitstheorie*. Springer-Verlag, Berlin, Heidelberg, 2006.
[9] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[10] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.
[11] Konrad Raczkowski and Andrzej Nędzusiak. Series. *Formalized Mathematics*, 2(**4**):449–452, 1991.
[12] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[13] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[14] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[15] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received March 22, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 7–14, 2012
DOI: 10.2478/v10037-012-0002-4

VERSITA
versita.com/fm/

Valuation Theory. Part I

Grzegorz Bancerek
Białystok Technical University
Poland

Hidetsune Kobayashi
Department of Mathematics
College of Science and Technology
Nihon University
8 Kanda Surugadai Chiyoda-ku
101-8308 Tokyo
Japan

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

Summary. In the article we introduce a valuation function over a field [1]. Ring of non negative elements and its ideal of positive elements have been also defined.

MML identifier: `FVALUAT1`, version: `7.12.01 4.167.1133`

The notation and terminology used here have been introduced in the following papers: [11], [19], [4], [15], [20], [8], [21], [10], [9], [16], [3], [5], [7], [18], [17], [13], [14], [6], [2], and [12].

1. Extended Reals

We use the following convention: x, y, z, s are extended real numbers, i is an integer, and n, m are natural numbers.

The following propositions are true:

(1) If $x = -x$, then $x = 0$.

(2) If $x + x = 0$, then $x = 0$.

ISSN 1426–2630(p), 1898-9934(e)

(3) If $0 \leq x \leq y$ and $0 \leq s \leq z$, then $x \cdot s \leq y \cdot z$.

(4) If $y \neq +\infty$ and $0 < x$ and $0 < y$, then $0 < \frac{x}{y}$.

(5) If $y \neq +\infty$ and $x < 0 < y$, then $\frac{x}{y} < 0$.

(6) If $y \neq -\infty$ and $0 < x$ and $y < 0$, then $\frac{x}{y} < 0$.

(7) If x, $y \in \mathbb{R}$ or $z \in \mathbb{R}$, then $\frac{x+y}{z} = \frac{x}{z} + \frac{y}{z}$.

(8) If $y \neq +\infty$ and $y \neq -\infty$ and $y \neq 0$, then $\frac{x}{y} \cdot y = x$.

(9) If $y \neq -\infty$ and $y \neq +\infty$ and $x \neq 0$ and $y \neq 0$, then $\frac{x}{y} \neq 0$.

Let x be a number. We say that x is extended integer if and only if:

(Def. 1) x is integer or $x = +\infty$.

Let us mention that every number which is extended integer is also extended real.

One can verify the following observations:

* $+\infty$ is extended integer,
* $-\infty$ is non extended integer,
* $\overline{1}$ is extended integer, positive, and real,
* every number which is integer is also extended integer, and
* every number which is real and extended integer is also integer.

Let us observe that there exists an element of $\overline{\mathbb{R}}$ which is real, extended integer, and positive and there exists an extended integer number which is positive.

An extended integer is an extended integer number.

In the sequel x, y, v denote extended integers.

One can prove the following propositions:

(10) If $x < y$, then $x + 1 \leq y$.

(11) $-\infty < x$.

Let X be an extended real-membered set. Let us assume that there exists a positive extended integer i_0 such that $i_0 \in X$. The functor least-positive X yielding a positive extended integer is defined by:

(Def. 2) least-positive $X \in X$ and for every positive extended integer i such that $i \in X$ holds least-positive $X \leq i$.

Let f be a binary relation. We say that f is extended integer valued if and only if:

(Def. 3) For every set x such that $x \in \operatorname{rng} f$ holds x is extended integer.

Let us note that there exists a function which is extended integer valued.

Let A be a set. Note that there exists a function from A into $\overline{\mathbb{R}}$ which is extended integer valued.

Let f be an extended integer valued function and let x be a set. Note that $f(x)$ is extended integer.

2. STRUCTURES

One can prove the following proposition

(12) Let K be a distributive left unital add-associative right zeroed right complementable non empty double loop structure. Then $-1_K \cdot -1_K = 1_K$.

Let K be a non empty double loop structure, let S be a subset of K, and let n be a natural number. The functor S^n yielding a subset of K is defined by:

(Def. 4)(i) $S^n =$ the carrier of K if $n = 0$,

(ii) there exists a finite sequence f of elements of $2^{\text{the carrier of } K}$ such that $S^n = f(\operatorname{len} f)$ and $\operatorname{len} f = n$ and $f(1) = S$ and for every natural number i such that i, $i+1 \in \operatorname{dom} f$ holds $f(i+1) = S * f_i$, otherwise.

In the sequel A denotes a subset of D. The following propositions are true:

(13) $A^1 = A$.

(14) $A^2 = A * A$.

Let R be a ring, let S be an ideal of R, and let n be a natural number. Observe that S^n is non empty, add closed, left ideal, and right ideal.

Let G be a non empty double loop structure, let g be an element of G, and let i be an integer. The functor g^i yielding an element of G is defined as follows:

(Def. 5) $g^i = \begin{cases} \operatorname{power}_G(g, |i|), & \text{if } 0 \leq i, \\ \operatorname{power}_G(g, |i|)^{-1}, & \text{otherwise.} \end{cases}$

Let G be a non empty double loop structure, let g be an element of G, and let n be a natural number. Then g^n can be characterized by the condition:

(Def. 6) $g^n = \operatorname{power}_G(g, n)$.

In the sequel K is a field-like non degenerated associative add-associative right zeroed right complementable distributive Abelian non empty double loop structure and a, b, c are elements of K. We now state two propositions:

(15) $a^{n+m} = a^n \cdot a^m$.

(16) If $a \neq 0_K$, then $a^i \neq 0_K$.

3. VALUATION

Let K be a double loop structure. We say that K has a valuation if and only if the condition (Def. 7) is satisfied.

(Def. 7) There exists an extended integer valued function f from K into $\overline{\mathbb{R}}$ such that

(i) $f(0_K) = +\infty$,

(ii) for every element a of K such that $a \neq 0_K$ holds $f(a) \in \mathbb{Z}$,

(iii) for all elements a, b of K holds $f(a \cdot b) = f(a) + f(b)$,

(iv) for every element a of K such that $0 \leq f(a)$ holds $0 \leq f(1_K + a)$, and

(v) there exists an element a of K such that $f(a) \neq 0$ and $f(a) \neq +\infty$.

Let K be a double loop structure. Let us assume that K has a valuation. An extended integer valued function from K into $\overline{\mathbb{R}}$ is said to be a valuation of K if it satisfies the conditions (Def. 8).

(Def. 8)(i) $\mathrm{It}(0_K) = +\infty$,

(ii) for every element a of K such that $a \neq 0_K$ holds $\mathrm{it}(a) \in \mathbb{Z}$,

(iii) for all elements a, b of K holds $\mathrm{it}(a \cdot b) = \mathrm{it}(a) + \mathrm{it}(b)$,

(iv) for every element a of K such that $0 \leq \mathrm{it}(a)$ holds $0 \leq \mathrm{it}(1_K + a)$, and

(v) there exists an element a of K such that $\mathrm{it}(a) \neq 0$ and $\mathrm{it}(a) \neq +\infty$.

In the sequel v denotes a valuation of K.

One can prove the following propositions:

(17) If K has a valuation, then $v(1_K) = 0$.

(18) If K has a valuation and $a \neq 0_K$, then $v(a) \neq +\infty$.

(19) If K has a valuation, then $v(-1_K) = 0$.

(20) If K has a valuation, then $v(-a) = v(a)$.

(21) If K has a valuation and $a \neq 0_K$, then $v(a^{-1}) = -v(a)$.

(22) If K has a valuation and $b \neq 0_K$, then $v(\frac{a}{b}) = v(a) - v(b)$.

(23) If K has a valuation and $a \neq 0_K$ and $b \neq 0_K$, then $v(\frac{a}{b}) = -v(\frac{b}{a})$.

(24) If K has a valuation and $b \neq 0_K$ and $0 \leq v(\frac{a}{b})$, then $v(b) \leq v(a)$.

(25) If K has a valuation and $a \neq 0_K$ and $b \neq 0_K$ and $v(\frac{a}{b}) \leq 0$, then $0 \leq v(\frac{b}{a})$.

(26) If K has a valuation and $b \neq 0_K$ and $v(\frac{a}{b}) \leq 0$, then $v(a) \leq v(b)$.

(27) If K has a valuation, then $\min(v(a), v(b)) \leq v(a + b)$.

(28) If K has a valuation and $v(a) < v(b)$, then $v(a) = v(a + b)$.

(29) If K has a valuation and $a \neq 0_K$, then $v(a^i) = i \cdot v(a)$.

(30) If K has a valuation and $0 \leq v(1_K + a)$, then $0 \leq v(a)$.

(31) If K has a valuation and $0 \leq v(1_K - a)$, then $0 \leq v(a)$.

(32) If K has a valuation and $a \neq 0_K$ and $v(a) \leq v(b)$, then $0 \leq v(\frac{b}{a})$.

(33) If K has a valuation, then $+\infty \in \operatorname{rng} v$.

(34) If $v(a) = 1$, then least-positive $\operatorname{rng} v = 1$.

(35) If K has a valuation, then least-positive $\operatorname{rng} v$ is integer.

(36) If K has a valuation, then for every element x of K such that $x \neq 0_K$ there exists an integer i such that $v(x) = i \cdot$ least-positive $\operatorname{rng} v$.

Let us consider K, v. Let us assume that K has a valuation. The functor Pgenerator v yielding an element of K is defined as follows:

(Def. 9) Pgenerator v = the element of $v^{-1}(\{\text{least-positive } \operatorname{rng} v\})$.

Let us consider K, v. Let us assume that K has a valuation. The functor normal-valuation v yields a valuation of K and is defined by:

(Def. 10) $v(a) = (\text{normal-valuation } v)(a) \cdot$ least-positive $\operatorname{rng} v$.

We now state a number of propositions:

(37) If K has a valuation, then $v(a) = 0$ iff (normal-valuation v)$(a) = 0$.

(38) If K has a valuation, then $v(a) = +\infty$ iff (normal-valuation v)$(a) = +\infty$.

(39) If K has a valuation, then $v(a) = v(b)$ iff (normal-valuation v)$(a) =$ (normal-valuation v)(b).

(40) If K has a valuation, then $v(a)$ is positive iff (normal-valuation v)(a) is positive.

(41) If K has a valuation, then $0 \leq v(a)$ iff $0 \leq$ (normal-valuation v)(a).

(42) If K has a valuation, then $v(a)$ is non negative iff (normal-valuation v)(a) is non negative.

(43) If K has a valuation, then (normal-valuation v)(Pgenerator v) $= 1$.

(44) If K has a valuation and $0 \leq v(a)$, then (normal-valuation v)$(a) \leq v(a)$.

(45) If K has a valuation and $v(a) = 1$, then normal-valuation $v = v$.

(46) If K has a valuation, then normal-valuation(normal-valuation v) $=$ normal-valuation v.

4. Valuation Ring

Let K be a non empty double loop structure and let v be a valuation of K. The functor NonNegElements v is defined as follows:

(Def. 11) NonNegElements $v = \{x \in K\colon 0 \leq v(x)\}$.

The following four propositions are true:

(47) Let K be a non empty double loop structure, v be a valuation of K, and a be an element of K. Then $a \in$ NonNegElements v if and only if $0 \leq v(a)$.

(48) For every non empty double loop structure K and for every valuation v of K holds NonNegElements $v \subseteq$ the carrier of K.

(49) For every non empty double loop structure K and for every valuation v of K such that K has a valuation holds $0_K \in$ NonNegElements v.

(50) If K has a valuation, then $1_K \in$ NonNegElements v.

Let us consider K, v. Let us assume that K has a valuation. The functor ValuatRing v yields a strict commutative non degenerated ring and is defined by the conditions (Def. 12).

(Def. 12)(i) The carrier of ValuatRing $v =$ NonNegElements v,

(ii) the addition of ValuatRing $v =$ (the addition of K)$\restriction$(NonNegElements $v \times$ NonNegElements v),

(iii) the multiplication of ValuatRing $v =$ (the multiplication of K)$\restriction$(NonNegElements $v \times$ NonNegElements v),

(iv) the zero of ValuatRing $v = 0_K$, and

(v) the one of ValuatRing $v = 1_K$.

The following propositions are true:

(51) If K has a valuation, then every element of $\mathrm{ValuatRing}\, v$ is an element of K.

(52) If K has a valuation, then $0 \leq v(a)$ iff a is an element of $\mathrm{ValuatRing}\, v$.

(53) If K has a valuation, then for every subset S of $\mathrm{ValuatRing}\, v$ holds 0 is a lower bound of $v^{\circ}S$.

(54) Suppose K has a valuation. Let x, y be elements of K and x_1, y_1 be elements of $\mathrm{ValuatRing}\, v$. If $x = x_1$ and $y = y_1$, then $x + y = x_1 + y_1$.

(55) Suppose K has a valuation. Let x, y be elements of K and x_1, y_1 be elements of $\mathrm{ValuatRing}\, v$. If $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.

(56) If K has a valuation, then $0_{\mathrm{ValuatRing}\, v} = 0_K$.

(57) If K has a valuation, then $1_{\mathrm{ValuatRing}\, v} = 1_K$.

(58) If K has a valuation, then for every element x of K and for every element y of $\mathrm{ValuatRing}\, v$ such that $x = y$ holds $-x = -y$.

(59) If K has a valuation, then $\mathrm{ValuatRing}\, v$ is integral domain-like.

(60) If K has a valuation, then for every element y of $\mathrm{ValuatRing}\, v$ holds $\mathrm{power}_K(y, n) = \mathrm{power}_{\mathrm{ValuatRing}\, v}(y, n)$.

Let us consider K, v. Let us assume that K has a valuation. The functor $\mathrm{PosElements}\, v$ yields an ideal of $\mathrm{ValuatRing}\, v$ and is defined as follows:

(Def. 13) $\mathrm{PosElements}\, v = \{x \in K\colon 0 < v(x)\}$.

Let us consider K, v. We introduce $\mathrm{vp}\, v$ as a synonym of $\mathrm{PosElements}\, v$.

Next we state three propositions:

(61) If K has a valuation, then $a \in \mathrm{vp}\, v$ iff $0 < v(a)$.

(62) If K has a valuation, then $0_K \in \mathrm{vp}\, v$.

(63) If K has a valuation, then $1_K \notin \mathrm{vp}\, v$.

Let us consider K, v and let S be a non empty subset of K. Let us assume that K has a valuation and S is a subset of $\mathrm{ValuatRing}\, v$. The functor $\min(S, v)$ yielding a subset of $\mathrm{ValuatRing}\, v$ is defined as follows:

(Def. 14) $\min(S, v) = v^{-1}(\{\inf(v^{\circ}S)\}) \cap S$.

The following four propositions are true:

(64) For every non empty subset S of K such that K has a valuation and S is a subset of $\mathrm{ValuatRing}\, v$ holds $\min(S, v) \subseteq S$.

(65) Let S be a non empty subset of K. Suppose K has a valuation and S is a subset of $\mathrm{ValuatRing}\, v$. Let x be an element of K. Then $x \in \min(S, v)$ if and only if the following conditions are satisfied:

(i) $x \in S$, and

(ii) for every element y of K such that $y \in S$ holds $v(x) \leq v(y)$.

(66) Suppose K has a valuation. Let I be a non empty subset of K and x be an element of ValuatRing v. If I is an ideal of ValuatRing v and $x \in \min(I, v)$, then $I = \{x\}$–ideal.

(67) For every non empty double loop structure R holds every add closed non empty subset of R is a set closed w.r.t. the addition of R.

Let R be a ring and let P be a right ideal of R. A submodule of RightMod(R) is called a submodule of P if:

(Def. 15) The carrier of it $= P$.

Let R be a ring and let P be a right ideal of R. Note that there exists a submodule of P which is strict. Next we state the proposition

(68) Let R be a ring, P be an ideal of R, M be a submodule of P, a be a binary operation on P, z be an element of P, and m be a function from $P \times$ the carrier of R into P. Suppose $a =$ (the addition of R)$\restriction(P \times P)$ and $m =$ (the multiplication of R)$\restriction(P \times$ the carrier of $R)$ and $z =$ the zero of R. Then the right module structure of $M = \langle P, a, z, m\rangle$.

Let R be a ring, let M_1, M_2 be right modules over R, and let h be a function from M_1 into M_2. We say that h is scalar linear if and only if:

(Def. 16) For every element x of M_1 and for every element r of R holds $h(x \cdot r) = h(x) \cdot r$.

Let R be a ring, let M_1 be a right module over R, and let M_2 be a submodule of M_1. Observe that incl(M_2, M_1) is additive and scalar linear.

Next we state a number of propositions:

(69) If K has a valuation and b is an element of ValuatRing v, then $v(a) \leq v(a) + v(b)$.

(70) If K has a valuation and a is an element of ValuatRing v, then power$_K(a, n)$ is an element of ValuatRing v.

(71) If K has a valuation, then for every element x of ValuatRing v such that $x \neq 0_K$ holds power$_K(x, n) \neq 0_K$.

(72) If K has a valuation and $v(a) = 0$, then a is an element of ValuatRing v and a^{-1} is an element of ValuatRing v.

(73) If K has a valuation and $a \neq 0_K$ and a is an element of ValuatRing v and a^{-1} is an element of ValuatRing v, then $v(a) = 0$.

(74) If K has a valuation and $v(a) = 0$, then for every ideal I of ValuatRing v holds $a \in I$ iff $I =$ the carrier of ValuatRing v.

(75) If K has a valuation, then Pgenerator v is an element of ValuatRing v.

(76) If K has a valuation, then vp v is proper.

(77) If K has a valuation, then for every element x of ValuatRing v such that $x \notin$ vp v holds $v(x) = 0$.

(78) If K has a valuation, then vp v is prime.

(79) If K has a valuation, then for every proper ideal I of ValuatRing v holds $I \subseteq \operatorname{vp} v$.

(80) If K has a valuation, then $\operatorname{vp} v$ is maximal.

(81) If K has a valuation, then for every maximal ideal I of ValuatRing v holds $I = \operatorname{vp} v$.

(82) If K has a valuation, then NonNegElements normal-valuation v = NonNegElements v.

(83) If K has a valuation, then ValuatRing normal-valuation v = ValuatRing v.

References

[1] Emil Artin. *Algebraic Numbers and Algebraic Functions*. Gordon and Breach Science Publishers, 1994.

[2] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Formalized Mathematics*, 9(**3**):565–582, 2001.

[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] Józef Białas. Properties of fields. *Formalized Mathematics*, 1(**5**):807–812, 1990.

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

[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] Artur Korniłowicz. Quotient rings. *Formalized Mathematics*, 13(**4**):573–576, 2005.

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

[14] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.

[15] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

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

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

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

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

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

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

Received April 7, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 15–22, 2012
DOI: 10.2478/v10037-012-0003-3

VERSITA
versita.com/fm/

Functional Space $C(\Omega)$, $C_0(\Omega)$

Katuhiko Kanazashi
Shizuoka City
Japan

Hiroyuki Okazaki[1]
Shinshu University
Nagano, Japan

Yasunari Shidama[2]
Shinshu University
Nagano, Japan

Summary. In this article, first we give a definition of a functional space which is constructed from all complex-valued continuous functions defined on a compact topological space. We prove that this functional space is a Banach algebra. Next, we give a definition of a function space which is constructed from all complex-valued continuous functions with bounded support. We also prove that this function space is a complex normed space.

MML identifier: CC0SP2, version: 7.12.01 4.167.1133

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

Let X be a topological structure and let f be a function from the carrier of X into $\mathbb{C}$. We say that f is continuous if and only if:

(Def. 1) For every subset Y of $\mathbb{C}$ such that Y is closed holds $f^{-1}(Y)$ is closed.

Let X be a 1-sorted structure and let y be a complex number. The functor $X \longmapsto y$ yielding a function from the carrier of X into $\mathbb{C}$ is defined by:

(Def. 2) $X \longmapsto y =$ (the carrier of X) $\longmapsto y$.

One can prove the following proposition

(1) Let X be a non empty topological space, y be a complex number, and f be a function from the carrier of X into $\mathbb{C}$. If $f = X \longmapsto y$, then f is continuous.

Let X be a non empty topological space and let y be a complex number. Observe that $X \longmapsto y$ is continuous.

[1]The work of this author was supported by JSPS KAKENHI 22300285.
[2]The work of this author was supported by JSPS KAKENHI 22300285.

ISSN 1426–2630(p), 1898-9934(e)

Let X be a non empty topological space. One can verify that there exists a function from the carrier of X into $\mathbb{C}$ which is continuous.

The following propositions are true:

(2) Let X be a non empty topological space and f be a function from the carrier of X into $\mathbb{C}$. Then f is continuous if and only if for every subset Y of $\mathbb{C}$ such that Y is open holds $f^{-1}(Y)$ is open.

(3) Let X be a non empty topological space and f be a function from the carrier of X into $\mathbb{C}$. Then f is continuous if and only if for every point x of X and for every subset V of $\mathbb{C}$ such that $f(x) \in V$ and V is open there exists a subset W of X such that $x \in W$ and W is open and $f^{\circ}W \subseteq V$.

(4) Let X be a non empty topological space and f, g be continuous functions from the carrier of X into $\mathbb{C}$. Then $f + g$ is a continuous function from the carrier of X into $\mathbb{C}$.

(5) Let X be a non empty topological space, a be a complex number, and f be a continuous function from the carrier of X into $\mathbb{C}$. Then $a \cdot f$ is a continuous function from the carrier of X into $\mathbb{C}$.

(6) Let X be a non empty topological space and f, g be continuous functions from the carrier of X into $\mathbb{C}$. Then $f - g$ is a continuous function from the carrier of X into $\mathbb{C}$.

(7) Let X be a non empty topological space and f, g be continuous functions from the carrier of X into $\mathbb{C}$. Then $f \cdot g$ is a continuous function from the carrier of X into $\mathbb{C}$.

(8) Let X be a non empty topological space and f be a continuous function from the carrier of X into $\mathbb{C}$. Then $|f|$ is a function from the carrier of X into $\mathbb{R}$ and $|f|$ is continuous.

Let X be a non empty topological space. The $\mathbb{C}$-continuous functions of X yields a subset of $\mathbb{C}$-Algebra(the carrier of X) and is defined by:

(Def. 3) The $\mathbb{C}$-continuous functions of $X = \{f : f$ ranges over continuous functions from the carrier of X into $\mathbb{C}\}$.

Let X be a non empty topological space. Observe that the $\mathbb{C}$-continuous functions of X is non empty.

Let X be a non empty topological space. Observe that the $\mathbb{C}$-continuous functions of X is $\mathbb{C}$-additively linearly closed and multiplicatively closed.

Let X be a non empty topological space. The $\mathbb{C}$-algebra of continuous functions of X yielding a complex algebra is defined by the condition (Def. 4).

(Def. 4) The $\mathbb{C}$-algebra of continuous functions of $X = \langle$the $\mathbb{C}$-continuous functions of X, mult(the $\mathbb{C}$-continuous functions of X, $\mathbb{C}$-Algebra(the carrier of X)), Add(the $\mathbb{C}$-continuous functions of X, $\mathbb{C}$-Algebra(the carrier of X)), Mult(the $\mathbb{C}$-continuous functions of X, $\mathbb{C}$-Algebra(the carrier of X)), One(the $\mathbb{C}$-continuous functions of X, $\mathbb{C}$-Algebra(the carrier of

$X)), \mathrm{Zero}(\text{the } \mathbb{C}\text{-continuous functions of } X, \mathbb{C}\text{-Algebra}(\text{the carrier of } X))\rangle$.

Next we state the proposition

(9) Let X be a non empty topological space. Then the $\mathbb{C}$-algebra of continuous functions of X is a complex subalgebra of $\mathbb{C}$-Algebra(the carrier of X).

Let X be a non empty topological space. Observe that the $\mathbb{C}$-algebra of continuous functions of X is strict and non empty.

Let X be a non empty topological space. One can check that the $\mathbb{C}$-algebra of continuous functions of X is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, commutative, associative, right unital, right distributive, vector distributive, scalar distributive, scalar associative, and vector associative.

Next we state several propositions:

(10) Let X be a non empty topological space, F, G, H be vectors of the $\mathbb{C}$-algebra of continuous functions of X, and f, g, h be functions from the carrier of X into $\mathbb{C}$. Suppose $f = F$ and $g = G$ and $h = H$. Then $H = F + G$ if and only if for every element x of the carrier of X holds $h(x) = f(x) + g(x)$.

(11) Let X be a non empty topological space, F, G be vectors of the $\mathbb{C}$-algebra of continuous functions of X, f, g be functions from the carrier of X into $\mathbb{C}$, and a be a complex number. Suppose $f = F$ and $g = G$. Then $G = a \cdot F$ if and only if for every element x of X holds $g(x) = a \cdot f(x)$.

(12) Let X be a non empty topological space, F, G, H be vectors of the $\mathbb{C}$-algebra of continuous functions of X, and f, g, h be functions from the carrier of X into $\mathbb{C}$. Suppose $f = F$ and $g = G$ and $h = H$. Then $H = F \cdot G$ if and only if for every element x of the carrier of X holds $h(x) = f(x) \cdot g(x)$.

(13) For every non empty topological space X holds $0_{\text{the } \mathbb{C}\text{-algebra of continuous functions of } X} = X \longmapsto 0_{\mathbb{C}}$.

(14) For every non empty topological space X holds $\mathbf{1}_{\text{the } \mathbb{C}\text{-algebra of continuous functions of } X} = X \longmapsto 1_{\mathbb{C}}$.

(15) Let A be a complex algebra and A_1, A_2 be complex subalgebras of A. Suppose the carrier of $A_1 \subseteq$ the carrier of A_2. Then A_1 is a complex subalgebra of A_2.

(16) Let X be a non empty compact topological space. Then the $\mathbb{C}$-algebra of continuous functions of X is a complex subalgebra of the $\mathbb{C}$-algebra of bounded functions of the carrier of X.

Let X be a non empty compact topological space. The $\mathbb{C}$-continuous functions norm of X yields a function from the $\mathbb{C}$-continuous functions of X into $\mathbb{R}$ and is defined by:

(Def. 5) The $\mathbb{C}$-continuous functions norm of $X = (\mathbb{C}\text{-BoundedFunctionsNorm}(\text{the carrier of } X))\restriction$the $\mathbb{C}$-continuous functions of X.

Let X be a non empty compact topological space. The $\mathbb{C}$-normed algebra of continuous functions of X yields a normed complex algebra structure and is defined by the condition (Def. 6).

(Def. 6) The $\mathbb{C}$-normed algebra of continuous functions of $X = \langle$the $\mathbb{C}$-continuous functions of X, mult(the $\mathbb{C}$-continuous functions of X, $\mathbb{C}$-Algebra(the carrier of X)), Add(the $\mathbb{C}$-continuous functions of X, $\mathbb{C}$-Algebra(the carrier of X)), Mult(the $\mathbb{C}$-continuous functions of X, $\mathbb{C}$-Algebra(the carrier of X)), One(the $\mathbb{C}$-continuous functions of X, $\mathbb{C}$-Algebra(the carrier of X)), Zero(the $\mathbb{C}$-continuous functions of X, $\mathbb{C}$-Algebra(the carrier of X)), the $\mathbb{C}$-continuous functions norm of $X\rangle$.

Let X be a non empty compact topological space. Note that the $\mathbb{C}$-normed algebra of continuous functions of X is non empty and strict.

Let X be a non empty compact topological space. Observe that the $\mathbb{C}$-normed algebra of continuous functions of X is unital.

