FORMALIZED MATHEMATICS
Vol.2, No.2, March–April 1991
Université Catholique de Louvain

Metrics in Cartesian Product [1]

Stanisława Kanas
Technical University of Rzeszów

Jan Stankiewicz
Technical University of Rzeszów

Summary. A continuation of the paper [8]. It deals with the method of creation of the distance in the Cartesian product of metric spaces. The distance of two points belonging to the Cartesian product of metric spaces has been defined as the sum of distances of appriopriate coordinates (or projections) of these points. It is shown that the product of metric spaces with such a distance is a metric space.

MML Identifier: METRIC_3.

The articles [7], [12], [4], [5], [2], [6], [1], [9], [3], [8], [11], and [10] provide the notation and terminology for this paper. We follow the rules: X, Y will denote metric spaces, x_1, y_1, z_1 will denote elements of the carrier of X, and x_2, y_2, z_2 will denote elements of the carrier of Y. The scheme *LambdaMCART* concerns a non-empty set $\mathcal{A}$, a non-empty set $\mathcal{B}$, a non-empty set $\mathcal{C}$, and a 4-ary functor $\mathcal{F}$ yielding an element of $\mathcal{C}$ and states that:

there exists a function f from $[\![[\![\mathcal{A}, \mathcal{B}]\!], [\![\mathcal{A}, \mathcal{B}]\!]]\!]$ into $\mathcal{C}$ such that for all elements x_1, y_1 of $\mathcal{A}$ and for all elements x_2, y_2 of $\mathcal{B}$ and for all elements x, y of $[\![\mathcal{A}, \mathcal{B}]\!]$ such that $x = \langle x_1, x_2 \rangle$ and $y = \langle y_1, y_2 \rangle$ holds $f(\langle x, y \rangle) = \mathcal{F}(x_1, y_1, x_2, y_2)$

for all values of the parameters.

Let us consider X, Y. The functor $\rho^{X \times Y}$ yielding a function from $[\![[\![$ the carrier of X, the carrier of $Y]\!], [\![$ the carrier of X, the carrier of $Y]\!]]\!]$ into $\mathbb{R}$ is defined by:

(Def.1) for all elements x_1, y_1 of the carrier of X and for all elements x_2, y_2 of the carrier of Y and for all elements x, y of $[\![$ the carrier of X, the carrier of $Y]\!]$ such that $x = \langle x_1, x_2 \rangle$ and $y = \langle y_1, y_2 \rangle$ holds $\rho^{X \times Y}(x, y) = \rho(x_1, y_1) + \rho(x_2, y_2)$.

The following proposition is true

[1]Supported by RPBP.III-24.B3

ISSN 0777–4028

(1) Let X be a metric space. Let Y be a metric space. Let F be a function from $[\![[\![$ the carrier of X, the carrier of $Y]\!], [\![$ the carrier of X, the carrier of $Y]\!]]\!]$ into $\mathbb{R}$. Then $F = \rho^{X \times Y}$ if and only if for all elements x_1, y_1 of the carrier of X and for all elements x_2, y_2 of the carrier of Y and for all elements x, y of $[\![$ the carrier of X, the carrier of $Y]\!]$ such that $x = \langle x_1, x_2 \rangle$ and $y = \langle y_1, y_2 \rangle$ holds $F(x, y) = \rho(x_1, y_1) + \rho(x_2, y_2)$.

One can prove the following proposition

(2) For all elements a, b of $\mathbb{R}$ such that $a + b = 0$ and $0 \leq a$ and $0 \leq b$ holds $a = 0$ and $b = 0$.

We now state four propositions:

(3) For every metric space M and for all elements a, b of the carrier of M holds $\rho(a, b) = 0$ if and only if $a = b$.

(5)[2] For all elements x, y of $[\![$ the carrier of X, the carrier of $Y]\!]$ such that $x = \langle x_1, x_2 \rangle$ and $y = \langle y_1, y_2 \rangle$ holds $\rho^{X \times Y}(x, y) = 0$ if and only if $x = y$.