Next we state the proposition

(17) Let X be a non empty compact topological space. Then the $\mathbb{C}$-normed algebra of continuous functions of X is a complex algebra.

Let X be a non empty compact topological space. One can check that the $\mathbb{C}$-normed algebra of continuous functions of X is right complementable, Abelian, add-associative, right zeroed, vector distributive, scalar distributive, scalar associative, associative, commutative, right distributive, right unital, and vector associative.

One can prove the following proposition

(18) Let X be a non empty compact topological space and F be a point of the $\mathbb{C}$-normed algebra of continuous functions of X. Then (Mult(the $\mathbb{C}$-continuous functions of X, $\mathbb{C}$-Algebra(the carrier of X)))$(1_{\mathbb{C}}, F) = F$.

Let X be a non empty compact topological space. Observe that the $\mathbb{C}$-normed algebra of continuous functions of X is vector distributive, scalar distributive, scalar associative, and scalar unital.

We now state a number of propositions:

(19) Let X be a non empty compact topological space. Then the $\mathbb{C}$-normed algebra of continuous functions of X is a complex linear space.

(20) Let X be a non empty compact topological space. Then $X \longmapsto 0 = 0_{\text{the } \mathbb{C}\text{-normed algebra of continuous functions of } X}$.

(21) Let X be a non empty compact topological space and F be a point of the $\mathbb{C}$-normed algebra of continuous functions of X. Then $0 \leq \|F\|$.

(22) Let X be a non empty compact topological space, f, g, h be functions from the carrier of X into $\mathbb{C}$, and F, G, H be points of the $\mathbb{C}$-normed

algebra of continuous functions of X. Suppose $f = F$ and $g = G$ and $h = H$. Then $H = F + G$ if and only if for every element x of X holds $h(x) = f(x) + g(x)$.

(23) Let a be a complex number, X be a non empty compact topological space, f, g be functions from the carrier of X into $\mathbb{C}$, and F, G be points of the $\mathbb{C}$-normed algebra of continuous functions of X. Suppose $f = F$ and $g = G$. Then $G = a \cdot F$ if and only if for every element x of X holds $g(x) = a \cdot f(x)$.

(24) Let X be a non empty compact topological space, f, g, h be functions from the carrier of X into $\mathbb{C}$, and F, G, H be points of the $\mathbb{C}$-normed algebra of continuous functions of X. Suppose $f = F$ and $g = G$ and $h = H$. Then $H = F \cdot G$ if and only if for every element x of X holds $h(x) = f(x) \cdot g(x)$.

(25) Let X be a non empty compact topological space.
Then $\|0_{\text{the } \mathbb{C}\text{-normed algebra of continuous functions of } X}\| = 0$.

(26) Let X be a non empty compact topological space and F be a point of the $\mathbb{C}$-normed algebra of continuous functions of X. Suppose $\|F\| = 0$. Then $F = 0_{\text{the } \mathbb{C}\text{-normed algebra of continuous functions of } X}$.

(27) Let a be a complex number, X be a non empty compact topological space, and F be a point of the $\mathbb{C}$-normed algebra of continuous functions of X. Then $\|a \cdot F\| = |a| \cdot \|F\|$.

(28) Let X be a non empty compact topological space and F, G be points of the $\mathbb{C}$-normed algebra of continuous functions of X. Then $\|F + G\| \leq \|F\| + \|G\|$.

Let X be a non empty compact topological space. Observe that the $\mathbb{C}$-normed algebra of continuous functions of X is discernible, reflexive, and complex normed space-like.

The following propositions are true:

(29) Let X be a non empty compact topological space, f, g, h be functions from the carrier of X into $\mathbb{C}$, and F, G, H be points of the $\mathbb{C}$-normed algebra of continuous functions of X. Suppose $f = F$ and $g = G$ and $h = H$. Then $H = F - G$ if and only if for every element x of X holds $h(x) = f(x) - g(x)$.

(30) Let X be a complex Banach space, Y be a subset of X, and s_1 be a sequence of X. Suppose Y is closed and $\operatorname{rng} s_1 \subseteq Y$ and s_1 is $\mathbb{C}$-Cauchy. Then s_1 is convergent and $\lim s_1 \in Y$.

(31) Let X be a non empty compact topological space and Y be a subset of the $\mathbb{C}$-normed algebra of bounded functions of the carrier of X. If $Y =$ the $\mathbb{C}$-continuous functions of X, then Y is closed.

(32) Let X be a non empty compact topological space and s_1 be a sequence

of the $\mathbb{C}$-normed algebra of continuous functions of X. If s_1 is $\mathbb{C}$-Cauchy, then s_1 is convergent.

Let X be a non empty compact topological space. One can verify that the $\mathbb{C}$-normed algebra of continuous functions of X is complete.

Let X be a non empty compact topological space. Observe that the $\mathbb{C}$-normed algebra of continuous functions of X is Banach Algebra-like.

Next we state three propositions:

(33) For every non empty topological space X and for all functions f, g from the carrier of X into $\mathbb{C}$ holds $\operatorname{support}(f+g) \subseteq \operatorname{support} f \cup \operatorname{support} g$.

(34) Let X be a non empty topological space, a be a complex number, and f be a function from the carrier of X into $\mathbb{C}$. Then $\operatorname{support}(a \cdot f) \subseteq \operatorname{support} f$.

(35) For every non empty topological space X and for all functions f, g from the carrier of X into $\mathbb{C}$ holds $\operatorname{support}(f \cdot g) \subseteq \operatorname{support} f \cup \operatorname{support} g$.

Let X be a non empty topological space. The $\boldsymbol{CC_0}$-functions of X yielding a non empty subset of the $\mathbb{C}$-vector space of the carrier of X is defined by the condition (Def. 7).

(Def. 7) The $\boldsymbol{CC_0}$-functions of $X = \{f; f \text{ ranges over functions from the carrier of } X \text{ into } \mathbb{C}: f \text{ is continuous} \wedge \bigvee_{Y:\ \text{non empty subset of } X} (Y \text{ is compact} \wedge \bigwedge_{A:\ \text{subset of } X} (A = \operatorname{support} f \Rightarrow \overline{A} \text{ is a subset of } Y))\}$.

The following propositions are true:

(36) Let X be a non empty topological space. Then the $\boldsymbol{CC_0}$-functions of X is a non empty subset of $\mathbb{C}$-Algebra(the carrier of X).

(37) Let X be a non empty topological space and W be a non empty subset of $\mathbb{C}$-Algebra(the carrier of X). Suppose $W =$ the $\boldsymbol{CC_0}$-functions of X. Then W is $\mathbb{C}$-additively linearly closed.

(38) For every non empty topological space X holds the $\boldsymbol{CC_0}$-functions of X is add closed.

(39) For every non empty topological space X holds the $\boldsymbol{CC_0}$-functions of X is linearly closed.

Let X be a non empty topological space. Observe that the $\boldsymbol{CC_0}$-functions of X is non empty and linearly closed.

The following propositions are true:

(40) Let V be a complex linear space and V_1 be a subset of V. Suppose V_1 is linearly closed and V_1 is not empty. Then $\langle V_1, \operatorname{Zero}(V_1, V), \operatorname{Add}(V_1, V), \operatorname{Mult}(V_1, V)\rangle$ is a subspace of V.

(41) Let X be a non empty topological space. Then $\langle$the $\boldsymbol{CC_0}$-functions of X, Zero(the $\boldsymbol{CC_0}$-functions of X, the $\mathbb{C}$-vector space of the carrier of X), Add(the $\boldsymbol{CC_0}$-functions of X, the $\mathbb{C}$-vector space of the carrier of X), Mult(the $\boldsymbol{CC_0}$-functions of X, the $\mathbb{C}$-vector space of the carrier of X)$\rangle$ is a subspace of the $\mathbb{C}$-vector space of the carrier of X.

Let X be a non empty topological space. The $\mathbb{C}$-vector space of $\boldsymbol{C_0}$-functions of X yielding a complex linear space is defined by the condition (Def. 8).

(Def. 8) The $\mathbb{C}$-vector space of $\boldsymbol{C_0}$-functions of X = $\langle$the $\boldsymbol{CC_0}$-functions of X, Zero(the $\boldsymbol{CC_0}$-functions of X, the $\mathbb{C}$-vector space of the carrier of X), Add(the $\boldsymbol{CC_0}$-functions of X, the $\mathbb{C}$-vector space of the carrier of X), Mult(the $\boldsymbol{CC_0}$-functions of X, the $\mathbb{C}$-vector space of the carrier of X)$\rangle$.

Next we state the proposition

(42) Let X be a non empty topological space and x be a set. If $x \in$ the $\boldsymbol{CC_0}$-functions of X, then $x \in \mathbb{C}$-BoundedFunctions (the carrier of X).

Let X be a non empty topological space. The $\boldsymbol{CC_0}$-functions norm of X yielding a function from the $\boldsymbol{CC_0}$-functions of X into $\mathbb{R}$ is defined by:

(Def. 9) The $\boldsymbol{CC_0}$-functions norm of X = ($\mathbb{C}$-BoundedFunctionsNorm (the carrier of X))$\restriction$the $\boldsymbol{CC_0}$-functions of X.

Let X be a non empty topological space. The $\mathbb{C}$-normed space of $\boldsymbol{C_0}$-functions of X yielding a complex normed space structure is defined by the condition (Def. 10).

(Def. 10) The $\mathbb{C}$-normed space of $\boldsymbol{C_0}$-functions of X = $\langle$the $\boldsymbol{CC_0}$-functions of X, Zero(the $\boldsymbol{CC_0}$-functions of X, the $\mathbb{C}$-vector space of the carrier of X), Add(the $\boldsymbol{CC_0}$-functions of X, the $\mathbb{C}$-vector space of the carrier of X), Mult(the $\boldsymbol{CC_0}$-functions of X, the $\mathbb{C}$-vector space of the carrier of X), the $\boldsymbol{CC_0}$-functions norm of $X\rangle$.

Let X be a non empty topological space. One can check that the $\mathbb{C}$-normed space of $\boldsymbol{C_0}$-functions of X is strict and non empty.

One can prove the following propositions:

(43) Let X be a non empty topological space and x be a set. Suppose $x \in$ the $\boldsymbol{CC_0}$-functions of X. Then $x \in$ the $\mathbb{C}$-continuous functions of X.

(44) For every non empty topological space X holds $0_{\text{the } \mathbb{C}\text{-vector space of } \boldsymbol{C_0}\text{-functions of } X} = X \longmapsto 0$.

(45) For every non empty topological space X holds $0_{\text{the } \mathbb{C}\text{-normed space of } \boldsymbol{C_0}\text{-functions of } X} = X \longmapsto 0$.

(46) Let a be a complex number, X be a non empty topological space, and F, G be points of the $\mathbb{C}$-normed space of $\boldsymbol{C_0}$-functions of X. Then $\|F\| = 0$ iff $F = 0_{\text{the } \mathbb{C}\text{-normed space of } \boldsymbol{C_0}\text{-functions of } X}$ and $\|a \cdot F\| = |a| \cdot \|F\|$ and $\|F + G\| \leq \|F\| + \|G\|$.

Let X be a non empty topological space. Note that the $\mathbb{C}$-normed space of $\boldsymbol{C_0}$-functions of X is reflexive, discernible, complex normed space-like, vector distributive, scalar distributive, scalar associative, scalar unital, Abelian, add-associative, right zeroed, and right complementable.

The following proposition is true

(47) Let X be a non empty topological space. Then the $\mathbb{C}$-normed space of $\boldsymbol{C_0}$-functions of X is a complex normed space.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[2] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[3] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.
[4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[5] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[7] Agata Darmochwał. Compact spaces. *Formalized Mathematics*, 1(**2**):383–386, 1990.
[8] Noboru Endou. Banach algebra of bounded complex linear operators. *Formalized Mathematics*, 12(**3**):237–242, 2004.
[9] Noboru Endou. Banach space of absolute summable complex sequences. *Formalized Mathematics*, 12(**2**):191–194, 2004.
[10] Noboru Endou. Complex Banach space of bounded linear operators. *Formalized Mathematics*, 12(**2**):201–209, 2004.
[11] Noboru Endou. Complex linear space and complex normed space. *Formalized Mathematics*, 12(**2**):93–102, 2004.
[12] Noboru Endou. Complex linear space of complex sequences. *Formalized Mathematics*, 12(**2**):109–117, 2004.
[13] Noboru Endou. Complex valued functions space. *Formalized Mathematics*, 12(**3**):231–235, 2004.
[14] Noboru Endou. Continuous functions on real and complex normed linear spaces. *Formalized Mathematics*, 12(**3**):403–419, 2004.
[15] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[16] Katuhiko Kanazashi, Hiroyuki Okazaki, and Yasunari Shidama. Banach algebra of bounded complex-valued functionals. *Formalized Mathematics*, 19(**2**):121–126, 2011, doi: 10.2478/v10037-011-0019-0.
[17] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[18] Chanapat Pacharapokin, Hiroshi Yamazaki, Yasunari Shidama, and Yatsuka Nakamura. Complex function differentiability. *Formalized Mathematics*, 17(**2**):67–72, 2009, doi: 10.2478/v10037-009-0007-9.
[19] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[20] Yasunari Shidama, Hikofumi Suzuki, and Noboru Endou. Banach algebra of bounded functionals. *Formalized Mathematics*, 16(**2**):115–122, 2008, doi:10.2478/v10037-008-0017-z.
[21] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[22] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[23] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 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 30, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 23–29, 2012
DOI: 10.2478/v10037-012-0004-2

VERSITA
versita.com/fm/

The Rotation Group

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Summary. We introduce length-preserving linear transformations of Euclidean topological spaces. We also introduce rotation which preserves orientation (proper rotation) and reverses orientation (improper rotation). We show that every rotation that preserves orientation can be represented as a composition of base proper rotations. And finally, we show that every rotation that reverses orientation can be represented as a composition of proper rotations and one improper rotation.

MML identifier: `MATRTOP3`, version: `7.12.01 4.167.1133`

The papers [11], [35], [36], [8], [10], [9], [3], [7], [14], [2], [30], [4], [19], [12], [31], [24], [34], [13], [22], [17], [1], [20], [15], [16], [40], [38], [33], [25], [28], [37], [23], [6], [39], [18], [21], [32], [5], [26], [29], and [27] provide the terminology and notation for this paper.

1. Preliminaries

We adopt the following rules: x, X are sets, α, α_1, α_2, r, s are real numbers, and i, j, k, m, n are natural numbers.

We now state three propositions:

(1) Let K be a field, M be a square matrix over K of dimension n, and P be a permutation of $\operatorname{Seg} n$. Then $\operatorname{Det}(((M \cdot P)^{\mathrm{T}} \cdot P)^{\mathrm{T}}) = \operatorname{Det} M$ and for all i, j such that $\langle i, j \rangle \in$ the indices of M holds $((M \cdot P)^{\mathrm{T}} \cdot P)^{\mathrm{T}}_{i,j} = M_{P(i),P(j)}$.

(2) For every field K and for every diagonal square matrix M over K of dimension n holds $M^{\mathrm{T}} = M$.

ISSN 1426–2630(p), 1898-9934(e)

(3) For every real-valued finite sequence f and for every i such that $i \in \operatorname{dom} f$ holds $\sum^2(f +\cdot (i, r)) = (\sum^2 f - f(i)^{\mathbf{2}}) + r^{\mathbf{2}}$.

Let us consider X and let F be a function yielding function. We say that F is X-support-yielding if and only if:

(Def. 1) For every function f and for every x such that $f \in \operatorname{dom} F$ and $F(f)(x) \neq f(x)$ holds $x \in X$.

Let us consider X. One can check that there exists a function yielding function which is X-support-yielding.

Let us consider X and let Y be a subset of X. One can check that every function yielding function which is Y-support-yielding is also X-support-yielding.

Let X, Y be sets. Note that every function yielding function which is X-support-yielding and Y-support-yielding is also $X \cap Y$-support-yielding. Let f be an X-support-yielding function yielding function and let g be a Y-support-yielding function yielding function. Note that $f \cdot g$ is $X \cup Y$-support-yielding.

Let us consider n. Observe that there exists a function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$ which is homogeneous.

Let us consider n, m. Observe that every function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^m_{\mathrm{T}}$ is finite sequence-yielding.

Let us consider n, m and let A be a matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension $n \times m$. One can check that $\operatorname{Mx2Tran} A$ is additive.

Let us consider n and let A be a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension n. Note that $\operatorname{Mx2Tran} A$ is homogeneous.

Let us consider n and let f, g be homogeneous functions from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$. Note that $f \cdot g$ is homogeneous.

2. Improper Rotation

In the sequel p, q are points of $\mathcal{E}^n_{\mathrm{T}}$.

Let us consider n, i. Let us assume that $i \in \operatorname{Seg} n$. The axial symmetry of i and n yields an invertible square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension n and is defined by the conditions (Def. 2).

(Def. 2)(i) (The axial symmetry of i and $n)_{i,i} = -1_{\mathbb{R}_{\mathrm{F}}}$, and

(ii) for all k, m such that $\langle k, m\rangle \in$ the indices of the axial symmetry of i and n holds if $k = m$ and $k \neq i$, then (the axial symmetry of i and $n)_{k,k} = 1_{\mathbb{R}_{\mathrm{F}}}$ and if $k \neq m$, then (the axial symmetry of i and $n)_{k,m} = 0_{\mathbb{R}_{\mathrm{F}}}$.

The following propositions are true:

(4) If $i \in \operatorname{Seg} n$, then Det (the axial symmetry of i and $n) = -1_{\mathbb{R}_{\mathrm{F}}}$.

(5) If i, $j \in \operatorname{Seg} n$ and $i \neq j$, then $({}^{@}p) \cdot$ (the axial symmetry of i and $n)_{\square,j} = p(j)$.

(6) If $i \in \operatorname{Seg} n$, then $({}^{@}p) \cdot$ (the axial symmetry of i and $n)_{\square,i} = -p(i)$.

(7) Suppose $i \in \operatorname{Seg} n$. Then

(i) the axial symmetry of i and n is diagonal, and

(ii) (the axial symmetry of i and $n)^\smile =$ the axial symmetry of i and n.

(8) If $i \in \operatorname{Seg} n$ and $i \neq j$, then (Mx2Tran (the axial symmetry of i and $n))(p)(j) = p(j)$.

(9) If $i \in \operatorname{Seg} n$, then (Mx2Tran (the axial symmetry of i and $n))(p)(i) = -p(i)$.

(10) If $i \in \operatorname{Seg} n$, then (Mx2Tran (the axial symmetry of i and $n))(p) = p +\cdot (i, -p(i))$.

(11) If $i \in \operatorname{Seg} n$, then Mx2Tran (the axial symmetry of i and $n)$ is $\{i\}$-support-yielding.

(12) For all elements a, b of $\mathbb{R}_{\mathrm{F}}$ such that $a = \cos r$ and $b = \sin r$ holds Det (the $0_{\mathbb{R}_{\mathrm{F}}}$-block diagonal of $\langle \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, I^{n\times n}_{\mathbb{R}_{\mathrm{F}}} \rangle) = 1_{\mathbb{R}_{\mathrm{F}}}$.

3. Proper Rotation

Let us consider n, α and let us consider i, j. Let us assume that $1 \leq i < j \leq n$. The functor Rotation(i, j, n, α) yielding an invertible square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension n is defined by the conditions (Def. 3).

(Def. 3)(i) $(\text{Rotation}(i, j, n, \alpha))_{i,i} = \cos\alpha$,

(ii) $(\text{Rotation}(i, j, n, \alpha))_{j,j} = \cos\alpha$,

(iii) $(\text{Rotation}(i, j, n, \alpha))_{i,j} = \sin\alpha$,

(iv) $(\text{Rotation}(i, j, n, \alpha))_{j,i} = -\sin\alpha$, and

(v) for all k, m such that $\langle k, m\rangle \in$ the indices of Rotation(i, j, n, α) holds if $k = m$ and $k \neq i$ and $k \neq j$, then $(\text{Rotation}(i, j, n, \alpha))_{k,k} = 1_{\mathbb{R}_{\mathrm{F}}}$ and if $k \neq m$ and $\{k, m\} \neq \{i, j\}$, then $(\text{Rotation}(i, j, n, \alpha))_{k,m} = 0_{\mathbb{R}_{\mathrm{F}}}$.

We now state a number of propositions:

(13) If $1 \leq i < j \leq n$, then Det Rotation$(i, j, n, \alpha) = 1_{\mathbb{R}_{\mathrm{F}}}$.

(14) If $1 \leq i < j \leq n$ and $k \in \operatorname{Seg} n$ and $k \neq i$ and $k \neq j$, then $({}^{@}p) \cdot (\text{Rotation}(i, j, n, \alpha))_{\square,k} = p(k)$.

(15) If $1 \leq i < j \leq n$, then $({}^{@}p) \cdot (\text{Rotation}(i, j, n, \alpha))_{\square,i} = p(i) \cdot \cos\alpha + p(j) \cdot -\sin\alpha$.

(16) If $1 \leq i < j \leq n$, then $({}^{@}p) \cdot (\text{Rotation}(i, j, n, \alpha))_{\square,j} = p(i) \cdot \sin\alpha + p(j) \cdot \cos\alpha$.

(17) If $1 \leq i < j \leq n$, then Rotation$(i, j, n, \alpha_1) \cdot$ Rotation$(i, j, n, \alpha_2) =$ Rotation$(i, j, n, \alpha_1 + \alpha_2)$.

(18) If $1 \leq i < j \leq n$, then Rotation$(i, j, n, 0) = I^{n\times n}_{\mathbb{R}_{\mathrm{F}}}$.

(19) If $1 \leq i < j \leq n$, then Rotation(i, j, n, α) is orthogonal and $(\text{Rotation}(i, j, n, \alpha))^\smile =$ Rotation$(i, j, n, -\alpha)$.

(20) If $1 \leq i < j \leq n$ and $k \neq i$ and $k \neq j$, then $(\text{Mx2Tran Rotation}(i, j, n, \alpha))(p)(k) = p(k)$.

(21) If $1 \leq i < j \leq n$, then $(\text{Mx2Tran Rotation}(i, j, n, \alpha))(p)(i) = p(i) \cdot \cos\alpha + p(j) \cdot -\sin\alpha$.

(22) If $1 \leq i < j \leq n$, then $(\text{Mx2Tran Rotation}(i, j, n, \alpha))(p)(j) = p(i) \cdot \sin\alpha + p(j) \cdot \cos\alpha$.

(23) If $1 \leq i < j \leq n$, then $(\text{Mx2Tran Rotation}(i, j, n, \alpha))(p) = (p\restriction(i -' 1)) \frown \langle p(i) \cdot \cos\alpha + p(j) \cdot -\sin\alpha \rangle \frown (p_{\restriction i}\restriction(j -' i -' 1)) \frown \langle p(i) \cdot \sin\alpha + p(j) \cdot \cos\alpha \rangle \frown (p_{\restriction j})$.

(24) If $1 \leq i < j \leq n$ and $s^{\mathbf{2}} \leq p(i)^{\mathbf{2}} + p(j)^{\mathbf{2}}$, then there exists α such that $(\text{Mx2Tran Rotation}(i, j, n, \alpha))(p)(i) = s$.

(25) If $1 \leq i < j \leq n$ and $s^{\mathbf{2}} \leq p(i)^{\mathbf{2}} + p(j)^{\mathbf{2}}$, then there exists α such that $(\text{Mx2Tran Rotation}(i, j, n, \alpha))(p)(j) = s$.

(26) If $1 \leq i < j \leq n$, then $\text{Mx2Tran Rotation}(i, j, n, \alpha)$ is $\{i, j\}$-support-yielding.

4. Length-Preserving Linear Transformations

Let us consider n and let f be a function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$. We say that f is rotation if and only if:

(Def. 4) $|p| = |f(p)|$.

One can prove the following proposition

(27) If $i \in \operatorname{Seg} n$, then Mx2Tran (the axial symmetry of i and n) is rotation.

Let us consider n and let f be a function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$. We say that f is base rotation if and only if the condition (Def. 5) is satisfied.

(Def. 5) There exists a finite sequence F of elements of the semigroup of functions onto the carrier of $\mathcal{E}^n_{\mathrm{T}}$ such that $f = \prod F$ and for every k such that $k \in \operatorname{dom} F$ there exist i, j, r such that $1 \leq i < j \leq n$ and $F(k) = \text{Mx2Tran Rotation}(i, j, n, r)$.

Let us consider n. One can check that $\mathrm{id}_{\mathcal{E}^n_{\mathrm{T}}}$ is base rotation.

Let us consider n. One can check that there exists a function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$ which is base rotation.

Let us consider n and let f, g be base rotation functions from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$. One can check that $f \cdot g$ is base rotation.

Next we state the proposition

(28) If $1 \leq i < j \leq n$, then $\text{Mx2Tran Rotation}(i, j, n, r)$ is base rotation.

Let us consider n. Observe that every function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$ which is base rotation is also homogeneous, additive, rotation, and homeomorphism.

Let us consider n and let f be a base rotation function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$. Note that f^{-1} is base rotation.

Let us consider n and let f, g be rotation functions from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$. One can check that $f \cdot g$ is rotation.

In the sequel f, f_1, f_2 are homogeneous additive functions from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$.

Let us consider n and let us consider f. The functor $\operatorname{AutMt} f$ yields a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension n and is defined as follows:

(Def. 6) $f = \operatorname{Mx2Tran} \operatorname{AutMt} f$.

Next we state several propositions:

(29) $\operatorname{AutMt}(f_1 \cdot f_2) = \operatorname{AutMt} f_2 \cdot \operatorname{AutMt} f_1$.

(30) Suppose $k \in X$ and $k \in \operatorname{Seg} n$. Then there exists f such that

(i) f is X-support-yielding and base rotation,

(ii) if $\overline{\overline{X \cap \operatorname{Seg} n}} > 1$, then $f(p)(k) \geq 0$, and

(iii) for every i such that $i \in X \cap \operatorname{Seg} n$ and $i \neq k$ holds $f(p)(i) = 0$.

(31) For every subset A of $\mathcal{E}^n_{\mathrm{T}}$ such that $f \restriction A = \mathrm{id}_A$ holds $f \restriction \operatorname{Lin}(A) = \mathrm{id}_{\operatorname{Lin}(A)}$.

(32) Let A be a subset of $\mathcal{E}^n_{\mathrm{T}}$. Suppose f is rotation and $f \restriction A = \mathrm{id}_A$. Let given i. Suppose $i \in \operatorname{Seg} n$ and the base finite sequence of n and $i \in \operatorname{Lin}(A)$. Then $f(p)(i) = p(i)$.

(33) Let f be a rotation function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$. Suppose f is X-support-yielding and for every i such that $i \in X \cap \operatorname{Seg} n$ holds $p(i) = 0$. Then $f(p) = p$.

(34) If $i \in \operatorname{Seg} n$ and $n \geq 2$, then there exists f such that f is base rotation and $f(p) = p +\cdot (i, -p(i))$.

(35) If f is $\{i\}$-support-yielding and rotation, then $\operatorname{AutMt} f =$ the axial symmetry of i and n or $\operatorname{AutMt} f = I^{n \times n}_{\mathbb{R}_{\mathrm{F}}}$.

(36) If f_1 is rotation, then there exists f_2 such that f_2 is base rotation and $f_2 \cdot f_1$ is $\{n\}$-support-yielding.

5. Rotation Matrix Classification

The following three propositions are true:

(37) If f is rotation, then $\operatorname{Det} \operatorname{AutMt} f = 1_{\mathbb{R}_{\mathrm{F}}}$ iff f is base rotation.