(6) For all elements x, y of $[\![$ the carrier of X, the carrier of $Y]\!]$ such that $x = \langle x_1, x_2 \rangle$ and $y = \langle y_1, y_2 \rangle$ holds $\rho^{X \times Y}(x, y) = \rho^{X \times Y}(y, x)$.

(7) For all elements x, y, z of $[\![$ the carrier of X, the carrier of $Y]\!]$ such that $x = \langle x_1, x_2 \rangle$ and $y = \langle y_1, y_2 \rangle$ and $z = \langle z_1, z_2 \rangle$ holds $\rho^{X \times Y}(x, z) \leq \rho^{X \times Y}(x, y) + \rho^{X \times Y}(y, z)$.

Let us consider X, Y, and let x, y be elements of $[\![$ the carrier of X, the carrier of $Y]\!]$. The functor $\rho(x, y)$ yielding a real number is defined as follows:

(Def.2) $\rho(x, y) = \rho^{X \times Y}(x, y)$.

We now state the proposition

(8) For all elements x, y of $[\![$ the carrier of X, the carrier of $Y]\!]$ holds $\rho(x, y) = \rho^{X \times Y}(x, y)$.

Let X, Y be metric spaces. The functor $[\![X, Y]\!]$ yields a metric space and is defined as follows:

(Def.3) $[\![X, Y]\!] = \langle [\![$ the carrier of X, the carrier of $Y]\!], \rho^{X \times Y} \rangle$.

One can prove the following proposition

(9) For every metric space X and for every metric space Y holds $\langle [\![$ the carrier of X, the carrier of $Y]\!], \rho^{X \times Y} \rangle$ is a metric space.

In the sequel Z will denote a metric space and x_3, y_3, z_3 will denote elements of the carrier of Z. The scheme *LambdaMCART1* deals with a non-empty set $\mathcal{A}$, a non-empty set $\mathcal{B}$, a non-empty set $\mathcal{C}$, a non-empty set $\mathcal{D}$, and a 6-ary functor $\mathcal{F}$ yielding an element of $\mathcal{D}$ and states that:

there exists a function f from $[\![[\![\mathcal{A}, \mathcal{B}, \mathcal{C}]\!], [\![\mathcal{A}, \mathcal{B}, \mathcal{C}]\!]]\!]$ into $\mathcal{D}$ such that for all elements x_1, y_1 of $\mathcal{A}$ and for all elements x_2, y_2 of $\mathcal{B}$ and for all elements x_3, y_3 of $\mathcal{C}$ and for all elements x, y of $[\![\mathcal{A}, \mathcal{B}, \mathcal{C}]\!]$ such that $x = \langle x_1, x_2, x_3 \rangle$ and $y = \langle y_1, y_2, y_3 \rangle$ holds $f(\langle x, y \rangle) = \mathcal{F}(x_1, y_1, x_2, y_2, x_3, y_3)$
for all values of the parameters.

[2]The proposition (4) was either repeated or obvious.

Let us consider X, Y, Z. The functor $\rho^{X \times Y \times Z}$ yielding a function from $[\!:[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]$, $[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]\,:\!]$ into $\mathbb{R}$ is defined by:

(Def.4) Let x_1, y_1 be elements of the carrier of X. Let x_2, y_2 be elements of the carrier of Y. Then for all elements x_3, y_3 of the carrier of Z and for all elements x, y of $[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]$ such that $x = \langle x_1, x_2, x_3 \rangle$ and $y = \langle y_1, y_2, y_3 \rangle$ holds $\rho^{X \times Y \times Z}(x, y) = \rho(x_1, y_1) + \rho(x_2, y_2) + \rho(x_3, y_3)$.

Next we state four propositions:

(10) Let X be a metric space. Let Y be a metric space. Let Z be a metric space. Let F be a function from $[\!:[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]$, $[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]\,:\!]$ into $\mathbb{R}$. Then $F = \rho^{X \times Y \times Z}$ if and only if for all elements x_1, y_1 of the carrier of X and for all elements x_2, y_2 of the carrier of Y and for all elements x_3, y_3 of the carrier of Z and for all elements x, y of $[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]$ such that $x = \langle x_1, x_2, x_3 \rangle$ and $y = \langle y_1, y_2, y_3 \rangle$ holds $F(x, y) = \rho(x_1, y_1) + \rho(x_2, y_2) + \rho(x_3, y_3)$.