(38) If f is rotation, then $\operatorname{Det} \operatorname{AutMt} f = 1_{\mathbb{R}_{\mathrm{F}}}$ or $\operatorname{Det} \operatorname{AutMt} f = -1_{\mathbb{R}_{\mathrm{F}}}$.

(39) If f_1 is rotation and $\operatorname{Det} \operatorname{AutMt} f_1 = -1_{\mathbb{R}_{\mathrm{F}}}$ and $i \in \operatorname{Seg} n$ and $\operatorname{AutMt} f_2 =$ the axial symmetry of i and n, then $f_1 \cdot f_2$ is base rotation.

Let us consider n and let f be a rotation homogeneous additive function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$. One can check that $\operatorname{AutMt} f$ is orthogonal.

Let us consider n. One can verify that every function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathcal{E}^n_{\mathrm{T}}$ which is homogeneous, additive, and rotation is also homeomorphism.

6. The Rotation Mapping a Given Point to Another Point

One can prove the following propositions:

(40) Suppose $n = 1$ and $|p| = |q|$. Then there exists f such that f is rotation and $f(p) = q$ either $\operatorname{AutMt} f =$ the axial symmetry of n and n or $\operatorname{AutMt} f = I_{\mathbb{R}_{\mathrm{F}}}^{n \times n}$.

(41) If $n \neq 1$ and $|p| = |q|$, then there exists f such that f is base rotation and $f(p) = q$.

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] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.
[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. 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] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[13] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[14] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[15] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.
[16] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(**5**):711–717, 1991.
[17] Artur Korniłowicz and Yasunari Shidama. Intersections of intervals and balls in $\mathcal{E}_{\mathrm{T}}^{n}$. *Formalized Mathematics*, 12(**3**):301–306, 2004.
[18] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[19] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.
[20] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[21] Anna Lango and Grzegorz Bancerek. Product of families of groups and vector spaces. *Formalized Mathematics*, 3(**2**):235–240, 1992.
[22] Michał Muzalewski. Categories of groups. *Formalized Mathematics*, 2(**4**):563–571, 1991.
[23] Yatsuka Nakamura. Determinant of some matrices of field elements. *Formalized Mathematics*, 14(**1**):1–5, 2006, doi:10.2478/v10037-006-0001-4.
[24] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[25] Karol Pąk. Basic properties of determinants of square matrices over a field. *Formalized Mathematics*, 15(**1**):17–25, 2007, doi:10.2478/v10037-007-0003-x.

[26] Karol Pąk. Basic properties of the rank of matrices over a field. *Formalized Mathematics*, 15(**4**):199–211, 2007, doi:10.2478/v10037-007-0024-5.
[27] Karol Pąk. Block diagonal matrices. *Formalized Mathematics*, 16(**3**):259–267, 2008, doi:10.2478/v10037-008-0031-1.
[28] Karol Pąk. Linear transformations of Euclidean topological spaces. *Formalized Mathematics*, 19(**2**):103–108, 2011, doi: 10.2478/v10037-011-0016-3.
[29] Nobuyuki Tamura and Yatsuka Nakamura. Determinant and inverse of matrices of real elements. *Formalized Mathematics*, 15(**3**):127–136, 2007, doi:10.2478/v10037-007-0014-7.
[30] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[31] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[32] Wojciech A. Trybulec. Basis of real linear space. *Formalized Mathematics*, 1(**5**):847–850, 1990.
[33] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[34] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[35] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[36] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[37] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.
[38] Xiaopeng Yue, Xiquan Liang, and Zhongpin Sun. Some properties of some special matrices. *Formalized Mathematics*, 13(**4**):541–547, 2005.
[39] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.
[40] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Received May 30, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 31–40, 2012
DOI: 10.2478/v10037-012-0005-1

VERSITA
versita.com/fm/

Differentiable Functions on Normed Linear Spaces[1]

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize differentiability of functions on normed linear spaces. Partial derivative, mean value theorem for vector-valued functions, continuous differentiability, etc. are formalized. As it is well known, there is no exact analog of the mean value theorem for vector-valued functions. However a certain type of generalization of the mean value theorem for vector-valued functions is obtained as follows: If $||f'(x+t\cdot h)||$ is bounded for t between 0 and 1 by some constant M, then $||f(x+t\cdot h)-f(x)|| \leq M\cdot||h||$. This theorem is called the mean value theorem for vector-valued functions. By this theorem, the relation between the (total) derivative and the partial derivatives of a function is derived [23].

MML identifier: NDIFF_5, version: 7.12.01 4.167.1133

The notation and terminology used here have been introduced in the following papers: [28], [29], [9], [4], [30], [12], [10], [25], [11], [1], [2], [26], [7], [3], [5], [8], [17], [22], [20], [27], [21], [31], [14], [24], [18], [16], [15], [19], [13], and [6].

1. Preliminaries

In this paper r is a real number and S, T are non trivial real normed spaces. Next we state several propositions:

(1) Let R be a function from $\mathbb{R}$ into S. Then R is rest-like if and only if for every real number r such that $r > 0$ there exists a real number d such that $d > 0$ and for every real number z such that $z \neq 0$ and $|z| < d$ holds $|z|^{-1} \cdot \|R_z\| < r$.

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

ISSN 1426–2630(p), 1898-9934(e)

(2) Let R be a rest of S. Suppose $R_0 = 0_S$. Let e be a real number. Suppose $e > 0$. Then there exists a real number d such that $d > 0$ and for every real number h such that $|h| < d$ holds $\|R_h\| \leq e \cdot |h|$.

(3) For every rest R of S and for every bounded linear operator L from S into T holds $L \cdot R$ is a rest of T.

(4) Let R_1 be a rest of S. Suppose $(R_1)_0 = 0_S$. Let R_2 be a rest of S, T. If $(R_2)_{0_S} = 0_T$, then for every linear L of S holds $R_2 \cdot (L + R_1)$ is a rest of T.

(5) Let R_1 be a rest of S. Suppose $(R_1)_0 = 0_S$. Let R_2 be a rest of S, T. Suppose $(R_2)_{0_S} = 0_T$. Let L_1 be a linear of S and L_2 be a bounded linear operator from S into T. Then $L_2 \cdot R_1 + R_2 \cdot (L_1 + R_1)$ is a rest of T.

(6) Let x_0 be an element of $\mathbb{R}$ and g be a partial function from $\mathbb{R}$ to the carrier of S. Suppose g is differentiable in x_0. Let f be a partial function from the carrier of S to the carrier of T. Suppose f is differentiable in g_{x_0}. Then $f \cdot g$ is differentiable in x_0 and $(f \cdot g)'(x_0) = f'(g_{x_0})(g'(x_0))$.

(7) Let S be a real normed space, x_1 be a finite sequence of elements of S, and y_1 be a finite sequence of elements of $\mathbb{R}$. Suppose $\operatorname{len} x_1 = \operatorname{len} y_1$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} x_1$ holds $y_1(i) = \|(x_1)_i\|$. Then $\|\sum x_1\| \leq \sum y_1$.

(8) Let S be a real normed space, x be a point of S, and N_1, N_2 be neighbourhoods of x. Then $N_1 \cap N_2$ is a neighbourhood of x.

(9) For every non-empty finite sequence X and for every set x such that $x \in \prod X$ holds x is a finite sequence.

Let G be a real norm space sequence. One can verify that $\prod G$ is constituted finite sequences.

Let G be a real linear space sequence, let z be an element of $\prod \overline{G}$, and let j be an element of $\operatorname{dom} G$. Then $z(j)$ is an element of $G(j)$.

One can prove the following propositions:

(10) The carrier of $\prod G = \prod \overline{G}$.

(11) Let i be an element of $\operatorname{dom} G$, r be a set, and x be a function. If $r \in$ the carrier of $G(i)$ and $x \in \prod \overline{G}$, then $x +\cdot (i, r) \in$ the carrier of $\prod G$.

Let G be a real norm space sequence. We say that G is nontrivial if and only if:

(Def. 1) For every element j of $\operatorname{dom} G$ holds $G(j)$ is non trivial.

Let us mention that there exists a real norm space sequence which is nontrivial.

Let G be a nontrivial real norm space sequence and let i be an element of $\operatorname{dom} G$. Note that $G(i)$ is non trivial.

Let G be a nontrivial real norm space sequence. Note that $\prod G$ is non trivial.

The following propositions are true:

(12) Let G be a real norm space sequence, p, q be points of $\prod G$, and r_0, p_0, q_0 be elements of $\prod \overline{G}$. Suppose $p = p_0$ and $q = q_0$. Then $p + q = r_0$ if and only if for every element i of $\operatorname{dom} G$ holds $r_0(i) = p_0(i) + q_0(i)$.

(13) Let G be a real norm space sequence, p be a point of $\prod G$, r be a real number, and r_0, p_0 be elements of $\prod \overline{G}$. Suppose $p = p_0$. Then $r \cdot p = r_0$ if and only if for every element i of $\operatorname{dom} G$ holds $r_0(i) = r \cdot p_0(i)$.

(14) Let G be a real norm space sequence and p_0 be an element of $\prod \overline{G}$. Then $0_{\prod G} = p_0$ if and only if for every element i of $\operatorname{dom} G$ holds $p_0(i) = 0_{G(i)}$.

(15) Let G be a real norm space sequence, p, q be points of $\prod G$, and r_0, p_0, q_0 be elements of $\prod \overline{G}$. Suppose $p = p_0$ and $q = q_0$. Then $p - q = r_0$ if and only if for every element i of $\operatorname{dom} G$ holds $r_0(i) = p_0(i) - q_0(i)$.

2. Mean Value Theorem for Vector-Valued Functions

Let S be a real linear space and let p, q be points of S. The functor $]p, q[$ yielding a subset of S is defined as follows:

(Def. 2) $]p, q[= \{p + t \cdot (q - p); t \text{ ranges over real numbers: } 0 < t \wedge t < 1\}$.

Let S be a real linear space and let p, q be points of S. We introduce $[p, q]$ as a synonym of $\mathcal{L}(p, q)$.

Next we state several propositions:

(16) For every real linear space S and for all points p, q of S holds $]p, q[\subseteq [p, q]$.

(17) Let T be a non trivial real normed space and R be a partial function from $\mathbb{R}$ to T. Suppose R is total. Then R is rest-like if and only if for every real number r such that $r > 0$ there exists a real number d such that $d > 0$ and for every real number z such that $z \neq 0$ and $|z| < d$ holds $\frac{\|R_z\|}{|z|} < r$.

(18) Let R be a function from $\mathbb{R}$ into $\mathbb{R}$. Then R is rest-like if and only if for every real number r such that $r > 0$ there exists a real number d such that $d > 0$ and for every real number z such that $z \neq 0$ and $|z| < d$ holds $\frac{|R(z)|}{|z|} < r$.

(19) Let S, T be non trivial real normed spaces, f be a partial function from S to T, p, q be points of S, and M be a real number. Suppose that

(i) $[p, q] \subseteq \operatorname{dom} f$,

(ii) for every point x of S such that $x \in [p, q]$ holds f is continuous in x,

(iii) for every point x of S such that $x \in]p, q[$ holds f is differentiable in x, and

(iv) for every point x of S such that $x \in]p, q[$ holds $\|f'(x)\| \leq M$.

Then $\|f_q - f_p\| \leq M \cdot \|q - p\|$.

(20) Let S, T be non trivial real normed spaces, f be a partial function from S to T, p, q be points of S, M be a real number, and L be a point of the real norm space of bounded linear operators from S into T. Suppose that

(i) $[p, q] \subseteq \operatorname{dom} f$,

(ii) for every point x of S such that $x \in [p, q]$ holds f is continuous in x,

(iii) for every point x of S such that $x \in]p, q[$ holds f is differentiable in x, and

(iv) for every point x of S such that $x \in]p, q[$ holds $\|f'(x) - L\| \leq M$.

Then $\|f_q - f_p - L(q - p)\| \leq M \cdot \|q - p\|$.

3. Partial Derivative of a Function of Several Variables

Let G be a real norm space sequence and let i be an element of $\operatorname{dom} G$. The projection onto i yielding a function from $\prod G$ into $G(i)$ is defined by:

(Def. 3) For every element x of $\prod \overline{G}$ holds (the projection onto $i)(x) = x(i)$.

Let G be a real norm space sequence, let i be an element of $\operatorname{dom} G$, and let x be an element of $\prod G$. The functor reproj(i, x) yielding a function from $G(i)$ into $\prod G$ is defined by:

(Def. 4) For every element r of $G(i)$ holds $(\text{reproj}(i, x))(r) = x +\cdot (i, r)$.

Let G be a nontrivial real norm space sequence and let j be a set. Let us assume that $j \in \operatorname{dom} G$. The functor modetrans$(G, j)$ yields an element of $\operatorname{dom} G$ and is defined by:

(Def. 5) $\text{modetrans}(G, j) = j$.

Let G be a nontrivial real norm space sequence, let F be a non trivial real normed space, let i be a set, let f be a partial function from $\prod G$ to F, and let x be an element of $\prod G$. We say that f is partially differentiable in x w.r.t. i if and only if:

(Def. 6) $f \cdot \text{reproj}(\text{modetrans}(G, i), x)$ is differentiable in (the projection onto modetrans$(G, i))(x)$.

Let G be a nontrivial real norm space sequence, let F be a non trivial real normed space, let i be a set, let f be a partial function from $\prod G$ to F, and let x be a point of $\prod G$. The functor partdiff(f, x, i) yielding a point of the real norm space of bounded linear operators from $G(\text{modetrans}(G, i))$ into F is defined as follows:

(Def. 7) $\text{partdiff}(f, x, i) = (f \cdot \text{reproj}(\text{modetrans}(G, i), x))'((\text{the projection onto modetrans}(G, i))(x))$.

4. Linearity of Partial Differential Operator

For simplicity, we adopt the following rules: G denotes a nontrivial real norm space sequence, F denotes a non trivial real normed space, i denotes an element of $\operatorname{dom} G$, f, f_1, f_2 denote partial functions from $\prod G$ to F, x denotes a point of $\prod G$, and X denotes a set.

Let G be a nontrivial real norm space sequence, let F be a non trivial real normed space, let i be a set, let f be a partial function from $\prod G$ to F, and let X be a set. We say that f is partially differentiable on X w.r.t. i if and only if:

(Def. 8) $X \subseteq \operatorname{dom} f$ and for every point x of $\prod G$ such that $x \in X$ holds $f \upharpoonright X$ is partially differentiable in x w.r.t. i.

Next we state several propositions:

(21) For every element x_2 of $G(i)$ holds $\|(\operatorname{reproj}(i, 0_{\prod G}))(x_2)\| = \|x_2\|$.

(22) Let G be a nontrivial real norm space sequence, i be an element of $\operatorname{dom} G$, x be a point of $\prod G$, and r be a point of $G(i)$. Then $(\operatorname{reproj}(i, x))(r) - x = (\operatorname{reproj}(i, 0_{\prod G}))(r - (\text{the projection onto } i)(x))$ and $x - (\operatorname{reproj}(i, x))(r) = (\operatorname{reproj}(i, 0_{\prod G}))((\text{the projection onto } i)(x) - r)$.

(23) Let G be a nontrivial real norm space sequence, i be an element of $\operatorname{dom} G$, x be a point of $\prod G$, and Z be a subset of $\prod G$. Suppose Z is open and $x \in Z$. Then there exists a neighbourhood N of (the projection onto i)(x) such that for every point z of $G(i)$ if $z \in N$, then $(\operatorname{reproj}(i, x))(z) \in Z$.

(24) Let G be a nontrivial real norm space sequence, T be a non trivial real normed space, i be a set, f be a partial function from $\prod G$ to T, and Z be a subset of $\prod G$. Suppose Z is open. Then f is partially differentiable on Z w.r.t. i if and only if $Z \subseteq \operatorname{dom} f$ and for every point x of $\prod G$ such that $x \in Z$ holds f is partially differentiable in x w.r.t. i.

(25) For every set i such that $i \in \operatorname{dom} G$ and f is partially differentiable on X w.r.t. i holds X is a subset of $\prod G$.

Let G be a nontrivial real norm space sequence, let S be a non trivial real normed space, and let i be a set. Let us assume that $i \in \operatorname{dom} G$. Let f be a partial function from $\prod G$ to S and let X be a set. Let us assume that f is partially differentiable on X w.r.t. i. The functor $f \upharpoonright^i X$ yields a partial function from $\prod G$ to the real norm space of bounded linear operators from $G(\operatorname{modetrans}(G, i))$ into S and is defined by:

(Def. 9) $\operatorname{dom}(f \upharpoonright^i X) = X$ and for every point x of $\prod G$ such that $x \in X$ holds $(f \upharpoonright^i X)_x = \operatorname{partdiff}(f, x, i)$.

One can prove the following propositions:

(26) For every set i such that $i \in \operatorname{dom} G$ holds $(f_1 + f_2) \cdot \operatorname{reproj}(\operatorname{modetrans}(G, i), x) = f_1 \cdot \operatorname{reproj}(\operatorname{modetrans}(G, i), x) + f_2 \cdot$

reproj(modetrans$(G,i),x)$ and $(f_1 - f_2)\cdot$ reproj(modetrans$(G,i),x) =$ $f_1\cdot$reproj(modetrans$(G,i),x) - f_2\cdot$reproj(modetrans$(G,i),x)$.

(27) For every set i such that $i \in \operatorname{dom} G$ holds $r\cdot(f\cdot$reproj(modetrans$(G,i),x)) =$ $(r\cdot f)\cdot$reproj(modetrans$(G,i),x)$.

(28) Let i be a set. Suppose $i \in \operatorname{dom} G$ and f_1 is partially differentiable in x w.r.t. i and f_2 is partially differentiable in x w.r.t. i. Then f_1+f_2 is partially differentiable in x w.r.t. i and partdiff$(f_1 + f_2, x, i) =$ partdiff$(f_1, x, i) +$ partdiff(f_2, x, i).

(29) Let i be a set. Suppose $i \in \operatorname{dom} G$ and f_1 is partially differentiable in x w.r.t. i and f_2 is partially differentiable in x w.r.t. i. Then f_1-f_2 is partially differentiable in x w.r.t. i and partdiff$(f_1 - f_2, x, i) =$ partdiff$(f_1, x, i) -$ partdiff(f_2, x, i).

(30) Let i be a set. Suppose $i \in \operatorname{dom} G$ and f is partially differentiable in x w.r.t. i. Then $r\cdot f$ is partially differentiable in x w.r.t. i and partdiff$(r\cdot f, x, i) = r\cdot$ partdiff(f, x, i).

5. Continuous Differentiatibility of Partial Derivative

Next we state the proposition

(31) $\|$(the projection onto $i)(x)\| \leq \|x\|$.

Let G be a nontrivial real norm space sequence. One can verify that every point of $\prod G$ is len G-element.

We now state a number of propositions:

(32) Let G be a nontrivial real norm space sequence, T be a non trivial real normed space, i be a set, Z be a subset of $\prod G$, and f be a partial function from $\prod G$ to T. Suppose Z is open. Then f is partially differentiable on Z w.r.t. i if and only if $Z \subseteq \operatorname{dom} f$ and for every point x of $\prod G$ such that $x \in Z$ holds f is partially differentiable in x w.r.t. i.

(33) Let i, j be elements of dom G, x be a point of $G(i)$, and z be an element of $\prod \overline{G}$ such that $z =$ (reproj$(i, 0_{\prod G}))(x)$. Then

(i) if $i = j$, then $z(j) = x$, and

(ii) if $i \neq j$, then $z(j) = 0_{G(j)}$.

(34) For all points x, y of $G(i)$ holds (reproj$(i, 0_{\prod G}))(x + y) =$ (reproj$(i, 0_{\prod G}))(x) +$ (reproj$(i, 0_{\prod G}))(y)$.

(35) Let x, y be points of $\prod G$. Then (the projection onto $i)(x + y) =$ (the projection onto $i)(x) +$ (the projection onto $i)(y)$.

(36) For all points x, y of $G(i)$ holds (reproj$(i, 0_{\prod G}))(x - y) =$ (reproj$(i, 0_{\prod G}))(x) -$ (reproj$(i, 0_{\prod G}))(y)$.

(37) Let x, y be points of $\prod G$. Then (the projection onto i)$(x - y)$ = (the projection onto i)(x) − (the projection onto i)(y).

(38) For every point x of $G(i)$ such that $x \neq 0_{G(i)}$ holds $(\mathrm{reproj}(i, 0_{\prod G}))(x) \neq 0_{\prod G}$.

(39) For every point x of $G(i)$ and for every element a of $\mathbb{R}$ holds $(\mathrm{reproj}(i, 0_{\prod G}))(a \cdot x) = a \cdot (\mathrm{reproj}(i, 0_{\prod G}))(x)$.

(40) Let x be a point of $\prod G$ and a be an element of $\mathbb{R}$. Then (the projection onto i)$(a \cdot x) = a \cdot$ (the projection onto i)(x).

(41) Let G be a nontrivial real norm space sequence, S be a non trivial real normed space, f be a partial function from $\prod G$ to S, x be a point of $\prod G$, and i be a set. Suppose f is differentiable in x. Then f is partially differentiable in x w.r.t. i and $\mathrm{partdiff}(f, x, i) = f'(x) \cdot \mathrm{reproj}(\mathrm{modetrans}(G, i), 0_{\prod G})$.

(42) Let S be a real normed space and h, g be finite sequences of elements of S. Suppose $\mathrm{len}\, h = \mathrm{len}\, g + 1$ and for every natural number i such that $i \in \mathrm{dom}\, g$ holds $g_i = h_i - h_{i+1}$. Then $h_1 - h_{\mathrm{len}\, h} = \sum g$.

(43) Let G be a nontrivial real norm space sequence, x, y be elements of $\prod \overline{G}$, and Z be a set. Then $x{+}{\cdot}y{\restriction}Z$ is an element of $\prod \overline{G}$.

(44) Let G be a nontrivial real norm space sequence, x, y be points of $\prod G$, Z, x_0 be elements of $\prod \overline{G}$, and X be a set. If $Z = 0_{\prod G}$ and $x_0 = x$ and $y = Z{+}{\cdot}x_0{\restriction}X$, then $\|y\| \leq \|x\|$.

(45) Let G be a nontrivial real norm space sequence, S be a non trivial real normed space, f be a partial function from $\prod G$ to S, and x, y be points of $\prod G$. Then there exists a finite sequence h of elements of $\prod G$ and there exists a finite sequence g of elements of S and there exist elements Z, y_0 of $\prod \overline{G}$ such that
$y_0 = y$ and $Z = 0_{\prod G}$ and $\mathrm{len}\, h = \mathrm{len}\, G + 1$ and $\mathrm{len}\, g = \mathrm{len}\, G$ and for every natural number i such that $i \in \mathrm{dom}\, h$ holds $h_i = Z{+}{\cdot}y_0{\restriction}\mathrm{Seg}((\mathrm{len}\, G + 1) -' i)$ and for every natural number i such that $i \in \mathrm{dom}\, g$ holds $g_i = f_{x+h_i} - f_{x+h_{i+1}}$ and for every natural number i and for every point h_1 of $\prod G$ such that $i \in \mathrm{dom}\, h$ and $h_i = h_1$ holds $\|h_1\| \leq \|y\|$ and $f_{x+y} - f_x = \sum g$.

(46) Let G be a nontrivial real norm space sequence, i be an element of $\mathrm{dom}\, G$, x, y be points of $\prod G$, and x_2 be a point of $G(i)$. If $y = (\mathrm{reproj}(i, x))(x_2)$, then (the projection onto i)$(y) = x_2$.

(47) Let G be a nontrivial real norm space sequence, i be an element of $\mathrm{dom}\, G$, y be a point of $\prod G$, and q be a point of $G(i)$. If $q =$ (the projection onto i)(y), then $y = (\mathrm{reproj}(i, y))(q)$.

(48) Let G be a nontrivial real norm space sequence, i be an element of $\mathrm{dom}\, G$, x, y be points of $\prod G$, and x_2 be a point of $G(i)$. If $y = (\mathrm{reproj}(i, x))(x_2)$, then $\mathrm{reproj}(i, x) = \mathrm{reproj}(i, y)$.

(49) Let G be a nontrivial real norm space sequence, i, j be elements of $\operatorname{dom} G$, x, y be points of $\prod G$, and x_2 be a point of $G(i)$. Suppose $y = (\operatorname{reproj}(i, x))(x_2)$ and $i \neq j$. Then (the projection onto j)$(x) =$ (the projection onto j)(y).

(50) Let G be a nontrivial real norm space sequence, F be a non trivial real normed space, i be an element of $\operatorname{dom} G$, x be a point of $\prod G$, x_2 be a point of $G(i)$, f be a partial function from $\prod G$ to F, and g be a partial function from $G(i)$ to F. If (the projection onto i)$(x) = x_2$ and $g = f \cdot \operatorname{reproj}(i, x)$, then $g'(x_2) = \operatorname{partdiff}(f, x, i)$.

(51) Let G be a nontrivial real norm space sequence, F be a non trivial real normed space, f be a partial function from $\prod G$ to F, x be a point of $\prod G$, i be a set, M be a real number, L be a point of the real norm space of bounded linear operators from $G(\operatorname{modetrans}(G, i))$ into F, and p, q be points of $G(\operatorname{modetrans}(G, i))$. Suppose that

(i) $i \in \operatorname{dom} G$,

(ii) for every point h of $G(\operatorname{modetrans}(G, i))$ such that $h \in]p, q[$ holds $\|\operatorname{partdiff}(f, (\operatorname{reproj}(\operatorname{modetrans}(G, i), x))(h), i) - L\| \leq M$,

(iii) for every point h of $G(\operatorname{modetrans}(G, i))$ such that $h \in [p, q]$ holds $(\operatorname{reproj}(\operatorname{modetrans}(G, i), x))(h) \in \operatorname{dom} f$, and

(iv) for every point h of $G(\operatorname{modetrans}(G, i))$ such that $h \in [p, q]$ holds f is partially differentiable in $(\operatorname{reproj}(\operatorname{modetrans}(G, i), x))(h)$ w.r.t. i.

Then $\|f_{(\operatorname{reproj}(\operatorname{modetrans}(G,i),x))(q)} - f_{(\operatorname{reproj}(\operatorname{modetrans}(G,i),x))(p)} - L(q - p)\| \leq M \cdot \|q - p\|$.

(52) Let G be a nontrivial real norm space sequence, x, y, z, w be points of $\prod G$, i be an element of $\operatorname{dom} G$, d be a real number, and p, q, r be points of $G(i)$. Suppose $\|y - x\| < d$ and $\|z - x\| < d$ and $p =$ (the projection onto i)(y) and $z = (\operatorname{reproj}(i, y))(q)$ and $r \in [p, q]$ and $w = (\operatorname{reproj}(i, y))(r)$. Then $\|w - x\| < d$.

(53) Let G be a nontrivial real norm space sequence, S be a non trivial real normed space, f be a partial function from $\prod G$ to S, X be a subset of $\prod G$, x, y, z be points of $\prod G$, i be a set, p, q be points of $G(\operatorname{modetrans}(G, i))$, and d, r be real numbers. Suppose that $i \in \operatorname{dom} G$ and X is open and $x \in X$ and $\|y - x\| < d$ and $\|z - x\| < d$ and $X \subseteq \operatorname{dom} f$ and for every point x of $\prod G$ such that $x \in X$ holds f is partially differentiable in x w.r.t. i and for every point z of $\prod G$ such that $\|z - x\| < d$ holds $z \in X$ and for every point z of $\prod G$ such that $\|z - x\| < d$ holds $\|\operatorname{partdiff}(f, z, i) - \operatorname{partdiff}(f, x, i)\| \leq r$ and $z = (\operatorname{reproj}(\operatorname{modetrans}(G, i), y))(p)$ and $q =$ (the projection onto $\operatorname{modetrans}(G, i)$)$(y)$. Then $\|f_z - f_y - (\operatorname{partdiff}(f, x, i))(p - q)\| \leq \|p - q\| \cdot r$.

(54) Let G be a nontrivial real norm space sequence, h be a finite sequence of elements of $\prod G$, y, x be points of $\prod G$, y_0, Z be elements of $\prod \overline{G}$, and j be an element of $\mathbb{N}$. Suppose $y = y_0$ and $Z = 0_{\prod G}$ and

$\operatorname{len} h = \operatorname{len} G + 1$ and $1 \leq j \leq \operatorname{len} G$ and for every natural number i such that $i \in \operatorname{dom} h$ holds $h_i = Z + \cdot y_0 \upharpoonright \operatorname{Seg}((\operatorname{len} G + 1) -' i)$. Then $x + h_j = (\operatorname{reproj}(\operatorname{modetrans}(G, (\operatorname{len} G + 1) -' j), x + h_{j+1}))((\text{the projection onto } \operatorname{modetrans}(G, (\operatorname{len} G + 1) -' j))(x + y))$.

(55) Let G be a nontrivial real norm space sequence, h be a finite sequence of elements of $\prod G$, y, x be points of $\prod G$, y_0, Z be elements of $\prod \overline{G}$, and j be an element of $\mathbb{N}$. Suppose $y = y_0$ and $Z = 0_{\prod G}$ and $\operatorname{len} h = \operatorname{len} G + 1$ and $1 \leq j \leq \operatorname{len} G$ and for every natural number i such that $i \in \operatorname{dom} h$ holds $h_i = Z + \cdot y_0 \upharpoonright \operatorname{Seg}((\operatorname{len} G + 1) -' i)$. Then (the projection onto $\operatorname{modetrans}(G, (\operatorname{len} G + 1) -' j))(x + y) - (\text{the projection onto } \operatorname{modetrans}(G, (\operatorname{len} G + 1) -' j))(x + h_{j+1}) = (\text{the projection onto } \operatorname{modetrans}(G, (\operatorname{len} G + 1) -' j))(y)$.

(56) Let G be a nontrivial real norm space sequence, S be a non trivial real normed space, f be a partial function from $\prod G$ to S, X be a subset of $\prod G$, and x be a point of $\prod G$. Suppose that

(i) X is open,

(ii) $x \in X$, and

(iii) for every set i such that $i \in \operatorname{dom} G$ holds f is partially differentiable on X w.r.t. i and $f \upharpoonright^i X$ is continuous on X.

Then

(iv) f is differentiable in x, and

(v) for every point h of $\prod G$ there exists a finite sequence w of elements of S such that $\operatorname{dom} w = \operatorname{dom} G$ and for every set i such that $i \in \operatorname{dom} G$ holds $w(i) = (\operatorname{partdiff}(f, x, i))((\text{the projection onto } \operatorname{modetrans}(G, i))(h))$ and $f'(x)(h) = \sum w$.

(57) Let G be a nontrivial real norm space sequence, F be a non trivial real normed space, f be a partial function from $\prod G$ to F, and X be a subset of $\prod G$. Suppose X is open. Then for every set i such that $i \in \operatorname{dom} G$ holds f is partially differentiable on X w.r.t. i and $f \upharpoonright^i X$ is continuous on X if and only if f is differentiable on X and $f'_{\upharpoonright X}$ is continuous on X.

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. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 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] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

[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. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.
[12] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[13] Czesław Byliński. Introduction to real linear topological spaces. *Formalized Mathematics*, 13(**1**):99–107, 2005.
[14] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[15] Noboru Endou, Yasunari Shidama, and Keiichi Miyajima. The product space of real normed spaces and its properties. *Formalized Mathematics*, 15(**3**):81–85, 2007, doi:10.2478/v10037-007-0010-y.
[16] Hiroshi Imura, Morishige Kimura, and Yasunari Shidama. The differentiable functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):321–327, 2004.
[17] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[18] Anna Lango and Grzegorz Bancerek. Product of families of groups and vector spaces. *Formalized Mathematics*, 3(**2**):235–240, 1992.
[19] Hiroyuki Okazaki, Noboru Endou, Keiko Narita, and Yasunari Shidama. Differentiable functions into real normed spaces. *Formalized Mathematics*, 19(**2**):69–72, 2011, doi: 10.2478/v10037-011-0012-7.
[20] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[21] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[22] Konrad Raczkowski and Paweł Sadowski. Real function differentiability. *Formalized Mathematics*, 1(**4**):797–801, 1990.
[23] Laurent Schwartz. Cours d'analyse, vol. 1. *Hermann Paris*, 1967.
[24] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.
[25] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[26] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[27] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[28] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[29] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[30] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[31] Hiroshi Yamazaki and Yasunari Shidama. Algebra of vector functions. *Formalized Mathematics*, 3(**2**):171–175, 1992.

Received June 2, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 41–45, 2012
DOI: 10.2478/v10037-012-0006-0

VERSITA
versita.com/fm/

Planes and Spheres as Topological Manifolds. Stereographic Projection

Marco Riccardi
Via del Pero 102
54038 Montignoso
Italy

Summary. The goal of this article is to show some examples of topological manifolds: planes and spheres in Euclidean space. In doing it, the article introduces the stereographic projection [25].

MML identifier: MFOLD_2, version: 7.12.01 4.167.1133

The papers [29], [34], [9], [14], [40], [41], [11], [10], [4], [2], [18], [13], [31], [20], [21], [30], [32], [16], [17], [35], [26], [1], [22], [38], [36], [24], [19], [37], [28], [6], [15], [8], [27], [39], [3], [42], [12], [23], [7], [5], and [33] provide the notation and terminology for this paper.

1. Preliminaries

Let us observe that $\emptyset$ is $\emptyset$-valued and $\emptyset$ is onto.

Next we state three propositions:

(1) For every function f and for every set Y holds $\operatorname{dom}(Y \upharpoonright f) = f^{-1}(Y)$.

(2) For every function f and for all sets Y_1, Y_2 such that $Y_2 \subseteq Y_1$ holds $(Y_1 \upharpoonright f)^{-1}(Y_2) = f^{-1}(Y_2)$.

(3) Let S, T be topological structures and f be a function from S into T. If f is homeomorphism, then f^{-1} is homeomorphism.

Let S, T be topological structures. Let us note that the predicate S and T are homeomorphic is symmetric.

For simplicity, we use the following convention: T_1, T_2, T_3 denote topological spaces, A_1 denotes a subset of T_1, A_2 denotes a subset of T_2, and A_3 denotes a subset of T_3.

ISSN 1426–2630(p), 1898-9934(e)

Next we state several propositions:

(4) Let f be a function from T_1 into T_2. Suppose f is homeomorphism. Let g be a function from $T_1{\restriction}f^{-1}(A_2)$ into $T_2{\restriction}A_2$. If $g = A_2{\restriction}f$, then g is homeomorphism.

(5) For every function f from T_1 into T_2 such that f is homeomorphism holds $f^{-1}(A_2)$ and A_2 are homeomorphic.

(6) If A_1 and A_2 are homeomorphic, then A_2 and A_1 are homeomorphic.

(7) If A_1 and A_2 are homeomorphic, then A_1 is empty iff A_2 is empty.

(8) If A_1 and A_2 are homeomorphic and A_2 and A_3 are homeomorphic, then A_1 and A_3 are homeomorphic.

(9) If T_1 is second-countable and T_1 and T_2 are homeomorphic, then T_2 is second-countable.

In the sequel n, k are natural numbers and M, N are non empty topological spaces.

The following propositions are true:

(10) If M is Hausdorff and M and N are homeomorphic, then N is Hausdorff.

(11) If M is n-locally Euclidean and M and N are homeomorphic, then N is n-locally Euclidean.

(12) If M is n-manifold and M and N are homeomorphic, then N is n-manifold.

(13) Let x_1, x_2 be finite sequences of elements of $\mathbb{R}$ and i be an element of $\mathbb{N}$. If $i \in \operatorname{dom}(x_1 \bullet x_2)$, then $(x_1 \bullet x_2)(i) = (x_1)_i \cdot (x_2)_i$ and $(x_1 \bullet x_2)_i = (x_1)_i \cdot (x_2)_i$.

(14) For all finite sequences x_1, x_2, y_1, y_2 of elements of $\mathbb{R}$ such that $\operatorname{len} x_1 = \operatorname{len} x_2$ and $\operatorname{len} y_1 = \operatorname{len} y_2$ holds $x_1 \frown y_1 \bullet x_2 \frown y_2 = (x_1 \bullet x_2) \frown (y_1 \bullet y_2)$.

(15) For all finite sequences x_1, x_2, y_1, y_2 of elements of $\mathbb{R}$ such that $\operatorname{len} x_1 = \operatorname{len} x_2$ and $\operatorname{len} y_1 = \operatorname{len} y_2$ holds $|(x_1 \frown y_1, x_2 \frown y_2)| = |(x_1, x_2)| + |(y_1, y_2)|$.

In the sequel p, q, p_1 are points of $\mathcal{E}^n_{\mathrm{T}}$ and r is a real number.

One can prove the following propositions:

(16) If $k \in \operatorname{Seg} n$, then $(p_1 + p_2)(k) = p_1(k) + p_2(k)$.

(17) For every set X holds X is a linear combination of $\mathbb{R}_{\mathbb{R}}^{\operatorname{Seg} n}$ iff X is a linear combination of $\mathcal{E}^n_{\mathrm{T}}$.

(18) Let F be a finite sequence of elements of $\mathcal{E}^n_{\mathrm{T}}$, f_1 be a function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathbb{R}$, F_1 be a finite sequence of elements of $\mathbb{R}_{\mathbb{R}}^{\operatorname{Seg} n}$, and f_2 be a function from $\mathbb{R}_{\mathbb{R}}^{\operatorname{Seg} n}$ into $\mathbb{R}$. If $f_1 = f_2$ and $F = F_1$, then $f_1 \cdot F = f_2 \cdot F_1$.

(19) Let F be a finite sequence of elements of $\mathcal{E}^n_{\mathrm{T}}$ and F_1 be a finite sequence of elements of $\mathbb{R}_{\mathbb{R}}^{\operatorname{Seg} n}$. If $F_1 = F$, then $\sum F = \sum F_1$.

(20) For every linear combination L_2 of $\mathbb{R}_{\mathbb{R}}^{\operatorname{Seg} n}$ and for every linear combination L_1 of $\mathcal{E}^n_{\mathrm{T}}$ such that $L_1 = L_2$ holds $\sum L_1 = \sum L_2$.

(21) Let A_4 be a subset of $\mathbb{R}_{\mathbb{R}}^{\operatorname{Seg} n}$ and A_5 be a subset of $\mathcal{E}_{\mathrm{T}}^n$. Suppose $A_4 = A_5$. Then A_4 is linearly independent if and only if A_5 is linearly independent.

(22) For every subset V of $\mathcal{E}_{\mathrm{T}}^n$ such that $V = \mathbb{R}\mathrm{N}\text{-Base}\, n$ there exists a linear combination l of V such that $p = \sum l$.

(23) $\mathbb{R}\mathrm{N}\text{-Base}\, n$ is a basis of $\mathcal{E}_{\mathrm{T}}^n$.

(24) Let V be a subset of $\mathcal{E}_{\mathrm{T}}^n$. Then $V \in$ the topology of $\mathcal{E}_{\mathrm{T}}^n$ if and only if for every p such that $p \in V$ there exists r such that $r > 0$ and $\operatorname{Ball}(p, r) \subseteq V$.

Let n be a natural number and let p be a point of $\mathcal{E}_{\mathrm{T}}^n$.

The functor InnerProduct p yields a function from $\mathcal{E}_{\mathrm{T}}^n$ into $\mathbb{R}^{\mathbf{1}}$ and is defined by:

(Def. 1) For every point q of $\mathcal{E}_{\mathrm{T}}^n$ holds $(\text{InnerProduct}\, p)(q) = |(p, q)|$.

Let us consider n, p. Note that InnerProduct p is continuous.

2. PLANES

Let us consider n and let us consider p, q. The functor $\operatorname{Plane}(p, q)$ yielding a subset of $\mathcal{E}_{\mathrm{T}}^n$ is defined as follows:

(Def. 2) $\operatorname{Plane}(p, q) = \{y; y \text{ ranges over points of } \mathcal{E}_{\mathrm{T}}^n \colon |(p, y - q)| = 0\}$.

The following propositions are true:

(25) $(\operatorname{transl}(p_1, \mathcal{E}_{\mathrm{T}}^n))^\circ \operatorname{Plane}(p, p_2) = \operatorname{Plane}(p, p_1 + p_2)$.

(26) If $p \neq 0_{\mathcal{E}_{\mathrm{T}}^n}$, then there exists a linearly independent subset A of $\mathcal{E}_{\mathrm{T}}^n$ such that $\overline{\overline{A}} = n - 1$ and $\Omega_{\operatorname{Lin}(A)} = \operatorname{Plane}(p, 0_{\mathcal{E}_{\mathrm{T}}^n})$.

(27) If $p_1 \neq 0_{\mathcal{E}_{\mathrm{T}}^n}$ and $p_2 \neq 0_{\mathcal{E}_{\mathrm{T}}^n}$, then there exists a function R from $\mathcal{E}_{\mathrm{T}}^n$ into $\mathcal{E}_{\mathrm{T}}^n$ such that R is homeomorphism and $R^\circ \operatorname{Plane}(p_1, 0_{\mathcal{E}_{\mathrm{T}}^n}) = \operatorname{Plane}(p_2, 0_{\mathcal{E}_{\mathrm{T}}^n})$.

Let us consider n and let us consider p, q. The functor $\operatorname{TPlane}(p, q)$ yields a non empty subspace of $\mathcal{E}_{\mathrm{T}}^n$ and is defined by:

(Def. 3) $\operatorname{TPlane}(p, q) = \mathcal{E}_{\mathrm{T}}^n \restriction \operatorname{Plane}(p, q)$.

The following three propositions are true:

(28) The base finite sequence of $n + 1$ and $n + 1 = (0_{\mathcal{E}_{\mathrm{T}}^n}) \frown \langle 1 \rangle$.

(29) For all points p, q of $\mathcal{E}_{\mathrm{T}}^{n+1}$ such that $p \neq 0_{\mathcal{E}_{\mathrm{T}}^{n+1}}$ holds $\mathcal{E}_{\mathrm{T}}^n$ and $\operatorname{TPlane}(p, q)$ are homeomorphic.

(30) For all points p, q of $\mathcal{E}_{\mathrm{T}}^{n+1}$ such that $p \neq 0_{\mathcal{E}_{\mathrm{T}}^{n+1}}$ holds $\operatorname{TPlane}(p, q)$ is n-manifold.

3. Spheres

Let us consider n. The functor $\mathbb{S}^n$ yields a topological space and is defined by:

(Def. 4) $\mathbb{S}^n = \mathrm{TopUnitCircle}(n+1)$.

Let us consider n. Note that $\mathbb{S}^n$ is non empty.

Let us consider n, p and let S be a subspace of $\mathcal{E}^n_{\mathrm{T}}$. Let us assume that $p \in \mathrm{Sphere}((0_{\mathcal{E}^n_{\mathrm{T}}}), 1)$. The functor $\sigma_{S,p}$ yielding a function from S into $\mathrm{TPlane}(p, 0_{\mathcal{E}^n_{\mathrm{T}}})$ is defined as follows:

(Def. 5) For every q such that $q \in S$ holds $(\sigma_{S,p})(q) = \frac{1}{1-|(q,p)|} \cdot (q - |(q,p)| \cdot p)$.

Next we state the proposition

(31) For every subspace S of $\mathcal{E}^n_{\mathrm{T}}$ such that $\Omega_S = \mathrm{Sphere}((0_{\mathcal{E}^n_{\mathrm{T}}}), 1) \setminus \{p\}$ and $p \in \mathrm{Sphere}((0_{\mathcal{E}^n_{\mathrm{T}}}), 1)$ holds $\sigma_{S,p}$ is homeomorphism.

Let us consider n. One can verify the following observations:

* $\mathbb{S}^n$ is second-countable,
* $\mathbb{S}^n$ is n-locally Euclidean, and
* $\mathbb{S}^n$ is n-manifold.

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. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[5] Grzegorz Bancerek. Monoids. *Formalized Mathematics*, 3(**2**):213–225, 1992.
[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[7] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 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. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[13] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[14] Agata Darmochwał. Families of subsets, subspaces and mappings in topological spaces. *Formalized Mathematics*, 1(**2**):257–261, 1990.
[15] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[16] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[17] Agata Darmochwał and Yatsuka Nakamura. Metric spaces as topological spaces – fundamental concepts. *Formalized Mathematics*, 2(**4**):605–608, 1991.
[18] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[19] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.

[20] Stanisława Kanas, Adam Lecko, and Mariusz Startek. Metric spaces. *Formalized Mathematics*, 1(**3**):607–610, 1990.
[21] Artur Korniłowicz and Yasunari Shidama. Intersections of intervals and balls in $\mathcal{E}^n_{\mathrm{T}}$. *Formalized Mathematics*, 12(**3**):301–306, 2004.
[22] Artur Korniłowicz and Yasunari Shidama. Some properties of circles on the plane. *Formalized Mathematics*, 13(**1**):117–124, 2005.
[23] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[24] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[25] John M. Lee. *Introduction to Topological Manifolds*. Springer-Verlag, New York Berlin Heidelberg, 2000.
[26] Robert Milewski. Bases of continuous lattices. *Formalized Mathematics*, 7(**2**):285–294, 1998.
[27] Yatsuka Nakamura, Artur Korniłowicz, Nagato Oya, and Yasunari Shidama. The real vector spaces of finite sequences are finite dimensional. *Formalized Mathematics*, 17(**1**):1–9, 2009, doi:10.2478/v10037-009-0001-2.
[28] Henryk Oryszczyszyn and Krzysztof Prażmowski. Real functions spaces. *Formalized Mathematics*, 1(**3**):555–561, 1990.
[29] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[30] Beata Padlewska. Locally connected spaces. *Formalized Mathematics*, 2(**1**):93–96, 1991.
[31] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[32] Karol Pąk. Basic properties of metrizable topological spaces. *Formalized Mathematics*, 17(**3**):201–205, 2009, doi: 10.2478/v10037-009-0024-8.
[33] Marco Riccardi. The definition of topological manifolds. *Formalized Mathematics*, 19(**1**):41–44, 2011, doi: 10.2478/v10037-011-0007-4.
[34] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[35] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[36] Wojciech A. Trybulec. Basis of real linear space. *Formalized Mathematics*, 1(**5**):847–850, 1990.
[37] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(**3**):581–588, 1990.
[38] Wojciech A. Trybulec. Subspaces and cosets of subspaces in real linear space. *Formalized Mathematics*, 1(**2**):297–301, 1990.
[39] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[40] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[41] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[42] Mariusz Żynel and Adam Guzowski. T_0 topological spaces. *Formalized Mathematics*, 5(**1**):75–77, 1996.

Received June 6, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 47–59, 2012
DOI: 10.2478/v10037-012-0007-z

VERSITA
versita.com/fm/

$\mathbb{Z}$-modules

Yuichi Futa
Shinshu University
Nagano, Japan

Hiroyuki Okazaki[1]
Shinshu University
Nagano, Japan

Yasunari Shidama[2]
Shinshu University
Nagano, Japan

Summary. In this article, we formalize $\mathbb{Z}$-module, that is a module over integer ring. $\mathbb{Z}$-module is necassary for lattice problems, LLL (Lenstra-Lenstra-Lovász) base reduction algorithm and cryptographic systems with lattices [11].

MML identifier: ZMODUL01, version: 7.12.01 4.167.1133

The papers [10], [17], [18], [7], [2], [9], [14], [8], [6], [13], [5], [1], [15], [4], [3], [19], [16], and [12] provide the terminology and notation for this paper.

1. Definition of $\mathbb{Z}$-module

We introduce $\mathbb{Z}$-module structures which are extensions of additive loop structure and are systems

$\langle$ a carrier, a zero, an addition, an external multiplication $\rangle$,

where the carrier is a set, the zero is an element of the carrier, the addition is a binary operation on the carrier, and the external multiplication is a function from $\mathbb{Z} \times$ the carrier into the carrier.

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

Let V be a $\mathbb{Z}$-module structure. A vector of V is an element of V.

In the sequel V denotes a non empty $\mathbb{Z}$-module structure and v denotes a vector of V.

Let us consider V, v and let a be an integer number. The functor $a \cdot v$ yields an element of V and is defined by:

(Def. 1) $a \cdot v =$ (the external multiplication of V)(a, v).

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

ISSN 1426–2630(p), 1898-9934(e)

Let Z_1 be a non empty set, let O be an element of Z_1, let F be a binary operation on Z_1, and let G be a function from $\mathbb{Z} \times Z_1$ into Z_1. One can verify that $\langle Z_1, O, F, G \rangle$ is non empty.

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

(Def. 2) For every a and for all vectors v, w of I_1 holds $a \cdot (v + w) = a \cdot v + a \cdot w$.

We say that I_1 is scalar distributive if and only if:

(Def. 3) For all a, b and for every vector v of I_1 holds $(a + b) \cdot v = a \cdot v + b \cdot v$.

We say that I_1 is scalar associative if and only if:

(Def. 4) For all a, b and for every vector v of I_1 holds $(a \cdot b) \cdot v = a \cdot (b \cdot v)$.

We say that I_1 is scalar unital if and only if:

(Def. 5) For every vector v of I_1 holds $1 \cdot v = v$.

The strict $\mathbb{Z}$-module structure the trivial structure of $\mathbb{Z}$-module is defined as follows:

(Def. 6) The trivial structure of $\mathbb{Z}$-module $= \langle 1, \mathrm{op}_0, \mathrm{op}_2, \pi_2(\mathbb{Z} \times 1) \rangle$.

Let us observe that the trivial structure of $\mathbb{Z}$-module is trivial and non empty.

Let us observe that there exists a non empty $\mathbb{Z}$-module structure which is strict, Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, and scalar unital.

A $\mathbb{Z}$-module is an Abelian add-associative right zeroed right complementable scalar distributive vector distributive scalar associative scalar unital non empty $\mathbb{Z}$-module structure.

In the sequel v, w denote vectors of V.

Let I_1 be a non empty $\mathbb{Z}$-module structure. We say that I_1 inherits cancelable on multiplication if and only if:

(Def. 7) For every a and for every vector v of I_1 such that $a \cdot v = 0_{(I_1)}$ holds $a = 0$ or $v = 0_{(I_1)}$.

The following propositions are true:

(1) If $a = 0$ or $v = 0_V$, then $a \cdot v = 0_V$.

(2) $-v = (-1) \cdot v$.

(3) If V inherits cancelable on multiplication and $v = -v$, then $v = 0_V$.

(4) If V inherits cancelable on multiplication and $v + v = 0_V$, then $v = 0_V$.

(5) $a \cdot -v = (-a) \cdot v$.

(6) $a \cdot -v = -a \cdot v$.

(7) $(-a) \cdot -v = a \cdot v$.

(8) $a \cdot (v - w) = a \cdot v - a \cdot w$.

(9) $(a - b) \cdot v = a \cdot v - b \cdot v$.

(10) If V inherits cancelable on multiplication and $a \neq 0$ and $a \cdot v = a \cdot w$, then $v = w$.

(11) If V inherits cancelable on multiplication and $v \neq 0_V$ and $a \cdot v = b \cdot v$, then $a = b$.

For simplicity, we follow the rules: V is a $\mathbb{Z}$-module, u, v, w are vectors of V, F, G, H, I are finite sequences of elements of V, j, k, n are elements of $\mathbb{N}$, and f_9 is a function from $\mathbb{N}$ into the carrier of V.

Next we state several propositions:

(12) If $\operatorname{len} F = \operatorname{len} G$ and for all k, v such that $k \in \operatorname{dom} F$ and $v = G(k)$ holds $F(k) = a \cdot v$, then $\sum F = a \cdot \sum G$.

(13) For every $\mathbb{Z}$-module V and for every integer a holds $a \cdot \sum(\varepsilon_{(\text{the carrier of } V)}) = 0_V$.

(14) For every $\mathbb{Z}$-module V and for every integer a and for all vectors v, u of V holds $a \cdot \sum\langle v, u\rangle = a \cdot v + a \cdot u$.

(15) For every $\mathbb{Z}$-module V and for every integer a and for all vectors v, u, w of V holds $a \cdot \sum\langle v, u, w\rangle = a \cdot v + a \cdot u + a \cdot w$.

(16) $(-a) \cdot v = -a \cdot v$.

(17) If $\operatorname{len} F = \operatorname{len} G$ and for every k such that $k \in \operatorname{dom} F$ holds $G(k) = a \cdot F_k$, then $\sum G = a \cdot \sum F$.

2. Submodules and Cosets of Submodules in $\mathbb{Z}$-module

We use the following convention: V, X are $\mathbb{Z}$-modules, V_1, V_2, V_3 are subsets of V, and x is a set.

Let us consider V, V_1. We say that V_1 is linearly closed if and only if:

(Def. 8) For all v, u such that v, $u \in V_1$ holds $v + u \in V_1$ and for all a, v such that $v \in V_1$ holds $a \cdot v \in V_1$.

One can prove the following propositions:

(18) If $V_1 \neq \emptyset$ and V_1 is linearly closed, then $0_V \in V_1$.

(19) If V_1 is linearly closed, then for every v such that $v \in V_1$ holds $-v \in V_1$.

(20) If V_1 is linearly closed, then for all v, u such that v, $u \in V_1$ holds $v - u \in V_1$.

(21) If the carrier of $V = V_1$, then V_1 is linearly closed.

(22) If V_1 is linearly closed and V_2 is linearly closed and $V_3 = \{v + u : v \in V_1 \wedge u \in V_2\}$, then V_3 is linearly closed.

Let us consider V. Observe that $\{0_V\}$ is linearly closed.

Let us consider V. Note that there exists a subset of V which is linearly closed.

Let us consider V and let V_1, V_2 be linearly closed subsets of V. Note that $V_1 \cap V_2$ is linearly closed.

Let us consider V. A $\mathbb{Z}$-module is called a submodule of V if it satisfies the conditions (Def. 9).

(Def. 9)(i) The carrier of it $\subseteq$ the carrier of V,

(ii) $0_{\text{it}} = 0_V$,

(iii) the addition of it = (the addition of V) $\restriction$ (the carrier of it), and

(iv) the external multiplication of it = (the external multiplication of V)$\restriction(\mathbb{Z} \times$ the carrier of it).

In the sequel W_2 denotes a submodule of V and w, w_1, w_2 denote vectors of W.

We now state a number of propositions:

(23) If $x \in W_1$ and W_1 is a submodule of W_2, then $x \in W_2$.

(24) If $x \in W$, then $x \in V$.

(25) w is a vector of V.

(26) $0_W = 0_V$.

(27) $0_{(W_1)} = 0_{(W_2)}$.

(28) If $w_1 = v$ and $w_2 = u$, then $w_1 + w_2 = v + u$.

(29) If $w = v$, then $a \cdot w = a \cdot v$.

(30) If $w = v$, then $-v = -w$.

(31) If $w_1 = v$ and $w_2 = u$, then $w_1 - w_2 = v - u$.

(32) V is a submodule of V.

(33) $0_V \in W$.

(34) $0_{(W_1)} \in W_2$.

(35) $0_W \in V$.

(36) If u, $v \in W$, then $u + v \in W$.

(37) If $v \in W$, then $a \cdot v \in W$.

(38) If $v \in W$, then $-v \in W$.

(39) If u, $v \in W$, then $u - v \in W$.

In the sequel d_1 is an element of D, A is a binary operation on D, and M is a function from $\mathbb{Z} \times D$ into D.

We now state several propositions:

(40) Suppose $V_1 = D$ and $d_1 = 0_V$ and $A =$ (the addition of V) $\restriction$ (V_1) and $M =$ (the external multiplication of V)$\restriction(\mathbb{Z} \times V_1)$. Then $\langle D, d_1, A, M \rangle$ is a submodule of V.

(41) For all strict $\mathbb{Z}$-modules V, X such that V is a submodule of X and X is a submodule of V holds $V = X$.

(42) If V is a submodule of X and X is a submodule of Y, then V is a submodule of Y.

(43) If the carrier of $W_1 \subseteq$ the carrier of W_2, then W_1 is a submodule of W_2.

(44) If for every v such that $v \in W_1$ holds $v \in W_2$, then W_1 is a submodule of W_2.

Let us consider V. Note that there exists a submodule of V which is strict.

Next we state several propositions:

(45) For all strict submodules W_1, W_2 of V such that the carrier of W_1 = the carrier of W_2 holds $W_1 = W_2$.

(46) For all strict submodules W_1, W_2 of V such that for every v holds $v \in W_1$ iff $v \in W_2$ holds $W_1 = W_2$.

(47) Let V be a strict $\mathbb{Z}$-module and W be a strict submodule of V. If the carrier of W = the carrier of V, then $W = V$.

(48) Let V be a strict $\mathbb{Z}$-module and W be a strict submodule of V. If for every vector v of V holds $v \in W$ iff $v \in V$, then $W = V$.

(49) If the carrier of $W = V_1$, then V_1 is linearly closed.

(50) If $V_1 \neq \emptyset$ and V_1 is linearly closed, then there exists a strict submodule W of V such that V_1 = the carrier of W.

Let us consider V. The functor $\mathbf{0}_V$ yielding a strict submodule of V is defined by:

(Def. 10) The carrier of $\mathbf{0}_V = \{0_V\}$.

Let us consider V. The functor Ω_V yields a strict submodule of V and is defined by:

(Def. 11) Ω_V = the $\mathbb{Z}$-module structure of V.

We now state several propositions:

(51) $\mathbf{0}_W = \mathbf{0}_V$.

(52) $\mathbf{0}_{(W_1)} = \mathbf{0}_{(W_2)}$.

(53) $\mathbf{0}_W$ is a submodule of V.

(54) $\mathbf{0}_V$ is a submodule of W.

(55) $\mathbf{0}_{(W_1)}$ is a submodule of W_2.

(56) Every strict $\mathbb{Z}$-module V is a submodule of Ω_V.

Let us consider V, v, W. The functor $v + W$ yields a subset of V and is defined as follows:

(Def. 12) $v + W = \{v + u : u \in W\}$.

Let us consider V, W. A subset of V is called a coset of W if:

(Def. 13) There exists v such that it $= v + W$.

In the sequel B, C are cosets of W.

The following propositions are true:

(57) $0_V \in v + W$ iff $v \in W$.

(58) $v \in v + W$.

(59) $0_V + W$ = the carrier of W.

(60) $v + \mathbf{0}_V = \{v\}$.

(61) $v + \Omega_V$ = the carrier of V.

(62) $0_V \in v + W$ iff $v + W =$ the carrier of W.

(63) $v \in W$ iff $v + W =$ the carrier of W.

(64) If $v \in W$, then $a \cdot v + W =$ the carrier of W.

(65) $u \in W$ iff $v + W = v + u + W$.

(66) $u \in W$ iff $v + W = (v - u) + W$.

(67) $v \in u + W$ iff $u + W = v + W$.

(68) If $u \in v_1 + W$ and $u \in v_2 + W$, then $v_1 + W = v_2 + W$.

(69) If $v \in W$, then $a \cdot v \in v + W$.

(70) $u + v \in v + W$ iff $u \in W$.

(71) $v - u \in v + W$ iff $u \in W$.

(72) $u \in v + W$ iff there exists v_1 such that $v_1 \in W$ and $u = v + v_1$.

(73) $u \in v + W$ iff there exists v_1 such that $v_1 \in W$ and $u = v - v_1$.

(74) There exists v such that $v_1, v_2 \in v + W$ iff $v_1 - v_2 \in W$.

(75) If $v + W = u + W$, then there exists v_1 such that $v_1 \in W$ and $v + v_1 = u$.

(76) If $v + W = u + W$, then there exists v_1 such that $v_1 \in W$ and $v - v_1 = u$.

(77) For all strict submodules W_1, W_2 of V such that $v + W_1 = v + W_2$ holds $W_1 = W_2$.

(78) For all strict submodules W_1, W_2 of V such that $v + W_1 = u + W_2$ holds $W_1 = W_2$.

(79) C is linearly closed iff $C =$ the carrier of W.

(80) For all strict submodules W_1, W_2 of V and for every coset C_1 of W_1 and for every coset C_2 of W_2 such that $C_1 = C_2$ holds $W_1 = W_2$.

(81) $\{v\}$ is a coset of $\mathbf{0}_V$.

(82) If V_1 is a coset of $\mathbf{0}_V$, then there exists v such that $V_1 = \{v\}$.

(83) The carrier of W is a coset of W.

(84) The carrier of V is a coset of Ω_V.

(85) If V_1 is a coset of Ω_V, then $V_1 =$ the carrier of V.

(86) $0_V \in C$ iff $C =$ the carrier of W.

(87) $u \in C$ iff $C = u + W$.

(88) If $u, v \in C$, then there exists v_1 such that $v_1 \in W$ and $u + v_1 = v$.

(89) If $u, v \in C$, then there exists v_1 such that $v_1 \in W$ and $u - v_1 = v$.

(90) There exists C such that $v_1, v_2 \in C$ iff $v_1 - v_2 \in W$.

(91) If $u \in B$ and $u \in C$, then $B = C$.

3. Operations on Submodules in $\mathbb{Z}$-module

For simplicity, we use the following convention: V is a $\mathbb{Z}$-module, W, W_1, W_2, W_3 are submodules of V, u, u_1, u_2, v, v_1, v_2 are vectors of V, a, a_1, a_2 are integer numbers, and X, Y, y, y_1, y_2 are sets.

Let us consider V, W_1, W_2. The functor $W_1 + W_2$ yielding a strict submodule of V is defined by:

(Def. 14) The carrier of $W_1 + W_2 = \{v + u : v \in W_1 \ \wedge \ u \in W_2\}$.

Let us notice that the functor $W_1 + W_2$ is commutative.

Let us consider V, W_1, W_2. The functor $W_1 \cap W_2$ yields a strict submodule of V and is defined as follows:

(Def. 15) The carrier of $W_1 \cap W_2 =$ (the carrier of W_1) $\cap$ (the carrier of W_2).

Let us observe that the functor $W_1 \cap W_2$ is commutative.

We now state a number of propositions:

(92) $x \in W_1 + W_2$ iff there exist v_1, v_2 such that $v_1 \in W_1$ and $v_2 \in W_2$ and $x = v_1 + v_2$.

(93) If $v \in W_1$ or $v \in W_2$, then $v \in W_1 + W_2$.

(94) $x \in W_1 \cap W_2$ iff $x \in W_1$ and $x \in W_2$.

(95) For every strict submodule W of V holds $W + W = W$.

(96) $W_1 + (W_2 + W_3) = (W_1 + W_2) + W_3$.

(97) W_1 is a submodule of $W_1 + W_2$.

(98) For every strict submodule W_2 of V holds W_1 is a submodule of W_2 iff $W_1 + W_2 = W_2$.

(99) For every strict submodule W of V holds $\mathbf{0}_V + W = W$.

(100) $\mathbf{0}_V + \Omega_V =$ the $\mathbb{Z}$-module structure of V.

(101) $\Omega_V + W =$ the $\mathbb{Z}$-module structure of V.

(102) For every strict $\mathbb{Z}$-module V holds $\Omega_V + \Omega_V = V$.

(103) For every strict submodule W of V holds $W \cap W = W$.

(104) $W_1 \cap (W_2 \cap W_3) = (W_1 \cap W_2) \cap W_3$.

(105) $W_1 \cap W_2$ is a submodule of W_1.

(106) For every strict submodule W_1 of V holds W_1 is a submodule of W_2 iff $W_1 \cap W_2 = W_1$.

(107) $\mathbf{0}_V \cap W = \mathbf{0}_V$.

(108) $\mathbf{0}_V \cap \Omega_V = \mathbf{0}_V$.

(109) For every strict submodule W of V holds $\Omega_V \cap W = W$.

(110) For every strict $\mathbb{Z}$-module V holds $\Omega_V \cap \Omega_V = V$.

(111) $W_1 \cap W_2$ is a submodule of $W_1 + W_2$.

(112) For every strict submodule W_2 of V holds $W_1 \cap W_2 + W_2 = W_2$.

(113) For every strict submodule W_1 of V holds $W_1 \cap (W_1 + W_2) = W_1$.

(114) $W_1 \cap W_2 + W_2 \cap W_3$ is a submodule of $W_2 \cap (W_1 + W_3)$.

(115) If W_1 is a submodule of W_2, then $W_2 \cap (W_1 + W_3) = W_1 \cap W_2 + W_2 \cap W_3$.

(116) $W_2 + W_1 \cap W_3$ is a submodule of $(W_1 + W_2) \cap (W_2 + W_3)$.

(117) If W_1 is a submodule of W_2, then $W_2 + W_1 \cap W_3 = (W_1 + W_2) \cap (W_2 + W_3)$.

(118) If W_1 is a strict submodule of W_3, then $W_1 + W_2 \cap W_3 = (W_1 + W_2) \cap W_3$.

(119) For all strict submodules W_1, W_2 of V holds $W_1 + W_2 = W_2$ iff $W_1 \cap W_2 = W_1$.

(120) For all strict submodules W_2, W_3 of V such that W_1 is a submodule of W_2 holds $W_1 + W_3$ is a submodule of $W_2 + W_3$.

(121) There exists W such that the carrier of W = (the carrier of W_1) $\cup$ (the carrier of W_2) if and only if W_1 is a submodule of W_2 or W_2 is a submodule of W_1.

Let us consider V. The functor $\mathrm{Sub}(V)$ yields a set and is defined by:

(Def. 16) For every x holds $x \in \mathrm{Sub}(V)$ iff x is a strict submodule of V.

Let us consider V. One can verify that $\mathrm{Sub}(V)$ is non empty.

We now state the proposition

(122) For every strict $\mathbb{Z}$-module V holds $V \in \mathrm{Sub}(V)$.

Let us consider V, W_1, W_2. We say that V is the direct sum of W_1 and W_2 if and only if:

(Def. 17) The $\mathbb{Z}$-module structure of $V = W_1 + W_2$ and $W_1 \cap W_2 = \mathbf{0}_V$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. We say that W has linear complement if and only if:

(Def. 18) There exists a submodule C of V such that V is the direct sum of C and W.

Let V be a $\mathbb{Z}$-module. Observe that there exists a submodule of V which has linear complement.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. Let us assume that W has linear complement. A submodule of V is called a linear complement of W if:

(Def. 19) V is the direct sum of it and W.

One can prove the following propositions:

(123) Let V be a $\mathbb{Z}$-module and W_1, W_2 be submodules of V. Suppose V is the direct sum of W_1 and W_2. Then W_2 is a linear complement of W_1.

(124) Let V be a $\mathbb{Z}$-module, W be a submodule of V with linear complement, and L be a linear complement of W. Then V is the direct sum of L and W and the direct sum of W and L.

(125) Let V be a $\mathbb{Z}$-module, W be a submodule of V with linear complement, and L be a linear complement of W. Then $W+L =$ the $\mathbb{Z}$-module structure of V.

(126) Let V be a $\mathbb{Z}$-module, W be a submodule of V with linear complement, and L be a linear complement of W. Then $W \cap L = \mathbf{0}_V$.

(127) If V is the direct sum of W_1 and W_2, then V is the direct sum of W_2 and W_1.

(128) Let V be a $\mathbb{Z}$-module, W be a submodule of V with linear complement, and L be a linear complement of W. Then W is a linear complement of L.

(129) Every $\mathbb{Z}$-module V is the direct sum of $\mathbf{0}_V$ and Ω_V and the direct sum of Ω_V and $\mathbf{0}_V$.

(130) For every $\mathbb{Z}$-module V holds $\mathbf{0}_V$ is a linear complement of Ω_V and Ω_V is a linear complement of $\mathbf{0}_V$.

In the sequel C is a coset of W, C_1 is a coset of W_1, and C_2 is a coset of W_2. Next we state several propositions:

(131) If C_1 meets C_2, then $C_1 \cap C_2$ is a coset of $W_1 \cap W_2$.

(132) Let V be a $\mathbb{Z}$-module and W_1, W_2 be submodules of V. Then V is the direct sum of W_1 and W_2 if and only if for every coset C_1 of W_1 and for every coset C_2 of W_2 there exists a vector v of V such that $C_1 \cap C_2 = \{v\}$.

(133) Let V be a $\mathbb{Z}$-module and W_1, W_2 be submodules of V. Then $W_1 + W_2 =$ the $\mathbb{Z}$-module structure of V if and only if for every vector v of V there exist vectors v_1, v_2 of V such that $v_1 \in W_1$ and $v_2 \in W_2$ and $v = v_1 + v_2$.

(134) If V is the direct sum of W_1 and W_2 and $v_1 + v_2 = u_1 + u_2$ and v_1, $u_1 \in W_1$ and v_2, $u_2 \in W_2$, then $v_1 = u_1$ and $v_2 = u_2$.

(135) Suppose $V = W_1 + W_2$ and there exists v such that for all v_1, v_2, u_1, u_2 such that $v_1 + v_2 = u_1 + u_2$ and v_1, $u_1 \in W_1$ and v_2, $u_2 \in W_2$ holds $v_1 = u_1$ and $v_2 = u_2$. Then V is the direct sum of W_1 and W_2.

Let us consider V, v, W_1, W_2. Let us assume that V is the direct sum of W_1 and W_2. The functor $v_{\langle W_1, W_2 \rangle}$ yields an element of (the carrier of V) $\times$ (the carrier of V) and is defined as follows:

(Def. 20) $v = (v_{\langle W_1, W_2 \rangle})_{\mathbf{1}} + (v_{\langle W_1, W_2 \rangle})_{\mathbf{2}}$ and $(v_{\langle W_1, W_2 \rangle})_{\mathbf{1}} \in W_1$ and $(v_{\langle W_1, W_2 \rangle})_{\mathbf{2}} \in W_2$.

Next we state several propositions:

(136) If V is the direct sum of W_1 and W_2, then $(v_{\langle W_1, W_2 \rangle})_{\mathbf{1}} = (v_{\langle W_2, W_1 \rangle})_{\mathbf{2}}$.

(137) If V is the direct sum of W_1 and W_2, then $(v_{\langle W_1, W_2 \rangle})_{\mathbf{2}} = (v_{\langle W_2, W_1 \rangle})_{\mathbf{1}}$.

(138) Let V be a $\mathbb{Z}$-module, W be a submodule of V with linear complement, L be a linear complement of W, v be a vector of V, and t be an element

of (the carrier of V) $\times$ (the carrier of V). If $t_{\mathbf{1}} + t_{\mathbf{2}} = v$ and $t_{\mathbf{1}} \in W$ and $t_{\mathbf{2}} \in L$, then $t = v_{\langle W,L \rangle}$.

(139) Let V be a $\mathbb{Z}$-module, W be a submodule of V with linear complement, L be a linear complement of W, and v be a vector of V. Then $(v_{\langle W,L \rangle})_{\mathbf{1}} + (v_{\langle W,L \rangle})_{\mathbf{2}} = v$.

(140) Let V be a $\mathbb{Z}$-module, W be a submodule of V with linear complement, L be a linear complement of W, and v be a vector of V. Then $(v_{\langle W,L \rangle})_{\mathbf{1}} \in W$ and $(v_{\langle W,L \rangle})_{\mathbf{2}} \in L$.

(141) Let V be a $\mathbb{Z}$-module, W be a submodule of V with linear complement, L be a linear complement of W, and v be a vector of V. Then $(v_{\langle W,L \rangle})_{\mathbf{1}} = (v_{\langle L,W \rangle})_{\mathbf{2}}$.

(142) Let V be a $\mathbb{Z}$-module, W be a submodule of V with linear complement, L be a linear complement of W, and v be a vector of V. Then $(v_{\langle W,L \rangle})_{\mathbf{2}} = (v_{\langle L,W \rangle})_{\mathbf{1}}$.

In the sequel A_1, A_2, B are elements of $\mathrm{Sub}(V)$.

Let us consider V. The functor $\mathrm{SubJoin}\, V$ yielding a binary operation on $\mathrm{Sub}(V)$ is defined by:

(Def. 21) For all A_1, A_2, W_1, W_2 such that $A_1 = W_1$ and $A_2 = W_2$ holds $(\mathrm{SubJoin}\, V)(A_1, A_2) = W_1 + W_2$.

Let us consider V. The functor $\mathrm{SubMeet}\, V$ yields a binary operation on $\mathrm{Sub}(V)$ and is defined by:

(Def. 22) For all A_1, A_2, W_1, W_2 such that $A_1 = W_1$ and $A_2 = W_2$ holds $(\mathrm{SubMeet}\, V)(A_1, A_2) = W_1 \cap W_2$.

One can prove the following proposition

(143) $\langle \mathrm{Sub}(V), \mathrm{SubJoin}\, V, \mathrm{SubMeet}\, V \rangle$ is a lattice.

Let us consider V. Note that $\langle \mathrm{Sub}(V), \mathrm{SubJoin}\, V, \mathrm{SubMeet}\, V \rangle$ is lattice-like.

We now state several propositions:

(144) For every $\mathbb{Z}$-module V holds $\langle \mathrm{Sub}(V), \mathrm{SubJoin}\, V, \mathrm{SubMeet}\, V \rangle$ is lower-bounded.

(145) For every $\mathbb{Z}$-module V holds $\langle \mathrm{Sub}(V), \mathrm{SubJoin}\, V, \mathrm{SubMeet}\, V \rangle$ is upper-bounded.

(146) For every $\mathbb{Z}$-module V holds $\langle \mathrm{Sub}(V), \mathrm{SubJoin}\, V, \mathrm{SubMeet}\, V \rangle$ is a bound lattice.

(147) For every $\mathbb{Z}$-module V holds $\langle \mathrm{Sub}(V), \mathrm{SubJoin}\, V, \mathrm{SubMeet}\, V \rangle$ is modular.

(148) Let V be a $\mathbb{Z}$-module and W_1, W_2, W_3 be strict submodules of V. If W_1 is a submodule of W_2, then $W_1 \cap W_3$ is a submodule of $W_2 \cap W_3$.

(149) Let V be a $\mathbb{Z}$-module and W be a strict submodule of V. Suppose that for every vector v of V holds $v \in W$. Then $W =$ the $\mathbb{Z}$-module structure

of V.

(150) There exists C such that $v \in C$.

4. Transformation of Abelian Group to $\mathbb{Z}$-module

Let A_3 be a non empty additive loop structure. The left integer multiplication of A_3 yielding a function from $\mathbb{Z} \times$ the carrier of A_3 into the carrier of A_3 is defined by the condition (Def. 23).

(Def. 23) Let i be an element of $\mathbb{Z}$ and a be an element of A_3. Then

(i) if $i \geq 0$, then (the left integer multiplication of A_3)$(i, a) =$ (Nat-mult-left A_3)(i, a), and

(ii) if $i < 0$, then (the left integer multiplication of A_3)$(i, a) =$ (Nat-mult-left A_3)$(-i, -a)$.

The following propositions are true:

(151) Let R be a non empty additive loop structure, a be an element of R, i be an element of $\mathbb{Z}$, and i_1 be an element of $\mathbb{N}$. If $i = i_1$, then (the left integer multiplication of R)$(i, a) = i_1 \cdot a$.

(152) Let R be a non empty additive loop structure, a be an element of R, and i be an element of $\mathbb{Z}$. If $i = 0$, then (the left integer multiplication of R)$(i, a) = 0_R$.

(153) Let R be an add-associative right zeroed right complementable non empty additive loop structure and i be an element of $\mathbb{N}$. Then (Nat-mult-left R)$(i, 0_R) = 0_R$.

(154) Let R be an add-associative right zeroed right complementable non empty additive loop structure and i be an element of $\mathbb{Z}$. Then (the left integer multiplication of R)$(i, 0_R) = 0_R$.

(155) Let R be a right zeroed non empty additive loop structure, a be an element of R, and i be an element of $\mathbb{Z}$. If $i = 1$, then (the left integer multiplication of R)$(i, a) = a$.

(156) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R, and i, j, k be elements of $\mathbb{N}$. If $i \leq j$ and $k = j - i$, then (Nat-mult-left R)$(k, a) =$ (Nat-mult-left R)$(j, a) -$ (Nat-mult-left R)(i, a).

(157) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R, and i be an element of $\mathbb{N}$. Then $-$(Nat-mult-left R)$(i, a) =$ (Nat-mult-left R)$(i, -a)$.

(158) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R, and i, j be elements of $\mathbb{Z}$. Suppose $i \in \mathbb{N}$ and $j \notin \mathbb{N}$. Then (the left integer multipli-

cation of $R)(i + j, a) =$ (the left integer multiplication of $R)(i, a) +$ (the left integer multiplication of $R)(j, a)$.

(159) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R, and i, j be elements of $\mathbb{Z}$. Then (the left integer multiplication of $R)(i + j, a) =$ (the left integer multiplication of $R)(i, a) +$ (the left integer multiplication of $R)(j, a)$.

(160) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a, b be elements of R, and i be an element of $\mathbb{N}$. Then (Nat-mult-left $R)(i, a + b) =$ (Nat-mult-left $R)(i, a) +$ (Nat-mult-left $R)(i, b)$.

(161) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a, b be elements of R, and i be an element of $\mathbb{Z}$. Then (the left integer multiplication of $R)(i, a + b) =$ (the left integer multiplication of $R)(i, a) +$ (the left integer multiplication of $R)(i, b)$.

(162) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R, and i, j be elements of $\mathbb{N}$. Then (Nat-mult-left $R)(i \cdot j, a) =$ (Nat-mult-left $R)(i,$ (Nat-mult-left $R)(j, a))$.

(163) Let R be an Abelian right zeroed add-associative right complementable non empty additive loop structure, a be an element of R, and i, j be elements of $\mathbb{Z}$. Then (the left integer multiplication of $R)(i \cdot j, a) =$ (the left integer multiplication of $R)(i,$ (the left integer multiplication of $R)(j, a))$.

(164) Let A_3 be a non empty Abelian add-associative right zeroed right complementable additive loop structure. Then $\langle$the carrier of A_3, the zero of A_3, the addition of A_3, the left integer multiplication of $A_3\rangle$ is a $\mathbb{Z}$-module.

References

[1] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(**3**):537–541, 1990.

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

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

[4] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

[5] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.

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

[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] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: A cryptographic perspective (the international series in engineering and computer science). 2002.
[12] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.
[13] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[14] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[15] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[16] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[17] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[18] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[19] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

Received May 8, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 61–63, 2012
DOI: 10.2478/v10037-012-0008-y

VERSITA
versita.com/fm/

Morphology for Image Processing. Part I[1]

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Czesław Byliński
University of Białystok
Poland

Katsumi Wasaki
Shinshu University
Nagano, Japan

Summary. In this article we defined mathematical morphology image processing with set operations. First, we defined Minkowski set operations and proved their properties. Next, we defined basic image processing, dilation and erosion proving basic fact about them [5], [8].

MML identifier: MORPH_01, version: 7.12.02 4.170.1134

The terminology and notation used in this paper have been introduced in the following papers: [10], [7], [1], [2], [6], [9], [4], and [3].

1. Minkowski Set Operations

Let E be a non empty RLS structure. A binary image of E is a subset of E.

In the sequel E denotes a real linear space and A denotes a binary image of E.

Let E be a real linear space and let A, B be binary images of E. The functor $A \ominus B$ yielding a binary image of E is defined as follows:

(Def. 1) $A \ominus B = \{z \in E\colon \bigwedge_{b\,:\,\text{element of } E} (b \in B \Rightarrow z - b \in A)\}$.

Let a be a real number, let E be a real linear space, and let A be a subset of E. We introduce $a \cdot A$ as a synonym of $a \odot A$. The following propositions are true:

(1) Let E be a real linear space and A, B be subsets of E. If $B = \emptyset$, then $A \oplus B = B$ and $B \oplus A = B$ and $A \ominus B =$ the carrier of E.

(2) For every real linear space E and for all subsets A, B of E such that $A \neq \emptyset$ and $B = \emptyset$ holds $B \ominus A = B$.

[1]The authors wants to thank Prof. Yasunari Shidama for his kind support during the course of this work.

ISSN 1426–2630(p), 1898-9934(e)

(3) Let E be a real linear space and A, B be subsets of E. If $B =$ the carrier of E and $A \neq \emptyset$, then $A \oplus B = B$ and $B \oplus A = B$.

(4) For every real linear space E and for all subsets A, B of E such that $B =$ the carrier of E holds $B \ominus A = B$.

(5) $A \oplus B = \bigcup\{b + A; b \text{ ranges over elements of } E\colon b \in B\}$.

Let E be a non empty RLS structure. A binary image family of E is a family of subsets of the carrier of E.

We follow the rules: F, G are binary image families of E and A, B, C are non empty binary images of E. We now state four propositions:

(6) $A \ominus B = \bigcap\{b + A; b \text{ ranges over elements of } E\colon b \in B\}$.

(7) $A \oplus B = \{v \in E\colon (v + (-1) \cdot B) \cap A \neq \emptyset\}$.

(8) $A \ominus B = \{v \in E\colon v + (-1) \cdot B \subseteq A\}$.

(9) ((The carrier of E) $\setminus A) \oplus B =$ (the carrier of E) $\setminus A \ominus B$ and ((the carrier of E) $\setminus A) \ominus B =$ (the carrier of E) $\setminus A \oplus B$.

Let E be a non empty Abelian additive loop structure and let A, B be subsets of E. Let us note that the functor $A \oplus B$ is commutative.

One can prove the following propositions:

(10) For every non empty add-associative additive loop structure E and for all subsets A, B, C of E holds $(A + B) + C = A + (B + C)$.

(11) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.

(12) $\bigcup F \oplus B = \bigcup\{X \oplus B; X \text{ ranges over binary images of } E\colon X \in F\}$.

(13) $A \oplus \bigcup F = \bigcup\{A \oplus X; X \text{ ranges over binary images of } E\colon X \in F\}$.

(14) $\bigcap F \oplus B \subseteq \bigcap\{X \oplus B; X \text{ ranges over binary images of } E\colon X \in F\}$.

(15) $A \oplus \bigcap F \subseteq \bigcap\{A \oplus X; X \text{ ranges over binary images of } E\colon X \in F\}$.

(16) For every non empty additive loop structure E and for all subsets A, B, C of E such that $B \subseteq C$ holds $A + B \subseteq A + C$.

(17) $(v + A) \oplus B = A \oplus (v + B)$ and $(v + A) \oplus B = v + A \oplus B$.

(18) $\bigcap F \ominus B = \bigcap\{X \ominus B; X \text{ ranges over binary images of } E\colon X \in F\}$.

(19) $\bigcap\{B \ominus X; X \text{ ranges over binary images of } E\colon X \in F\} \subseteq B \ominus \bigcap F$.

(20) $\bigcup\{X \ominus B; X \text{ ranges over binary images of } E\colon X \in F\} \subseteq \bigcup F \ominus B$.

(21) If $F \neq \emptyset$, then $B \ominus \bigcup F = \bigcap\{B \ominus X; X \text{ ranges over binary images of } E\colon X \in F\}$.

(22) If $A \subseteq B$, then $A \ominus C \subseteq B \ominus C$.

(23) If $A \subseteq B$, then $C \ominus B \subseteq C \ominus A$.

(24) $(v + A) \ominus B = A \ominus (v + B)$ and $(v + A) \ominus B = v + A \ominus B$.

(25) $A \ominus B \ominus C = A \ominus (B \oplus C)$.

2. Dilation and Erosion

Let E be a real linear space and let B be a binary image of E. The functor dilation B yields a function from $2^{\text{the carrier of } E}$ into $2^{\text{the carrier of } E}$ and is defined as follows:

(Def. 2) For every binary image A of E holds $(\text{dilation}\, B)(A) = A \oplus B$.

Let E be a real linear space and let B be a binary image of E. The functor erosion B yields a function from $2^{\text{the carrier of } E}$ into $2^{\text{the carrier of } E}$ and is defined by:

(Def. 3) For every binary image A of E holds $(\text{erosion}\, B)(A) = A \ominus B$.

The following propositions are true:

(26) $(\text{dilation}\, B)(\bigcup F) = \bigcup\{(\text{dilation}\, B)(X); X \text{ ranges over binary images of } E\colon X \in F\}$.

(27) If $A \subseteq B$, then $(\text{dilation}\, C)(A) \subseteq (\text{dilation}\, C)(B)$.

(28) $(\text{dilation}\, C)(v + A) = v + (\text{dilation}\, C)(A)$.

(29) $(\text{erosion}\, B)(\bigcap F) = \bigcap\{(\text{erosion}\, B)(X); X \text{ ranges over binary images of } E\colon X \in F\}$.

(30) If $A \subseteq B$, then $(\text{erosion}\, C)(A) \subseteq (\text{erosion}\, C)(B)$.

(31) $(\text{erosion}\, C)(v + A) = v + (\text{erosion}\, C)(A)$.

(32) $(\text{dilation}\, C)((\text{the carrier of } E) \setminus A) = (\text{the carrier of } E) \setminus (\text{erosion}\, C)(A)$ and $(\text{erosion}\, C)((\text{the carrier of } E) \setminus A) = (\text{the carrier of } E) \setminus (\text{dilation}\, C)(A)$.

(33) $(\text{dilation}\, C)((\text{dilation}\, B)(A)) = (\text{dilation}(\text{dilation}\, C)(B))(A)$ and $(\text{erosion}\, C)((\text{erosion}\, B)(A)) = (\text{erosion}(\text{dilation}\, C)(B))(A)$.

References

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

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

[3] Yuzhong Ding and Xiquan Liang. Preliminaries to mathematical morphology and its properties. *Formalized Mathematics*, 13(**2**):221–225, 2005.

[4] Noboru Endou, Takashi Mitsuishi, and Yasunari Shidama. Dimension of real unitary space. *Formalized Mathematics*, 11(**1**):23–28, 2003.

[5] H.J.A.M. Heijimans. *Morphological Image Operators*. Academic Press, 1994.

[6] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[7] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[8] P. Soille. *Morphological Image Analysis: Principles and Applications*. Springer, 2003.

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

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

Received September 21, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 65–71, 2012
DOI: 10.2478/v10037-012-0009-x

VERSITA
versita.com/fm/

The Differentiable Functions from $\mathbb{R}$ into $\mathcal{R}^n$

Keiko Narita
Hirosaki-city
Aomori, Japan

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

Yasunari Shidama[1]
Shinshu University
Nagano, Japan

Summary. In control engineering, differentiable partial functions from $\mathbb{R}$ into $\mathcal{R}^n$ play a very important role. In this article, we formalized basic properties of such functions.

MML identifier: NDIFF_4, version: 7.12.02 4.171.1135

The notation and terminology used in this paper are introduced in the following articles: [25], [26], [6], [2], [27], [8], [7], [24], [1], [4], [3], [5], [9], [22], [20], [28], [21], [10], [23], [17], [13], [11], [12], [15], [19], [18], [16], and [14].

Let us observe that there exists a sequence of real numbers which is convergent to 0 and non-zero.

For simplicity, we adopt the following convention: x_0, r denote real numbers, i, m denote elements of $\mathbb{N}$, n denotes a non empty element of $\mathbb{N}$, Y denotes a subset of $\mathbb{R}$, Z denotes an open subset of $\mathbb{R}$, and f_1, f_2 denote partial functions from $\mathbb{R}$ to $\mathcal{R}^n$.

The following proposition is true

(1) For all partial functions f_1, f_2 from $\mathbb{R}$ to $\mathcal{R}^m$ holds $f_1 - f_2 = f_1 + -f_2$.

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

ISSN 1426–2630(p), 1898-9934(e)

Let n be a non empty element of $\mathbb{N}$, let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, and let x be a real number. We say that f is differentiable in x if and only if:

(Def. 1) There exists a partial function g from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ such that $f = g$ and g is differentiable in x.

One can prove the following proposition

(2) Let n be a non empty element of $\mathbb{N}$, f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, h be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, and x be a real number. Suppose $h = f$. Then f is differentiable in x if and only if h is differentiable in x.

Let n be a non empty element of $\mathbb{N}$, let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, and let x be a real number. The functor $f'(x)$ yields an element of $\mathcal{R}^n$ and is defined as follows:

(Def. 2) There exists a partial function g from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ such that $f = g$ and $f'(x) = g'(x)$.

One can prove the following proposition

(3) Let n be a non empty element of $\mathbb{N}$, f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, h be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, and x be a real number. If $h = f$, then $f'(x) = h'(x)$.

Let us consider n, f, X. We say that f is differentiable on X if and only if:

(Def. 3) $X \subseteq \operatorname{dom} f$ and for every x such that $x \in X$ holds $f \upharpoonright X$ is differentiable in x.

The following propositions are true:

(4) If f is differentiable on X, then X is a subset of $\mathbb{R}$.

(5) f is differentiable on Z iff $Z \subseteq \operatorname{dom} f$ and for every x such that $x \in Z$ holds f is differentiable in x.

(6) If f is differentiable on Y, then Y is open.

Let us consider n, f, X. Let us assume that f is differentiable on X. The functor $f'_{\upharpoonright X}$ yields a partial function from $\mathbb{R}$ to $\mathcal{R}^n$ and is defined by:

(Def. 4) $\operatorname{dom}(f'_{\upharpoonright X}) = X$ and for every x such that $x \in X$ holds $f'_{\upharpoonright X}(x) = f'(x)$.

One can prove the following propositions:

(7) Suppose $Z \subseteq \operatorname{dom} f$ and there exists an element r of $\mathcal{R}^n$ such that $\operatorname{rng} f = \{r\}$. Then f is differentiable on Z and for every x such that $x \in Z$ holds $(f'_{\upharpoonright Z})_x = \langle \underbrace{0, \ldots, 0}_{n} \rangle$.

(8) Let x_0 be a real number, f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, and N be a neighbourhood of x_0. Suppose $f = g$ and f is differentiable in x_0 and $N \subseteq \operatorname{dom} f$. Let given h, c.

Suppose $\operatorname{rng} c = \{x_0\}$ and $\operatorname{rng}(h+c) \subseteq N$. Then $h^{-1} \cdot ((g_*(h+c)) - (g_*c))$ is convergent and $f'(x_0) = \lim(h^{-1} \cdot ((g_*(h+c)) - (g_*c)))$.

(9) If f is differentiable in x_0, then $r \cdot f$ is differentiable in x_0 and $(r \cdot f)'(x_0) = r \cdot f'(x_0)$.

(10) If f is differentiable in x_0, then $-f$ is differentiable in x_0 and $(-f)'(x_0) = -f'(x_0)$.

(11) If f_1 is differentiable in x_0 and f_2 is differentiable in x_0, then $f_1 + f_2$ is differentiable in x_0 and $(f_1 + f_2)'(x_0) = {f_1}'(x_0) + {f_2}'(x_0)$.

(12) If f_1 is differentiable in x_0 and f_2 is differentiable in x_0, then $f_1 - f_2$ is differentiable in x_0 and $(f_1 - f_2)'(x_0) = {f_1}'(x_0) - {f_2}'(x_0)$.

(13) Suppose $Z \subseteq \operatorname{dom} f$ and f is differentiable on Z. Then $r \cdot f$ is differentiable on Z and for every x such that $x \in Z$ holds $(r \cdot f)'_{\restriction Z}(x) = r \cdot f'(x)$.

(14) If $Z \subseteq \operatorname{dom} f$ and f is differentiable on Z, then $-f$ is differentiable on Z and for every x such that $x \in Z$ holds $(-f)'_{\restriction Z}(x) = -f'(x)$.

(15) Suppose $Z \subseteq \operatorname{dom}(f_1 + f_2)$ and f_1 is differentiable on Z and f_2 is differentiable on Z. Then $f_1 + f_2$ is differentiable on Z and for every x such that $x \in Z$ holds $(f_1 + f_2)'_{\restriction Z}(x) = {f_1}'(x) + {f_2}'(x)$.

(16) Suppose $Z \subseteq \operatorname{dom}(f_1 - f_2)$ and f_1 is differentiable on Z and f_2 is differentiable on Z. Then $f_1 - f_2$ is differentiable on Z and for every x such that $x \in Z$ holds $(f_1 - f_2)'_{\restriction Z}(x) = {f_1}'(x) - {f_2}'(x)$.

(17) If $Z \subseteq \operatorname{dom} f$ and $f \restriction Z$ is constant, then f is differentiable on Z and for every x such that $x \in Z$ holds $f'_{\restriction Z}(x) = \langle \underbrace{0, \ldots, 0}_{n} \rangle$.

(18) Let r, p be elements of $\mathcal{R}^n$. Suppose $Z \subseteq \operatorname{dom} f$ and for every x such that $x \in Z$ holds $f_x = x \cdot r + p$. Then f is differentiable on Z and for every x such that $x \in Z$ holds $f'_{\restriction Z}(x) = r$.

(19) For every real number x_0 such that f is differentiable in x_0 holds f is continuous in x_0.

(20) If f is differentiable on X, then $f \restriction X$ is continuous.

(21) If f is differentiable on X and $Z \subseteq X$, then f is differentiable on Z.

Let n be a non empty element of $\mathbb{N}$ and let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. We say that f is differentiable if and only if:

(Def. 5) f is differentiable on $\operatorname{dom} f$.

Let us consider n. One can check that $\mathbb{R} \longmapsto \langle \underbrace{0, \ldots, 0}_{n} \rangle$ is differentiable.

Let us consider n. Note that there exists a function from $\mathbb{R}$ into $\mathcal{R}^n$ which is differentiable.

One can prove the following proposition

(22) For every differentiable partial function f from $\mathbb{R}$ to $\mathcal{R}^n$ such that $Z \subseteq \operatorname{dom} f$ holds f is differentiable on Z.

In the sequel G_1, R are rests of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and D_1, L are linears of $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Next we state a number of propositions:

(23) Let R be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose R is total. Then R is rest-like if and only if for every real number r such that $r > 0$ there exists a real number d such that $d > 0$ and for every real number z such that $z \neq 0$ and $|z| < d$ holds $|z|^{-1} \cdot \|R_z\| < r$.

(24) Let g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and x_0 be a real number. Suppose $1 \leq i \leq n$ and g is differentiable in x_0. Then $\mathrm{Proj}(i,n) \cdot g$ is differentiable in x_0 and $(\mathrm{Proj}(i,n))(g'(x_0)) = (\mathrm{Proj}(i,n) \cdot g)'(x_0)$.

(25) Let g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and x_0 be a real number. Then g is differentiable in x_0 if and only if for every element i of $\mathbb{N}$ such that $1 \leq i \leq n$ holds $\mathrm{Proj}(i,n) \cdot g$ is differentiable in x_0.

(26) Let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$ and x_0 be a real number. Suppose $1 \leq i \leq n$ and f is differentiable in x_0. Then $\mathrm{Proj}(i,n) \cdot f$ is differentiable in x_0 and $(\mathrm{Proj}(i,n))(f'(x_0)) = (\mathrm{Proj}(i,n) \cdot f)'(x_0)$.

(27) Let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$ and x_0 be a real number. Then f is differentiable in x_0 if and only if for every element i of $\mathbb{N}$ such that $1 \leq i \leq n$ holds $\mathrm{Proj}(i,n) \cdot f$ is differentiable in x_0.

(28) Let g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $1 \leq i \leq n$ and g is differentiable on X. Then $\mathrm{Proj}(i,n) \cdot g$ is differentiable on X and $\mathrm{Proj}(i,n) \cdot g'_{\restriction X} = (\mathrm{Proj}(i,n) \cdot g)'_{\restriction X}$.

(29) Let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. Suppose $1 \leq i \leq n$ and f is differentiable on X. Then $\mathrm{Proj}(i,n) \cdot f$ is differentiable on X and $\mathrm{Proj}(i,n) \cdot f'_{\restriction X} = (\mathrm{Proj}(i,n) \cdot f)'_{\restriction X}$.

(30) Let g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Then g is differentiable on X if and only if for every element i of $\mathbb{N}$ such that $1 \leq i \leq n$ holds $\mathrm{Proj}(i,n) \cdot g$ is differentiable on X.

(31) Let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. Then f is differentiable on X if and only if for every element i of $\mathbb{N}$ such that $1 \leq i \leq n$ holds $\mathrm{Proj}(i,n) \cdot f$ is differentiable on X.

(32) For every function J from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ into $\mathbb{R}$ and for every point x_0 of $\langle \mathcal{E}^1, \|\cdot\| \rangle$ such that $J = \mathrm{proj}(1,1)$ holds J is continuous in x_0.

(33) For every function I from $\mathbb{R}$ into $\langle \mathcal{E}^1, \|\cdot\| \rangle$ such that $I = \mathrm{proj}(1,1)^{-1}$ holds I is continuous in x_0.

(34) Let S, T be real normed spaces, f_1 be a partial function from S to $\mathbb{R}$, f_2 be a partial function from $\mathbb{R}$ to T, and x_0 be a point of S. Suppose $x_0 \in \mathrm{dom}(f_2 \cdot f_1)$ and f_1 is continuous in x_0 and f_2 is continuous in $(f_1)_{x_0}$. Then $f_2 \cdot f_1$ is continuous in x_0.

(35) Let J be a function from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ into $\mathbb{R}$, x_0 be a point of $\langle \mathcal{E}^1, \|\cdot\| \rangle$, y_0 be an element of $\mathbb{R}$, g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, and f

be a partial function from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $J = \mathrm{proj}(1,1)$ and $x_0 \in \mathrm{dom}\, f$ and $y_0 \in \mathrm{dom}\, g$ and $x_0 = \langle y_0 \rangle$ and $f = g \cdot J$. Then f is continuous in x_0 if and only if g is continuous in y_0.

(36) Let I be a function from $\mathbb{R}$ into $\langle \mathcal{E}^1, \|\cdot\| \rangle$, x_0 be a point of $\langle \mathcal{E}^1, \|\cdot\| \rangle$, y_0 be an element of $\mathbb{R}$, g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, and f be a partial function from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $I = \mathrm{proj}(1,1)^{-1}$ and $x_0 \in \mathrm{dom}\, f$ and $y_0 \in \mathrm{dom}\, g$ and $x_0 = \langle y_0 \rangle$ and $f \cdot I = g$. Then f is continuous in x_0 if and only if g is continuous in y_0.

(37) For every function I from $\mathbb{R}$ into $\langle \mathcal{E}^1, \|\cdot\| \rangle$ such that $I = \mathrm{proj}(1,1)^{-1}$ holds I is differentiable in x_0 and $I'(x_0) = \langle 1 \rangle$.

Let n be a non empty element of $\mathbb{N}$, let f be a partial function from $\langle \mathcal{E}^n, \|\cdot\| \rangle$ to $\mathbb{R}$, and let x be a point of $\langle \mathcal{E}^n, \|\cdot\| \rangle$. We say that f is differentiable in x if and only if the condition (Def. 6) is satisfied.

(Def. 6) There exists a partial function g from $\mathcal{R}^n$ to $\mathbb{R}$ and there exists an element y of $\mathcal{R}^n$ such that $f = g$ and $x = y$ and g is differentiable in y.

Let n be a non empty element of $\mathbb{N}$, let f be a partial function from $\langle \mathcal{E}^n, \|\cdot\| \rangle$ to $\mathbb{R}$, and let x be a point of $\langle \mathcal{E}^n, \|\cdot\| \rangle$. The functor $f'(x)$ yields a function from $\langle \mathcal{E}^n, \|\cdot\| \rangle$ into $\mathbb{R}$ and is defined by:

(Def. 7) There exists a partial function g from $\mathcal{R}^n$ to $\mathbb{R}$ and there exists an element y of $\mathcal{R}^n$ such that $f = g$ and $x = y$ and $f'(x) = g'(y)$.

We now state several propositions:

(38) Let J be a function from $\mathcal{R}^1$ into $\mathbb{R}$ and x_0 be an element of $\mathcal{R}^1$. If $J = \mathrm{proj}(1,1)$, then J is differentiable in x_0 and $J'(x_0) = J$.

(39) Let J be a function from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ into $\mathbb{R}$ and x_0 be a point of $\langle \mathcal{E}^1, \|\cdot\| \rangle$. If $J = \mathrm{proj}(1,1)$, then J is differentiable in x_0 and $J'(x_0) = J$.

(40) Let I be a function from $\mathbb{R}$ into $\langle \mathcal{E}^1, \|\cdot\| \rangle$. Suppose $I = \mathrm{proj}(1,1)^{-1}$. Then

(i) for every rest R of $\langle \mathcal{E}^1, \|\cdot\| \rangle$, $\langle \mathcal{E}^n, \|\cdot\| \rangle$ holds $R \cdot I$ is a rest of $\langle \mathcal{E}^n, \|\cdot\| \rangle$, and

(ii) for every linear operator L from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ into $\langle \mathcal{E}^n, \|\cdot\| \rangle$ holds $L \cdot I$ is a linear of $\langle \mathcal{E}^n, \|\cdot\| \rangle$.

(41) Let J be a function from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ into $\mathbb{R}$. Suppose $J = \mathrm{proj}(1,1)$. Then

(i) for every rest R of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ holds $R \cdot J$ is a rest of $\langle \mathcal{E}^1, \|\cdot\| \rangle$, $\langle \mathcal{E}^n, \|\cdot\| \rangle$, and

(ii) for every linear L of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ holds $L \cdot J$ is a bounded linear operator from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ into $\langle \mathcal{E}^n, \|\cdot\| \rangle$.

(42) Let I be a function from $\mathbb{R}$ into $\langle \mathcal{E}^1, \|\cdot\| \rangle$, x_0 be a point of $\langle \mathcal{E}^1, \|\cdot\| \rangle$, y_0 be an element of $\mathbb{R}$, g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, and f be a partial function from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $I = \mathrm{proj}(1,1)^{-1}$ and $x_0 \in \mathrm{dom}\, f$ and $y_0 \in \mathrm{dom}\, g$ and $x_0 = \langle y_0 \rangle$ and $f \cdot I = g$ and f is

differentiable in x_0. Then g is differentiable in y_0 and $g'(y_0) = f'(x_0)(\langle 1\rangle)$ and for every element r of $\mathbb{R}$ holds $f'(x_0)(\langle r\rangle) = r \cdot g'(y_0)$.

(43) Let I be a function from $\mathbb{R}$ into $\langle \mathcal{E}^1, \|\cdot\|\rangle$, x_0 be a point of $\langle \mathcal{E}^1, \|\cdot\|\rangle$, y_0 be an element of $\mathbb{R}$, g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\|\rangle$, and f be a partial function from $\langle \mathcal{E}^1, \|\cdot\|\rangle$ to $\langle \mathcal{E}^n, \|\cdot\|\rangle$. Suppose $I = \mathrm{proj}(1,1)^{-1}$ and $x_0 \in \mathrm{dom}\, f$ and $y_0 \in \mathrm{dom}\, g$ and $x_0 = \langle y_0\rangle$ and $f \cdot I = g$. Then f is differentiable in x_0 if and only if g is differentiable in y_0.

(44) Let J be a function from $\langle \mathcal{E}^1, \|\cdot\|\rangle$ into $\mathbb{R}$, x_0 be a point of $\langle \mathcal{E}^1, \|\cdot\|\rangle$, y_0 be an element of $\mathbb{R}$, g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\|\rangle$, and f be a partial function from $\langle \mathcal{E}^1, \|\cdot\|\rangle$ to $\langle \mathcal{E}^n, \|\cdot\|\rangle$. Suppose $J = \mathrm{proj}(1,1)$ and $x_0 \in \mathrm{dom}\, f$ and $y_0 \in \mathrm{dom}\, g$ and $x_0 = \langle y_0\rangle$ and $f = g \cdot J$. Then f is differentiable in x_0 if and only if g is differentiable in y_0.

(45) Let J be a function from $\langle \mathcal{E}^1, \|\cdot\|\rangle$ into $\mathbb{R}$, x_0 be a point of $\langle \mathcal{E}^1, \|\cdot\|\rangle$, y_0 be an element of $\mathbb{R}$, g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\|\rangle$, and f be a partial function from $\langle \mathcal{E}^1, \|\cdot\|\rangle$ to $\langle \mathcal{E}^n, \|\cdot\|\rangle$. Suppose $J = \mathrm{proj}(1,1)$ and $x_0 \in \mathrm{dom}\, f$ and $y_0 \in \mathrm{dom}\, g$ and $x_0 = \langle y_0\rangle$ and $f = g \cdot J$ and g is differentiable in y_0. Then f is differentiable in x_0 and $g'(y_0) = f'(x_0)(\langle 1\rangle)$ and for every element r of $\mathbb{R}$ holds $f'(x_0)(\langle r\rangle) = r \cdot g'(y_0)$.

(46) Let R be a rest of $\langle \mathcal{E}^n, \|\cdot\|\rangle$. Suppose $R_0 = 0_{\langle \mathcal{E}^n, \|\cdot\|\rangle}$. Let e be a real number. Suppose $e > 0$. Then there exists a real number d such that $d > 0$ and for every real number h such that $|h| < d$ holds $\|R_h\| \leq e \cdot |h|$.

In the sequel m, n denote non empty elements of $\mathbb{N}$.

One can prove the following propositions:

(47) For every rest R of $\langle \mathcal{E}^n, \|\cdot\|\rangle$ and for every bounded linear operator L from $\langle \mathcal{E}^n, \|\cdot\|\rangle$ into $\langle \mathcal{E}^m, \|\cdot\|\rangle$ holds $L \cdot R$ is a rest of $\langle \mathcal{E}^m, \|\cdot\|\rangle$.

(48) Let R_1 be a rest of $\langle \mathcal{E}^n, \|\cdot\|\rangle$. Suppose $(R_1)_0 = 0_{\langle \mathcal{E}^n, \|\cdot\|\rangle}$. Let R_2 be a rest of $\langle \mathcal{E}^n, \|\cdot\|\rangle$, $\langle \mathcal{E}^m, \|\cdot\|\rangle$. Suppose $(R_2)_{0_{\langle \mathcal{E}^n, \|\cdot\|\rangle}} = 0_{\langle \mathcal{E}^m, \|\cdot\|\rangle}$. Let L be a linear of $\langle \mathcal{E}^n, \|\cdot\|\rangle$. Then $R_2 \cdot (L + R_1)$ is a rest of $\langle \mathcal{E}^m, \|\cdot\|\rangle$.

(49) Let R_1 be a rest of $\langle \mathcal{E}^n, \|\cdot\|\rangle$. Suppose $(R_1)_0 = 0_{\langle \mathcal{E}^n, \|\cdot\|\rangle}$. Let R_2 be a rest of $\langle \mathcal{E}^n, \|\cdot\|\rangle$, $\langle \mathcal{E}^m, \|\cdot\|\rangle$. Suppose $(R_2)_{0_{\langle \mathcal{E}^n, \|\cdot\|\rangle}} = 0_{\langle \mathcal{E}^m, \|\cdot\|\rangle}$. Let L_1 be a linear of $\langle \mathcal{E}^n, \|\cdot\|\rangle$ and L_2 be a bounded linear operator from $\langle \mathcal{E}^n, \|\cdot\|\rangle$ into $\langle \mathcal{E}^m, \|\cdot\|\rangle$. Then $L_2 \cdot R_1 + R_2 \cdot (L_1 + R_1)$ is a rest of $\langle \mathcal{E}^m, \|\cdot\|\rangle$.

(50) Let x_0 be an element of $\mathbb{R}$ and g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\|\rangle$. Suppose g is differentiable in x_0. Let f be a partial function from $\langle \mathcal{E}^n, \|\cdot\|\rangle$ to $\langle \mathcal{E}^m, \|\cdot\|\rangle$. Suppose f is differentiable in g_{x_0}. Then $f \cdot g$ is differentiable in x_0 and $(f \cdot g)'(x_0) = f'(g_{x_0})(g'(x_0))$.

References

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

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

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 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] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[11] Noboru Endou and Yasunari Shidama. Completeness of the real Euclidean space. *Formalized Mathematics*, 13(**4**):577–580, 2005.
[12] Noboru Endou, Yasunari Shidama, and Keiichi Miyajima. Partial differentiation on normed linear spaces $\mathcal{R}^n$. *Formalized Mathematics*, 15(**2**):65–72, 2007, doi:10.2478/v10037-007-0008-5.
[13] Hiroshi Imura, Morishige Kimura, and Yasunari Shidama. The differentiable functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):321–327, 2004.
[14] Takao Inoué, Adam Naumowicz, Noboru Endou, and Yasunari Shidama. Partial differentiation of vector-valued functions on n-dimensional real normed linear spaces. *Formalized Mathematics*, 19(**1**):1–9, 2011, doi: 10.2478/v10037-011-0001-x.
[15] Keiichi Miyajima and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into $\mathcal{R}^n$. *Formalized Mathematics*, 17(**2**):179–185, 2009, doi: 10.2478/v10037-009-0021-y.
[16] Keiko Narita, Artur Kornilowicz, and Yasunari Shidama. More on the continuity of real functions. *Formalized Mathematics*, 19(**4**):233–239, 2011, doi: 10.2478/v10037-011-0032-3.
[17] Takaya Nishiyama, Keiji Ohkubo, and Yasunari Shidama. The continuous functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):269–275, 2004.
[18] Hiroyuki Okazaki, Noboru Endou, Keiko Narita, and Yasunari Shidama. Differentiable functions into real normed spaces. *Formalized Mathematics*, 19(**2**):69–72, 2011, doi: 10.2478/v10037-011-0012-7.
[19] 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.
[20] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[21] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[22] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[23] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.
[24] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[25] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[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.
[28] Hiroshi Yamazaki and Yasunari Shidama. Algebra of vector functions. *Formalized Mathematics*, 3(**2**):171–175, 1992.

Received September 28, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 73–77, 2012
DOI: 10.2478/v10037-012-0010-4

VERSITA
versita.com/fm/

Some Basic Properties of Some Special Matrices. Part III[1]

Xiquan Liang
Qingdao University of Science and Technology
China

Tao Wang
Qingdao University of Science and Technology
China

Summary. This article describes definitions of subsymmetric matrix, anti-subsymmetric matrix, central symmetric matrix, symmetry circulant matrix and their basic properties.

MML identifier: MATRIX17, version: 7.12.02 4.174.1136

The notation and terminology used here have been introduced in the following papers: [7], [9], [13], [6], [14], [1], [3], [18], [17], [4], [2], [8], [11], [12], [16], [15], [5], and [10].

1. Basic Properties of Subordinate Symmetric Matrices

For simplicity, we use the following convention: n denotes a natural number, K denotes a field, a, b denote elements of K, p, q denote finite sequences of elements of K, and M_1, M_2 denote square matrices over K of dimension n.

Let K be a field, let n be a natural number, and let M be a square matrix over K of dimension n. We say that M is subsymmetric if and only if:

(Def. 1) For all natural numbers i, j, k, l such that $\langle i, j\rangle \in$ the indices of M and $k = (n+1) - j$ and $l = (n+1) - i$ holds $M_{i,j} = M_{k,l}$.

Let us consider n, K, a. Note that $(a)^{n\times n}$ is subsymmetric.

Let us consider n, K. Observe that there exists a square matrix over K of dimension n which is subsymmetric.

[1] Authors thanks Andrzej Trybulec and Yatsuka Nakamura for the help during writing this article.

ISSN 1426–2630(p), 1898-9934(e)

Let us consider n, K and let M be a subsymmetric square matrix over K of dimension n. Note that $-M$ is subsymmetric.

Let us consider n, K and let M_1, M_2 be subsymmetric square matrices over K of dimension n. One can check that $M_1 + M_2$ is subsymmetric.

Let us consider n, K, a and let M be a subsymmetric square matrix over K of dimension n. Note that $a \cdot M$ is subsymmetric.

Let us consider n, K and let M_1, M_2 be subsymmetric square matrices over K of dimension n. One can verify that $M_1 - M_2$ is subsymmetric.

Let us consider n, K and let M be a subsymmetric square matrix over K of dimension n. Observe that M^{T} is subsymmetric.

Let us consider n, K. Observe that every square matrix over K of dimension n which is line circulant is also subsymmetric and every square matrix over K of dimension n which is column circulant is also subsymmetric.

Let K be a field, let n be a natural number, and let M be a square matrix over K of dimension n. We say that M is anti-subsymmetric if and only if:

(Def. 2) For all natural numbers i, j, k, l such that $\langle i, j \rangle \in$ the indices of M and $k = (n+1) - j$ and $l = (n+1) - i$ holds $M_{i,j} = -M_{k,l}$.

Let us consider n, K. One can verify that there exists a square matrix over K of dimension n which is anti-subsymmetric.

The following proposition is true

(1) Let K be a Fanoian field, n, i, j, k, l be natural numbers, and M_1 be a square matrix over K of dimension n. Suppose $\langle i, j \rangle \in$ the indices of M_1 and $i + j = n + 1$ and $k = (n+1) - j$ and $l = (n+1) - i$ and M_1 is anti-subsymmetric. Then $(M_1)_{i,j} = 0_K$.

Let us consider n, K and let M be an anti-subsymmetric square matrix over K of dimension n. Note that $-M$ is anti-subsymmetric.

Let us consider n, K and let M_1, M_2 be anti-subsymmetric square matrices over K of dimension n. Observe that $M_1 + M_2$ is anti-subsymmetric.

Let us consider n, K, a and let M be an anti-subsymmetric square matrix over K of dimension n. One can verify that $a \cdot M$ is anti-subsymmetric.

Let us consider n, K and let M_1, M_2 be anti-subsymmetric square matrices over K of dimension n. One can check that $M_1 - M_2$ is anti-subsymmetric.

Let us consider n, K and let M be an anti-subsymmetric square matrix over K of dimension n. One can verify that M^{T} is anti-subsymmetric.

2. Basic Properties of Central Symmetric Matrices

Let K be a field, let n be a natural number, and let M be a square matrix over K of dimension n. We say that M is central symmetric if and only if:

(Def. 3) For all natural numbers i, j, k, l such that $\langle i, j \rangle \in$ the indices of M and $k = (n+1) - i$ and $l = (n+1) - j$ holds $M_{i,j} = M_{k,l}$.

Let us consider n, K, a. Note that $(a)^{n\times n}$ is central symmetric.

Let us consider n, K. One can verify that there exists a square matrix over K of dimension n which is central symmetric.

Let us consider n, K and let M be a central symmetric square matrix over K of dimension n. One can verify that $-M$ is central symmetric.

Let us consider n, K and let M_1, M_2 be central symmetric square matrices over K of dimension n. One can verify that $M_1 + M_2$ is central symmetric.

Let us consider n, K, a and let M be a central symmetric square matrix over K of dimension n. Note that $a \cdot M$ is central symmetric.

Let us consider n, K and let M_1, M_2 be central symmetric square matrices over K of dimension n. Observe that $M_1 - M_2$ is central symmetric.

Let us consider n, K and let M be a central symmetric square matrix over K of dimension n. Observe that M^{T} is central symmetric.

Let us consider n, K. Note that every square matrix over K of dimension n which is symmetric and subsymmetric is also central symmetric.

3. Basic Properties of Symmetric Circulant Matrices

Let K be a set, let M be a matrix over K, and let p be a finite sequence. We say that M is symmetry circulant about p if and only if the conditions (Def. 4) are satisfied.

(Def. 4)(i) $\operatorname{len} p = \operatorname{width} M$,

(ii) for all natural numbers i, j such that $\langle i, j\rangle \in$ the indices of M and $i + j \neq \operatorname{len} p + 1$ holds $M_{i,j} = p(((i + j) - 1) \bmod \operatorname{len} p)$, and

(iii) for all natural numbers i, j such that $\langle i, j\rangle \in$ the indices of M and $i + j = \operatorname{len} p + 1$ holds $M_{i,j} = p(\operatorname{len} p)$.

The following propositions are true:

(2) $(a)^{n\times n}$ is symmetry circulant about $n \mapsto a$.

(3) If M_1 is symmetry circulant about p, then $a \cdot M_1$ is symmetry circulant about $a \cdot p$.

(4) If M_1 is symmetry circulant about p, then $-M_1$ is symmetry circulant about $-p$.

(5) If M_1 is symmetry circulant about p and M_2 is symmetry circulant about q, then $M_1 + M_2$ is symmetry circulant about $p + q$.

Let K be a set and let M be a matrix over K. We say that M is symmetry circulant if and only if:

(Def. 5) There exists a finite sequence p of elements of K such that $\operatorname{len} p = \operatorname{width} M$ and M is symmetry circulant about p.

Let K be a non empty set and let p be a finite sequence of elements of K. We say that p is first symmetry of circulant if and only if:

(Def. 6) There exists a square matrix over K of dimension $\operatorname{len} p$ which is symmetry circulant about p.

Let K be a non empty set and let p be a finite sequence of elements of K. Let us assume that p is first symmetry of circulant. The functor $\operatorname{SCirc} p$ yielding a square matrix over K of dimension $\operatorname{len} p$ is defined as follows:

(Def. 7) $\operatorname{SCirc} p$ is symmetry circulant about p.

Let us consider n, K, a. Note that $(a)^{n\times n}$ is symmetry circulant.

Let us consider n, K. Note that there exists a square matrix over K of dimension n which is symmetry circulant.

In the sequel D is a non empty set, t is a finite sequence of elements of D, and A is a square matrix over D of dimension n.

We now state the proposition

(6) Let p be a finite sequence of elements of D. Suppose $0 < n$ and A is symmetry circulant about p. Then A^{T} is symmetry circulant about p.

Let us consider n, K, a and let M_1 be a symmetry circulant square matrix over K of dimension n. Note that $a \cdot M_1$ is symmetry circulant.

Let us consider n, K and let M_1, M_2 be symmetry circulant square matrices over K of dimension n. Note that $M_1 + M_2$ is symmetry circulant.

Let us consider n, K and let M_1 be a symmetry circulant square matrix over K of dimension n. Note that $-M_1$ is symmetry circulant.

Let us consider n, K and let M_1, M_2 be symmetry circulant square matrices over K of dimension n. Observe that $M_1 - M_2$ is symmetry circulant.

The following propositions are true:

(7) If A is symmetry circulant and $n > 0$, then A^{T} is symmetry circulant.

(8) If p is first symmetry of circulant, then $-p$ is first symmetry of circulant.

(9) If p is first symmetry of circulant, then $\operatorname{SCirc}(-p) = -\operatorname{SCirc} p$.

(10) Suppose p is first symmetry of circulant and q is first symmetry of circulant and $\operatorname{len} p = \operatorname{len} q$. Then $p + q$ is first symmetry of circulant.

(11) If $\operatorname{len} p = \operatorname{len} q$ and p is first symmetry of circulant and q is first symmetry of circulant, then $\operatorname{SCirc}(p + q) = \operatorname{SCirc} p + \operatorname{SCirc} q$.

(12) If p is first symmetry of circulant, then $a \cdot p$ is first symmetry of circulant.

(13) If p is first symmetry of circulant, then $\operatorname{SCirc}(a \cdot p) = a \cdot \operatorname{SCirc} p$.

(14) If p is first symmetry of circulant, then $a \cdot \operatorname{SCirc} p + b \cdot \operatorname{SCirc} p = \operatorname{SCirc}((a + b) \cdot p)$.

(15) If p is first symmetry of circulant and q is first symmetry of circulant and $\operatorname{len} p = \operatorname{len} q$, then $a \cdot \operatorname{SCirc} p + a \cdot \operatorname{SCirc} q = \operatorname{SCirc}(a \cdot (p + q))$.

(16) Suppose p is first symmetry of circulant and q is first symmetry of circulant and $\operatorname{len} p = \operatorname{len} q$. Then $a \cdot \operatorname{SCirc} p + b \cdot \operatorname{SCirc} q = \operatorname{SCirc}(a \cdot p + b \cdot q)$.

(17) If M_1 is symmetry circulant, then ${M_1}^{\mathrm{T}} = M_1$.

Let us consider n, K. Note that every square matrix over K of dimension n which is symmetry circulant is also symmetric.

REFERENCES

[1] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[2] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[3] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[7] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.
[8] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(**5**):711–717, 1991.
[9] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[10] Karol Pąk. Basic properties of the rank of matrices over a field. *Formalized Mathematics*, 15(**4**):199–211, 2007, doi:10.2478/v10037-007-0024-5.
[11] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[12] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[13] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[14] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[15] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[16] Xiaopeng Yue, Xiquan Liang, and Zhongpin Sun. Some properties of some special matrices. *Formalized Mathematics*, 13(**4**):541–547, 2005.
[17] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.
[18] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Received October 23, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 79–86, 2012
DOI: 10.2478/v10037-012-0011-3

VERSITA
versita.com/fm/

Riemann Integral of Functions from $\mathbb{R}$ into n-dimensional Real Normed Space

Keiichi Miyajima
Ibaraki University
Faculty of Engineering
Hitachi, Japan

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

Yasunari Shidama[1]
Shinshu University
Nagano, Japan

Summary. In this article, we define the Riemann integral on functions $\mathbb{R}$ into n-dimensional real normed space and prove the linearity of this operator. As a result, the Riemann integration can be applied to the wider range. Our method refers to the [21].

MML identifier: INTEGR19, version: 7.12.02 4.175.1137

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

1. On the Functions from $\mathbb{R}$ into n-dimensional Real Space

For simplicity, we adopt the following convention: X denotes a set, n denotes an element of $\mathbb{N}$, a, b, c, d, e, r, x_0 denote real numbers, A denotes a non empty closed-interval subset of $\mathbb{R}$, f, g, h denote partial functions from $\mathbb{R}$ to $\mathcal{R}^n$, and E denotes an element of $\mathcal{R}^n$. We now state a number of propositions:

(1) If $a \leq c \leq b$, then $c \in [a, b]$ and $[a, c] \subseteq [a, b]$ and $[c, b] \subseteq [a, b]$.

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

ISSN 1426–2630(p), 1898-9934(e)

(2) If $a \leq c \leq d \leq b$ and $[a, b] \subseteq X$, then $[c, d] \subseteq X$.

(3) If $a \leq b$ and c, $d \in [a, b]$ and $[a, b] \subseteq X$, then $[\min(c, d), \max(c, d)] \subseteq X$.

(4) If $a \leq c \leq d \leq b$ and $[a, b] \subseteq \operatorname{dom} f$ and $[a, b] \subseteq \operatorname{dom} g$, then $[c, d] \subseteq \operatorname{dom}(f + g)$.

(5) If $a \leq c \leq d \leq b$ and $[a, b] \subseteq \operatorname{dom} f$ and $[a, b] \subseteq \operatorname{dom} g$, then $[c, d] \subseteq \operatorname{dom}(f - g)$.

(6) Let f be a partial function from $\mathbb{R}$ to $\mathbb{R}$. Suppose $a \leq c \leq d \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$. Then $r \cdot f$ is integrable on $[c, d]$ and $(r \cdot f)\restriction[c, d]$ is bounded.

(7) Let f, g be partial functions from $\mathbb{R}$ to $\mathbb{R}$. Suppose that $a \leq c \leq d \leq b$ and f is integrable on $[a, b]$ and g is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $g\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and $[a, b] \subseteq \operatorname{dom} g$. Then $f - g$ is integrable on $[c, d]$ and $(f - g)\restriction[c, d]$ is bounded.

(8) Suppose $a \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and $c \in [a, b]$. Then f is integrable on $[a, c]$ and f is integrable on $[c, b]$ and $\int_a^b f(x)dx = \int_a^c f(x)dx + \int_c^b f(x)dx$.

(9) Suppose $a \leq c \leq d \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$. Then f is integrable on $[c, d]$ and $f\restriction[c, d]$ is bounded.

(10) Suppose that $a \leq c \leq d \leq b$ and f is integrable on $[a, b]$ and g is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $g\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and $[a, b] \subseteq \operatorname{dom} g$. Then $f + g$ is integrable on $[c, d]$ and $(f + g)\restriction[c, d]$ is bounded.

(11) Suppose $a \leq c \leq d \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$. Then $r \cdot f$ is integrable on $[c, d]$ and $(r \cdot f)\restriction[c, d]$ is bounded.

(12) Suppose $a \leq c \leq d \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$. Then $-f$ is integrable on $[c, d]$ and $(-f)\restriction[c, d]$ is bounded.

(13) Suppose that $a \leq c \leq d \leq b$ and f is integrable on $[a, b]$ and g is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $g\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and $[a, b] \subseteq \operatorname{dom} g$. Then $f - g$ is integrable on $[c, d]$ and $(f - g)\restriction[c, d]$ is bounded.

(14) Let n be a non empty element of $\mathbb{N}$ and f be a function from A into $\mathcal{R}^n$. Then f is bounded if and only if $|f|$ is bounded.

(15) If f is bounded and $A \subseteq \operatorname{dom} f$, then $f\restriction A$ is bounded.

(16) Let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$ and g be a function from A into $\mathcal{R}^n$. If f is bounded and $f = g$, then g is bounded.

(17) For every partial function f from $\mathbb{R}$ to $\mathcal{R}^n$ and for every function g from

A into $\mathcal{R}^n$ such that $f = g$ holds $|f| = |g|$.

(18) If $A \subseteq \operatorname{dom} h$, then $|h\restriction A| = |h|\restriction A$.

(19) Let n be a non empty element of $\mathbb{N}$ and h be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. If $A \subseteq \operatorname{dom} h$ and $h\restriction A$ is bounded, then $|h|\restriction A$ is bounded.

(20) Let n be a non empty element of $\mathbb{N}$ and h be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. Suppose $A \subseteq \operatorname{dom} h$ and $h\restriction A$ is bounded and h is integrable on A and $|h|$ is integrable on A. Then $|\int\limits_A h(x)dx| \leq \int\limits_A |h|(x)dx$.

(21) Let n be a non empty element of $\mathbb{N}$ and h be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. Suppose $a \leq b$ and $[a, b] \subseteq \operatorname{dom} h$ and h is integrable on $[a, b]$ and $|h|$ is integrable on $[a, b]$ and $h\restriction[a, b]$ is bounded. Then $|\int\limits_a^b h(x)dx| \leq \int\limits_a^b |h|(x)dx$.

(22) Let n be a non empty element of $\mathbb{N}$ and f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. Suppose that $a \leq b$ and f is integrable on $[a, b]$ and $|f|$ is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$. Then $|f|$ is integrable on $[\min(c, d), \max(c, d)]$ and $|f|\restriction[\min(c, d), \max(c, d)]$ is bounded and $|\int\limits_c^d f(x)dx| \leq \int\limits_{\min(c,d)}^{\max(c,d)} |f|(x)dx$.

(23) Let n be a non empty element of $\mathbb{N}$ and f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. Suppose that $a \leq b$ and $c \leq d$ and f is integrable on $[a, b]$ and $|f|$ is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$. Then $|f|$ is integrable on $[c, d]$ and $|f|\restriction[c, d]$ is bounded and $|\int\limits_c^d f(x)dx| \leq \int\limits_c^d |f|(x)dx$ and $|\int\limits_d^c f(x)dx| \leq \int\limits_c^d |f|(x)dx$.

(24) Let n be a non empty element of $\mathbb{N}$ and f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. Suppose that $a \leq b$ and $c \leq d$ and f is integrable on $[a, b]$ and $|f|$ is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$ and for every real number x such that $x \in [c, d]$ holds $|f_x| \leq e$. Then $|\int\limits_c^d f(x)dx| \leq e \cdot (d - c)$ and $|\int\limits_d^c f(x)dx| \leq e \cdot (d - c)$.

(25) If $a \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$, then $\int\limits_c^d (r \cdot f)(x)dx = r \cdot \int\limits_c^d f(x)dx$.

(26) If $a \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$, then $\int\limits_c^d (-f)(x)dx = -\int\limits_c^d f(x)dx$.

(27) Suppose that $a \leq b$ and f is integrable on $[a, b]$ and g is integrable on $[a, b]$ and $f \restriction [a, b]$ is bounded and $g \restriction [a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and $[a, b] \subseteq \operatorname{dom} g$ and c, $d \in [a, b]$. Then $\int_c^d (f + g)(x)dx = \int_c^d f(x)dx + \int_c^d g(x)dx$.

(28) Suppose that $a \leq b$ and f is integrable on $[a, b]$ and g is integrable on $[a, b]$ and $f \restriction [a, b]$ is bounded and $g \restriction [a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and $[a, b] \subseteq \operatorname{dom} g$ and c, $d \in [a, b]$. Then $\int_c^d (f - g)(x)dx = \int_c^d f(x)dx - \int_c^d g(x)dx$.

(29) Suppose $a \leq b$ and $[a, b] \subseteq \operatorname{dom} f$ and for every real number x such that $x \in [a, b]$ holds $f(x) = E$. Then f is integrable on $[a, b]$ and $f \restriction [a, b]$ is bounded and $\int_a^b f(x)dx = (b - a) \cdot E$.

(30) Suppose $a \leq b$ and for every real number x such that $x \in [a, b]$ holds $f(x) = E$ and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$. Then $\int_c^d f(x)dx = (d - c) \cdot E$.

(31) If $a \leq b$ and f is integrable on $[a, b]$ and $f \restriction [a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$, then $\int_a^d f(x)dx = \int_a^c f(x)dx + \int_c^d f(x)dx$.

(32) Suppose that $a \leq b$ and f is integrable on $[a, b]$ and $f \restriction [a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$ and for every real number x such that $x \in [\min(c, d), \max(c, d)]$ holds $|f_x| \leq e$. Then $|\int_c^d f(x)dx| \leq n \cdot e \cdot |d - c|$.

(33) $\int_b^a f(x)dx = -\int_a^b f(x)dx$.

2. On the Functions from $\mathbb{R}$ into n-dimensional Real Normed Space

Let R be a real normed space, let X be a non empty set, and let g be a partial function from X to R. We say that g is bounded if and only if:

(Def. 1) There exists a real number r such that for every set y such that $y \in \operatorname{dom} g$ holds $\|g_y\| < r$.

Next we state a number of propositions:

(34) Let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$ and g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. If $f = g$, then f is bounded iff g is bounded.

(35) Let X, Y be sets and f_1, f_2 be partial functions from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $f_1 \restriction X$ is bounded and $f_2 \restriction Y$ is bounded. Then $(f_1 + f_2) \restriction (X \cap Y)$ is bounded and $(f_1 - f_2) \restriction (X \cap Y)$ is bounded.

(36) Let f be a function from A into $\mathcal{R}^n$, g be a function from A into $\langle \mathcal{E}^n, \|\cdot\| \rangle$, D be a Division of A, p be a finite sequence of elements of $\mathcal{R}^n$, and q be a finite sequence of elements of $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $f = g$ and $p = q$. Then p is a middle volume of f and D if and only if q is a middle volume of g and D.

(37) Let f be a function from A into $\mathcal{R}^n$, g be a function from A into $\langle \mathcal{E}^n, \|\cdot\| \rangle$, D be a Division of A, p be a middle volume of f and D, and q be a middle volume of g and D. If $f = g$ and $p = q$, then middle $\mathrm{sum}(f, p) =$ middle $\mathrm{sum}(g, q)$.

(38) Let f be a function from A into $\mathcal{R}^n$, g be a function from A into $\langle \mathcal{E}^n, \|\cdot\| \rangle$, T be a division sequence of A, p be a function from $\mathbb{N}$ into $(\mathcal{R}^n)^*$, and q be a function from $\mathbb{N}$ into (the carrier of $\langle \mathcal{E}^n, \|\cdot\| \rangle)^*$. Suppose $f = g$ and $p = q$. Then p is a middle volume sequence of f and T if and only if q is a middle volume sequence of g and T.

(39) Let f be a function from A into $\mathcal{R}^n$, g be a function from A into $\langle \mathcal{E}^n, \|\cdot\| \rangle$, T be a division sequence of A, S be a middle volume sequence of f and T, and U be a middle volume sequence of g and T. If $f = g$ and $S = U$, then middle $\mathrm{sum}(f, S) =$ middle $\mathrm{sum}(g, U)$.

(40) Let f be a function from A into $\mathcal{R}^n$, g be a function from A into $\langle \mathcal{E}^n, \|\cdot\| \rangle$, I be an element of $\mathcal{R}^n$, and J be a point of $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $f = g$ and $I = J$. Then the following statements are equivalent

(i) for every division sequence T of A and for every middle volume sequence S of f and T such that δ_T is convergent and $\lim(\delta_T) = 0$ holds middle $\mathrm{sum}(f, S)$ is convergent and $\lim$ middle $\mathrm{sum}(f, S) = I$,

(ii) for every division sequence T of A and for every middle volume sequence S of g and T such that δ_T is convergent and $\lim(\delta_T) = 0$ holds middle $\mathrm{sum}(g, S)$ is convergent and $\lim$ middle $\mathrm{sum}(g, S) = J$.

(41) Let f be a function from A into $\mathcal{R}^n$ and g be a function from A into $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $f = g$ and f is bounded. Then f is integrable if and only if g is integrable.

(42) Let f be a function from A into $\mathcal{R}^n$ and g be a function from A into $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $f = g$ and f is bounded and integrable. Then g is integrable and integral $f =$ integral g.

(43) Let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$ and g be a partial function

from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $f = g$ and $f \restriction A$ is bounded and $A \subseteq \operatorname{dom} f$. Then f is integrable on A if and only if g is integrable on A.

(44) Let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$ and g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $f = g$ and $f \restriction A$ is bounded and $A \subseteq \operatorname{dom} f$ and f is integrable on A. Then g is integrable on A and $\int\limits_A f(x)dx = \int\limits_A g(x)dx$.

(45) Let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$ and g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $f = g$ and $a \leq b$ and $f \restriction [a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and f is integrable on $[a, b]$. Then $\int\limits_a^b f(x)dx = \int\limits_a^b g(x)dx$.

(46) Let f, g be partial functions from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $a \leq b$ and f is integrable on $[a, b]$ and g is integrable on $[a, b]$ and $[a, b] \subseteq \operatorname{dom} f$ and $[a, b] \subseteq \operatorname{dom} g$. Then $\int\limits_a^b (f + g)(x)dx = \int\limits_a^b f(x)dx + \int\limits_a^b g(x)dx$ and $\int\limits_a^b (f - g)(x)dx = \int\limits_a^b f(x)dx - \int\limits_a^b g(x)dx$.

(47) For every partial function f from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ such that $a \leq b$ and $[a, b] \subseteq \operatorname{dom} f$ holds $\int\limits_b^a f(x)dx = -\int\limits_a^b f(x)dx$.

(48) Let f be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and g be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. Suppose $f = g$ and $a \leq b$ and $[a, b] \subseteq \operatorname{dom} f$ and $f \restriction [a, b]$ is bounded and f is integrable on $[a, b]$ and c, $d \in [a, b]$. Then $\int\limits_c^d f(x)dx = \int\limits_c^d g(x)dx$.

(49) Let f, g be partial functions from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose that $a \leq b$ and f is integrable on $[a, b]$ and g is integrable on $[a, b]$ and $f \restriction [a, b]$ is bounded and $g \restriction [a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and $[a, b] \subseteq \operatorname{dom} g$ and c, $d \in [a, b]$. Then $\int\limits_c^d (f + g)(x)dx = \int\limits_c^d f(x)dx + \int\limits_c^d g(x)dx$.

(50) Let f, g be partial functions from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose that $a \leq b$ and f is integrable on $[a, b]$ and g is integrable on $[a, b]$ and $f \restriction [a, b]$ is bounded and $g \restriction [a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and $[a, b] \subseteq \operatorname{dom} g$ and c, $d \in [a, b]$. Then $\int\limits_c^d (f - g)(x)dx = \int\limits_c^d f(x)dx - \int\limits_c^d g(x)dx$.

(51) Let E be a point of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and f be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $a \leq b$ and $[a, b] \subseteq \operatorname{dom} f$ and for every real number

x such that $x \in [a, b]$ holds $f(x) = E$. Then f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $\int_a^b f(x)dx = (b - a) \cdot E$.

(52) Let E be a point of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and f be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $a \leq b$ and $[a, b] \subseteq \operatorname{dom} f$ and for every real number x such that $x \in [a, b]$ holds $f(x) = E$ and c, $d \in [a, b]$. Then $\int_c^d f(x)dx = (d - c) \cdot E$.

(53) Let f be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $a \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$. Then $\int_a^d f(x)dx = \int_a^c f(x)dx + \int_c^d f(x)dx$.

(54) Let f be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose that $a \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$ and for every real number x such that $x \in [\min(c, d), \max(c, d)]$ holds $\|f_x\| \leq e$. Then $\|\int_c^d f(x)dx\| \leq n \cdot e \cdot |d - c|$.

3. Fundamental Theorem of Calculus

The following two propositions are true:

(55)[2] Let n be a non empty element of $\mathbb{N}$ and F, f be partial functions from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose that $a \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and $]a, b[\subseteq \operatorname{dom} F$ and for every real number x such that $x \in]a, b[$ holds $F(x) = \int_a^x f(x)dx$ and $x_0 \in]a, b[$ and f is continuous in x_0. Then F is differentiable in x_0 and $F'(x_0) = f_{x_0}$.

(56) Let n be a non empty element of $\mathbb{N}$ and f be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $a \leq b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and $x_0 \in]a, b[$ and f is continuous in x_0. Then there exists a partial function F from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ such that $]a, b[\subseteq \operatorname{dom} F$ and for every real number x such that $x \in]a, b[$ holds $F(x) = \int_a^x f(x)dx$ and F is differentiable in x_0 and $F'(x_0) = f_{x_0}$.

[2] Fundamental Theorem of Calculus (for $\mathcal{R}^n$)

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 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] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[10] Noboru Endou and Artur Korniłowicz. The definition of the Riemann definite integral and some related lemmas. *Formalized Mathematics*, 8(**1**):93–102, 1999.
[11] Noboru Endou and Yasunari Shidama. Completeness of the real Euclidean space. *Formalized Mathematics*, 13(**4**):577–580, 2005.
[12] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Darboux's theorem. *Formalized Mathematics*, 9(**1**):197–200, 2001.
[13] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definition of integrability for partial functions from $\mathbb{R}$ to $\mathbb{R}$ and integrability for continuous functions. *Formalized Mathematics*, 9(**2**):281–284, 2001.
[14] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Scalar multiple of Riemann definite integral. *Formalized Mathematics*, 9(**1**):191–196, 2001.
[15] 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.
[16] Keiichi Miyajima and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into $\mathcal{R}^n$. *Formalized Mathematics*, 17(**2**):179–185, 2009, doi: 10.2478/v10037-009-0021-y.
[17] Keiko Narita, Artur Kornilowicz, and Yasunari Shidama. More on the continuity of real functions. *Formalized Mathematics*, 19(**4**):233–239, 2011, doi: 10.2478/v10037-011-0032-3.
[18] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[19] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[20] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[21] Murray R. Spiegel. *Theory and Problems of Vector Analysis*. McGraw-Hill, 1974.
[22] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[23] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[24] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[25] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[26] Hiroshi Yamazaki and Yasunari Shidama. Algebra of vector functions. *Formalized Mathematics*, 3(**2**):171–175, 1992.

Received October 27, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 87–95, 2012
DOI: 10.2478/v10037-012-0012-2

VERSITA
versita.com/fm/

Operations of Points on Elliptic Curve in Projective Coordinates

Yuichi Futa
Shinshu University
Nagano, Japan

Hiroyuki Okazaki[1]
Shinshu University
Nagano, Japan

Daichi Mizushima
Shinshu University
Nagano, Japan

Yasunari Shidama[2]
Shinshu University
Nagano, Japan

Summary. In this article, we formalize operations of points on an elliptic curve over **GF**(**p**). Elliptic curve cryptography [7], whose security is based on a difficulty of discrete logarithm problem of elliptic curves, is important for information security. We prove that the two operations of points: `compell`$_{\texttt{ProjCo}}$ and `addell`$_{\texttt{ProjCo}}$ are unary and binary operations of a point over the elliptic curve.

MML identifier: `EC_PF_2`, version: `7.12.02 4.176.1140`

The terminology and notation used here are introduced in the following papers: [5], [17], [3], [1], [13], [4], [2], [12], [14], [10], [9], [16], [15], [8], [11], and [6].

1. Arithmetic in **GF**(**p**)

For simplicity, we adopt the following convention: i, j denote integers, n denotes a natural number, K denotes a field, and a_1, a_2, a_3, a_4, a_5, a_6 denote elements of K.

One can prove the following propositions:

(1) If $a_1 = -a_2$, then ${a_1}^2 = {a_2}^2$.

(2) $(1_K)^{-1} = 1_K$.

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

ISSN 1426–2630(p), 1898-9934(e)

(3) If $a_2 \neq 0_K$ and $a_4 \neq 0_K$ and $a_1 \cdot {a_2}^{-1} = a_3 \cdot {a_4}^{-1}$, then $a_1 \cdot a_4 = a_2 \cdot a_3$.

(4) If $a_2 \neq 0_K$ and $a_4 \neq 0_K$ and $a_1 \cdot a_4 = a_2 \cdot a_3$, then $a_1 \cdot {a_2}^{-1} = a_3 \cdot {a_4}^{-1}$.

(5) If $a_1 = 0_K$ and $n > 1$, then ${a_1}^n = 0_K$.

(6) If $a_1 = -a_2$, then $-a_1 = a_2$.

(7) $a_1+a_2+a_3+a_4 = a_4+a_2+a_3+a_1$ and $a_1+a_2+a_3+a_4 = a_1+a_4+a_3+a_2$.

(8) $(a_1 + a_2 + a_3) + a_4 = a_1 + (a_2 + a_3 + a_4)$ and $(a_1 + a_2 + a_3 + a_4) + a_5 = a_1 + (a_2 + a_3 + a_4 + a_5)$.

(9) $(a_1 + a_2 + a_3 + a_4 + a_5) + a_6 = a_1 + (a_2 + a_3 + a_4 + a_5 + a_6)$.

(10) $a_1 \cdot a_2 \cdot a_3 \cdot a_4 = a_4 \cdot a_2 \cdot a_3 \cdot a_1$ and $a_1 \cdot a_2 \cdot a_3 \cdot a_4 = a_1 \cdot a_4 \cdot a_3 \cdot a_2$.

(11) $(a_1 \cdot a_2 \cdot a_3) \cdot a_4 = a_1 \cdot (a_2 \cdot a_3 \cdot a_4)$ and $(a_1 \cdot a_2 \cdot a_3 \cdot a_4) \cdot a_5 = a_1 \cdot (a_2 \cdot a_3 \cdot a_4 \cdot a_5)$.

(12) $(a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5) \cdot a_6 = a_1 \cdot (a_2 \cdot a_3 \cdot a_4 \cdot a_5 \cdot a_6)$ and $a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5 \cdot a_6 = a_1 \cdot (a_2 \cdot a_3 \cdot a_4) \cdot a_5 \cdot a_6$.

(13) $(a_1 \cdot a_2 \cdot a_3)^n = {a_1}^n \cdot {a_2}^n \cdot {a_3}^n$.

(14) $a_1 \cdot (a_2 + a_3 + a_4) = a_1 \cdot a_2 + a_1 \cdot a_3 + a_1 \cdot a_4$ and $a_1 \cdot ((a_2 + a_3) - a_4) = (a_1 \cdot a_2 + a_1 \cdot a_3) - a_1 \cdot a_4$ and $a_1 \cdot ((a_2 - a_3) + a_4) = (a_1 \cdot a_2 - a_1 \cdot a_3) + a_1 \cdot a_4$ and $a_1 \cdot (a_2 - a_3 - a_4) = a_1 \cdot a_2 - a_1 \cdot a_3 - a_1 \cdot a_4$ and $a_1 \cdot (-a_2 + a_3 + a_4) = -a_1 \cdot a_2 + a_1 \cdot a_3 + a_1 \cdot a_4$ and $a_1 \cdot ((-a_2 + a_3) - a_4) = (-a_1 \cdot a_2 + a_1 \cdot a_3) - a_1 \cdot a_4$ and $a_1 \cdot ((-a_2 - a_3) + a_4) = (-a_1 \cdot a_2 - a_1 \cdot a_3) + a_1 \cdot a_4$ and $a_1 \cdot (-a_2 - a_3 - a_4) = -a_1 \cdot a_2 - a_1 \cdot a_3 - a_1 \cdot a_4$.

(15) $(a_1 + a_2) \cdot (a_1 - a_2) = {a_1}^2 - {a_2}^2$.

(16) $(a_1 + a_2) \cdot (({a_1}^2 - a_1 \cdot a_2) + {a_2}^2) = {a_1}^3 + {a_2}^3$.

(17) $(a_1 - a_2) \cdot ({a_1}^2 + a_1 \cdot a_2 + {a_2}^2) = {a_1}^3 - {a_2}^3$.

Let n, p be natural numbers. We say that p is n or greater if and only if:

(Def. 1) $n \leq p$.

Let us note that there exists a natural number which is 5 or greater and prime.

The following propositions are true:

(18) For all elements g_1, g_2, g_3, a of $\mathrm{GF}(p)$ such that $g_1 = i \bmod p$ and $g_2 = j \bmod p$ and $g_3 = (i + j) \bmod p$ holds $g_1 \cdot a + g_2 \cdot a = g_3 \cdot a$.

(19) For all elements g_1, g_2, a of $\mathrm{GF}(p)$ such that $g_1 = i \bmod p$ and $g_2 = j \bmod p$ and $j = i + 1$ holds $g_1 \cdot a + a = g_2 \cdot a$.

(20) For all elements g_4, a of $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ holds $a + a = g_4 \cdot a$.

(21) For all elements g_1, g_2, g_3, a of $\mathrm{GF}(p)$ such that $g_1 = i \bmod p$ and $g_2 = j \bmod p$ and $g_3 = (i - j) \bmod p$ holds $g_1 \cdot a - g_2 \cdot a = g_3 \cdot a$.

(22) For all elements g_1, g_2, a of $\mathrm{GF}(p)$ such that $g_1 = i \bmod p$ and $g_2 = j \bmod p$ and $i = j + 1$ holds $g_1 \cdot a - g_2 \cdot a = a$.

(23) For all elements g_1, g_2, a of $\mathrm{GF}(p)$ such that $g_1 = i \bmod p$ and $g_2 = j \bmod p$ and $i = j + 1$ holds $g_1 \cdot a - a = g_2 \cdot a$.

(24) For all elements g_4, a of $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ holds $g_4 \cdot a - a = a$.

(25) For all elements g_4, a, b of $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ holds $(a+b)^2 = a^2 + g_4 \cdot a \cdot b + b^2$.

(26) For all elements g_4, a, b of $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ holds $(a-b)^2 = (a^2 - g_4 \cdot a \cdot b) + b^2$.

(27) For all elements g_4, a, b, c, d of $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ holds $(a \cdot c + b \cdot d)^2 = a^2 \cdot c^2 + g_4 \cdot a \cdot b \cdot c \cdot d + b^2 \cdot d^2$.

(28) Let p be a prime number, n be a natural number, and g_4 be an element of $\mathrm{GF}(p)$. If $p > 2$ and $g_4 = 2 \bmod p$, then $g_4 \neq 0_{\mathrm{GF}(p)}$ and ${g_4}^n \neq 0_{\mathrm{GF}(p)}$.

(29) Let p be a prime number, n be a natural number, and g_4, g_5 be elements of $\mathrm{GF}(p)$. If $p > 3$ and $g_5 = 3 \bmod p$, then $g_5 \neq 0_{\mathrm{GF}(p)}$ and ${g_5}^n \neq 0_{\mathrm{GF}(p)}$.

2. Parameters of an Elliptic Curve

Let p be a 5 or greater prime number. The parameters of elliptic curve p yielding a subset of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) is defined as follows:

(Def. 2) The parameters of elliptic curve $p = \{\langle a, b\rangle; a$ ranges over elements of $\mathrm{GF}(p)$, b ranges over elements of $\mathrm{GF}(p)$: $\mathrm{Disc}(a) \neq 0_{\mathrm{GF}(p)}\}$.

Let p be a 5 or greater prime number. Observe that the parameters of elliptic curve p is non empty.

Let p be a 5 or greater prime number and let z be an element of the parameters of elliptic curve p. Then $z_{\mathbf{1}}$ is an element of $\mathrm{GF}(p)$. Then $z_{\mathbf{2}}$ is an element of $\mathrm{GF}(p)$.

The following proposition is true

(30) Let p be a 5 or greater prime number and z be an element of the parameters of elliptic curve p. Then $p > 3$ and $\mathrm{Disc}(z_{\mathbf{1}}) \neq 0_{\mathrm{GF}(p)}$.

For simplicity, we adopt the following rules: p_1, p_2, p_3 denote sets, P_1, P_2, P_3 denote elements of $\mathrm{GF}(p)$, P denotes an element of $\mathrm{ProjCo}(\mathrm{GF}(p))$, and O denotes an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$.

Let p be a prime number, let a, b be elements of $\mathrm{GF}(p)$, and let P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$. The functor $P_{\mathbf{1}}$ yields an element of $\mathrm{GF}(p)$ and is defined as follows:

(Def. 3) If $P = \langle p_1, p_2, p_3\rangle$, then $P_{\mathbf{1}} = p_1$.

The functor $P_{\mathbf{2}}$ yielding an element of $\mathrm{GF}(p)$ is defined as follows:

(Def. 4) If $P = \langle p_1, p_2, p_3\rangle$, then $P_{\mathbf{2}} = p_2$.

The functor $P_{\mathbf{3}}$ yielding an element of $\mathrm{GF}(p)$ is defined by:

(Def. 5) If $P = \langle p_1, p_2, p_3\rangle$, then $P_{\mathbf{3}} = p_3$.

We now state three propositions:

(31) For every prime number p and for all elements a, b of $\mathrm{GF}(p)$ and for every element P of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$ holds $P = \langle P_{\mathbf{1}}, P_{\mathbf{2}}, P_{\mathbf{3}} \rangle$.

(32) Let p be a prime number, a, b be elements of $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$, and Q be an element of $\mathrm{ProjCo}(\mathrm{GF}(p))$. Then $P = Q$ if and only if the following conditions are satisfied:

(i) $P_{\mathbf{1}} = Q_{\mathbf{1}}$,

(ii) $P_{\mathbf{2}} = Q_{\mathbf{2}}$, and

(iii) $P_{\mathbf{3}} = Q_{\mathbf{3}}$.

(33) Let p be a prime number, a, b, P_1, P_2, P_3 be elements of $\mathrm{GF}(p)$, and P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$. If $P = \langle P_1, P_2, P_3 \rangle$, then $P_{\mathbf{1}} = P_1$ and $P_{\mathbf{2}} = P_2$ and $P_{\mathbf{3}} = P_3$.

Let p be a prime number, let P be an element of $\mathrm{ProjCo}(\mathrm{GF}(p))$, and let C_1 be a function from (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) into $\mathrm{GF}(p)$. We say that P is on curve defined by an equation C_1 if and only if:

(Def. 6) $C_1(P) = 0_{\mathrm{GF}(p)}$.

The following two propositions are true:

(34) P is on curve defined by an equation $\mathrm{EC}_{\mathrm{WEqProjCo}}(a)$ iff P is an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$.

(35) Let p be a prime number, a, b be elements of $\mathrm{GF}(p)$, and P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$. Then $(P_{\mathbf{2}})^2 \cdot P_{\mathbf{3}} - ((P_{\mathbf{1}})^3 + a \cdot P_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + b \cdot (P_{\mathbf{3}})^3) = 0_{\mathrm{GF}(p)}$.

Let p be a prime number and let P be an element of $\mathrm{ProjCo}(\mathrm{GF}(p))$. The represent point of P yields an element of $\mathrm{ProjCo}(\mathrm{GF}(p))$ and is defined by:

(Def. 7)(i) The represent point of $P = \langle P_{\mathbf{1}} \cdot (P_{\mathbf{3}})^{-1}, P_{\mathbf{2}} \cdot (P_{\mathbf{3}})^{-1}, 1 \rangle$ if $P_{\mathbf{3}} \neq 0$,

(ii) the represent point of $P = \langle 0, 1, 0 \rangle$ if $P_{\mathbf{3}} = 0$,

(iii) $P_{\mathbf{3}} = 0$, otherwise.

The following propositions are true:

(36) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then the represent point of $P \equiv P$ and the represent point of $P \in \mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$.

(37) Let p be a prime number, a, b be elements of $\mathrm{GF}(p)$, and P be an element of $\mathrm{ProjCo}(\mathrm{GF}(p))$. Suppose (the represent point of $P)_{\mathbf{3}} = 0$. Then the represent point of $P = \langle 0, 1, 0 \rangle$ and $P_{\mathbf{3}} = 0$.

(38) Let p be a prime number, a, b be elements of $\mathrm{GF}(p)$, and P be an element of $\mathrm{ProjCo}(\mathrm{GF}(p))$. Suppose (the represent point of $P)_{\mathbf{3}} \neq 0$. Then the represent point of $P = \langle P_{\mathbf{1}} \cdot (P_{\mathbf{3}})^{-1}, P_{\mathbf{2}} \cdot (P_{\mathbf{3}})^{-1}, 1 \rangle$ and $P_{\mathbf{3}} \neq 0$.

(39) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $P \equiv Q$ if and only if the represent point of P = the represent point of Q.

3. Operations of Points on an Elliptic Curve over $\mathbf{GF}(\mathbf{p})$

Let p be a 5 or greater prime number and let z be an element of the parameters of elliptic curve p. The functor $\mathrm{compell}_{\mathrm{ProjCo}}(z, p)$ yields a function from $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ into $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ and is defined as follows:

(Def. 8) For every element P of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ holds $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P) = \langle P_{\mathbf{1}}, -P_{\mathbf{2}}, P_{\mathbf{3}} \rangle$.

Let p be a 5 or greater prime number, let z be an element of the parameters of elliptic curve p, let F be a function from $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ into $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and let P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $F(P)$ is an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$.

We now state a number of propositions:

(40) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and O be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $O = \langle 0, 1, 0 \rangle$, then $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(O) \equiv O$.

(41) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))((\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P)) = P$.

(42) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Suppose $P_{\mathbf{3}} \neq 0$. Then the represent point of $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P) = (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))$(the represent point of P).

(43) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $P = Q$ if and only if $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P) = (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$.

(44) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $P_{\mathbf{3}} \neq 0$, then $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P)$ iff $P_{\mathbf{2}} = 0$.

(45) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $P_{\mathbf{3}} \neq 0$, then $P_{\mathbf{1}} = Q_{\mathbf{1}}$ and $P_{\mathbf{3}} = Q_{\mathbf{3}}$ iff $P = Q$ or $P = (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$.

(46) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $P \equiv Q$ if and only if $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P) \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$.

(47) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$ if and only if $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P) \equiv Q$.

(48) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Suppose $P_{\mathbf{3}} \neq 0$ and $Q_{\mathbf{3}} \neq 0$. Then the represent point of $P = (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))$(the

represent point of Q) if and only if $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z,p))(Q)$.

(49) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $P \equiv Q$, then $P_{\mathbf{2}} \cdot Q_{\mathbf{3}} = Q_{\mathbf{2}} \cdot P_{\mathbf{3}}$.

(50) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Suppose $P_{\mathbf{3}} \neq 0$ and $Q_{\mathbf{3}} \neq 0$. Then $P \equiv Q$ or $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z,p))(Q)$ if and only if $P_{\mathbf{1}} \cdot Q_{\mathbf{3}} = Q_{\mathbf{1}} \cdot P_{\mathbf{3}}$.

(51) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $P_{\mathbf{3}} \neq 0$ and $Q_{\mathbf{3}} \neq 0$ and $P_{\mathbf{2}} \neq 0$, then if $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z,p))(Q)$, then $P_{\mathbf{2}} \cdot Q_{\mathbf{3}} \neq Q_{\mathbf{2}} \cdot P_{\mathbf{3}}$.

(52) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, and P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $P \not\equiv Q$ and $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z,p))(Q)$, then $P_{\mathbf{2}} \cdot Q_{\mathbf{3}} \neq Q_{\mathbf{2}} \cdot P_{\mathbf{3}}$.

(53) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_5 be an element of $\mathrm{GF}(p)$, and P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $g_5 = 3 \bmod p$ and $P_{\mathbf{2}} = 0$ and $P_{\mathbf{3}} \neq 0$, then $z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2 \neq 0$.

(54) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_4, g_6, g_7, g_8 be elements of $\mathrm{GF}(p)$, P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that

(i) $g_4 = 2 \bmod p$,

(ii) $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$,

(iii) $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$,

(iv) $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$, and

(v) $R = \langle g_7 \cdot g_8,\ g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}},\ {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \rangle$.

Then $g_7 \cdot P_{\mathbf{3}} \cdot R_{\mathbf{2}} = -(g_6 \cdot (R_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot R_{\mathbf{3}}) + g_7 \cdot P_{\mathbf{2}} \cdot R_{\mathbf{3}})$.

(55) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_4, g_6, g_7, g_8 be elements of $\mathrm{GF}(p)$, P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that

(i) $g_4 = 2 \bmod p$,

(ii) $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$,

(iii) $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$,

(iv) $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$, and

(v) $R = \langle g_7 \cdot g_8,\ g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}},\ {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \rangle$.

Then $-{g_7}^2 \cdot (P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{1}} + P_{\mathbf{3}} \cdot Q_{\mathbf{1}} \cdot R_{\mathbf{3}} + P_{\mathbf{1}} \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}}) + P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}} \cdot {g_6}^2 = 0_{\mathrm{GF}(p)}$.

(56) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_4, g_6, g_7, g_8 be elements of $\mathrm{GF}(p)$, P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that

(i) $g_4 = 2 \bmod p$,

(ii) $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$,

(iii) $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$,

(iv) $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$, and

(v) $R = \langle g_7 \cdot g_8,\ g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}},\ {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \rangle$.

Then $z_{\mathbf{2}} \cdot {g_7}^2 \cdot (P_{\mathbf{3}})^2 \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}} = -{g_7}^2 \cdot P_{\mathbf{3}} \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{1}} \cdot R_{\mathbf{1}} + (g_7 \cdot P_{\mathbf{2}} - g_6 \cdot P_{\mathbf{1}})^2 \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}}$.

(57) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_4, g_6, g_7, g_8 be elements of $\mathrm{GF}(p)$, P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that

(i) $g_4 = 2 \bmod p$,

(ii) $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$,

(iii) $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$,

(iv) $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$, and

(v) $R = \langle g_7 \cdot g_8,\ g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}},\ {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \rangle$.

Then $z_{\mathbf{1}} \cdot {g_7}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}} = {g_7}^2 \cdot (P_{\mathbf{1}} \cdot Q_{\mathbf{1}} \cdot R_{\mathbf{3}} + P_{\mathbf{3}} \cdot Q_{\mathbf{1}} \cdot R_{\mathbf{1}} + P_{\mathbf{1}} \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{1}}) + g_4 \cdot g_6 \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}} \cdot (g_7 \cdot P_{\mathbf{2}} - g_6 \cdot P_{\mathbf{1}})$.

(58) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_4, g_6, g_7, g_8 be elements of $\mathrm{GF}(p)$, P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that

(i) $g_4 = 2 \bmod p$,

(ii) $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$,

(iii) $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$,

(iv) $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$, and

(v) $R = \langle g_7 \cdot g_8,\ g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}},\ {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \rangle$.

Then ${g_7}^2 \cdot (P_{\mathbf{3}})^2 \cdot Q_{\mathbf{3}} \cdot ((R_{\mathbf{2}})^2 \cdot R_{\mathbf{3}} - ((R_{\mathbf{1}})^3 + z_{\mathbf{1}} \cdot R_{\mathbf{1}} \cdot (R_{\mathbf{3}})^2 + z_{\mathbf{2}} \cdot (R_{\mathbf{3}})^3)) = 0_{\mathrm{GF}(p)}$.

(59) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10} be elements of $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ and $R = \langle g_4 \cdot g_{10} \cdot g_7,\ g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2,\ g_9 \cdot {g_7}^3 \rangle$. Then $g_4 \cdot g_7 \cdot P_{\mathbf{3}} \cdot R_{\mathbf{2}} = -(g_6 \cdot (P_{\mathbf{3}} \cdot R_{\mathbf{1}} - P_{\mathbf{1}} \cdot R_{\mathbf{3}}) + g_4 \cdot g_7 \cdot P_{\mathbf{2}} \cdot R_{\mathbf{3}})$.

(60) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10} be elements of $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ and $R = \langle g_4 \cdot g_{10} \cdot g_7,\ g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2,\ g_9 \cdot {g_7}^3 \rangle$. Then $g_{11} \cdot {g_7}^2 \cdot P_{\mathbf{3}} \cdot R_{\mathbf{1}} = R_{\mathbf{3}} \cdot ({g_6}^2 \cdot P_{\mathbf{3}} - g_9 \cdot {g_7}^2 \cdot P_{\mathbf{1}})$.

(61) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10} be elements of $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ and $R = \langle g_4 \cdot g_{10} \cdot g_7,\ g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2,\ g_9 \cdot {g_7}^3 \rangle$. Then $g_{11} \cdot {g_7}^2 \cdot (P_{\mathbf{3}})^2 \cdot (z_{\mathbf{2}} \cdot R_{\mathbf{3}}) = R_{\mathbf{3}} \cdot (g_4 \cdot g_7 \cdot P_{\mathbf{2}} - g_6 \cdot P_{\mathbf{1}})^2 - g_{11} \cdot {g_7}^2 \cdot (P_{\mathbf{1}})^2 \cdot R_{\mathbf{1}}$.

(62) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10} be elements of $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ and $R = \langle g_4 \cdot g_{10} \cdot g_7,\ g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2,\ g_9 \cdot {g_7}^3 \rangle$. Then $g_4 \cdot {g_7}^2 \cdot (P_{\mathbf{3}})^2 \cdot (z_{\mathbf{1}} \cdot R_{\mathbf{3}}) = g_6 \cdot P_{\mathbf{3}} \cdot R_{\mathbf{3}} \cdot (g_4 \cdot g_7 \cdot P_{\mathbf{2}} - g_6 \cdot P_{\mathbf{1}}) + {g_7}^2 \cdot (g_{11} \cdot P_{\mathbf{1}} \cdot P_{\mathbf{3}} \cdot R_{\mathbf{1}} + g_4 \cdot (P_{\mathbf{1}})^2 \cdot R_{\mathbf{3}})$.

(63) Let p be a 5 or greater prime number, z be an element of the parameters of elliptic curve p, g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10} be elements of $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ and $R = \langle g_4 \cdot g_{10} \cdot g_7,\ g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2,\ g_9 \cdot {g_7}^3 \rangle$. Then $g_{11} \cdot {g_7}^2 \cdot (P_{\mathbf{3}})^2 \cdot ((R_{\mathbf{2}})^2 \cdot R_{\mathbf{3}} - ((R_{\mathbf{1}})^3 + z_{\mathbf{1}} \cdot R_{\mathbf{1}} \cdot (R_{\mathbf{3}})^2 + z_{\mathbf{2}} \cdot (R_{\mathbf{3}})^3)) = 0_{\mathrm{GF}(p)}$.

Let p be a 5 or greater prime number and let z be an element of the parameters of elliptic curve p. The functor $\mathrm{addell}_{\mathrm{ProjCo}}(z, p)$ yields a function from $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}}) \times \mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ into $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ and is defined by the condition (Def. 9).

(Def. 9) Let P, Q, O be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ such that $O = \langle 0, 1, 0 \rangle$. Then

(i) if $P \equiv O$, then $(\mathrm{addell}_{\mathrm{ProjCo}}(z, p))(P, Q) = Q$,

(ii) if $Q \equiv O$ and $P \not\equiv O$, then $(\mathrm{addell}_{\mathrm{ProjCo}}(z, p))(P, Q) = P$,

(iii) if $P \not\equiv O$ and $Q \not\equiv O$ and $P \not\equiv Q$, then for all elements g_4, g_6, g_7, g_8 of $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ and $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$ and $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$ and $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$ holds $(\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,Q) = \langle g_7 \cdot g_8,\ g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}},\ {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \rangle$, and

(iv) if $P \not\equiv O$ and $Q \not\equiv O$ and $P \equiv Q$, then for all elements g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10} of $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ holds $(\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,Q) = \langle g_4 \cdot g_{10} \cdot g_7,\ g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2,\ g_9 \cdot {g_7}^3 \rangle$.

Let p be a 5 or greater prime number, let z be an element of the parameters of elliptic curve p, let F be a function from $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}}) \times \mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ into $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and let Q, R be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $F(Q,R)$ is an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[2] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[5] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[6] 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.
[7] G. Seroussi I. Blake and N. Smart. *Elliptic Curves in Cryptography*. Number 265 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.
[8] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[9] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[10] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[11] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.
[12] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[13] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[14] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[15] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[16] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[17] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received November 3, 2011