(12)[3] For all elements x, y of $[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]$ such that $x = \langle x_1, x_2, x_3 \rangle$ and $y = \langle y_1, y_2, y_3 \rangle$ holds $\rho^{X \times Y \times Z}(x, y) = 0$ if and only if $x = y$.

(13) For all elements x, y of $[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]$ such that $x = \langle x_1, x_2, x_3 \rangle$ and $y = \langle y_1, y_2, y_3 \rangle$ holds $\rho^{X \times Y \times Z}(x, y) = \rho^{X \times Y \times Z}(y, x)$.

(14) Let x, y, z be elements of $[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]$. Then if $x = \langle x_1, x_2, x_3 \rangle$ and $y = \langle y_1, y_2, y_3 \rangle$ and $z = \langle z_1, z_2, z_3 \rangle$, then $\rho^{X \times Y \times Z}(x, z) \leq \rho^{X \times Y \times Z}(x, y) + \rho^{X \times Y \times Z}(y, z)$.

Let X, Y, Z be metric spaces. The functor $[\!:X, Y, Z\,:\!]$ yields a metric space and is defined by:

(Def.5) $[\!:X, Y, Z\,:\!] = \langle [\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!], \rho^{X \times Y \times Z} \rangle$.

Let us consider X, Y, Z, and let x, y be elements of $[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]$. The functor $\rho(x, y)$ yielding a real number is defined by:

(Def.6) $\rho(x, y) = \rho^{X \times Y \times Z}(x, y)$.

The following propositions are true:

(15) For all elements x, y of $[\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!]$ holds $\rho(x, y) = \rho^{X \times Y \times Z}(x, y)$.

(16) For every metric space X and for every metric space Y and for every metric space Z holds $\langle [\!:$ the carrier of X, the carrier of Y, the carrier of $Z\,:\!], \rho^{X \times Y \times Z} \rangle$ is a metric space.

[3] The proposition (11) was either repeated or obvious.

In the sequel W is a metric space and x_4, y_4, z_4 are elements of the carrier of W. The scheme *LambdaMCART2* deals with a non-empty set $\mathcal{A}$, a non-empty set $\mathcal{B}$, a non-empty set $\mathcal{C}$, a non-empty set $\mathcal{D}$, a non-empty set $\mathcal{E}$, and a 8-ary functor $\mathcal{F}$ yielding an element of $\mathcal{E}$ and states that:

there exists a function f from $[\![[\![\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}]\!], [\![\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}]\!]]\!]$ into $\mathcal{E}$ such that for all elements x_1, y_1 of $\mathcal{A}$ and for all elements x_2, y_2 of $\mathcal{B}$ and for all elements x_3, y_3 of $\mathcal{C}$ and for all elements x_4, y_4 of $\mathcal{D}$ and for all elements x, y of $[\![\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}]\!]$ such that $x = \langle x_1, x_2, x_3, x_4 \rangle$ and $y = \langle y_1, y_2, y_3, y_4 \rangle$ holds $f(\langle x, y \rangle) = \mathcal{F}(x_1, y_1, x_2, y_2, x_3, y_3, x_4, y_4)$
for all values of the parameters.

Let us consider X, Y, Z, W. The functor $\rho^{X \times Y \times Z \times W}$ yielding a function from $[\![[\![$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W]\!]$, $[\![$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W]\!]]\!]$ into $\mathbb{R}$ is defined as follows:

(Def.7) Let x_1, y_1 be elements of the carrier of X. Let x_2, y_2 be elements of the carrier of Y. Let x_3, y_3 be elements of the carrier of Z. Let x_4, y_4 be elements of the carrier of W. Then for all elements x, y of $[\![$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W]\!]$ such that $x = \langle x_1, x_2, x_3, x_4 \rangle$ and $y = \langle y_1, y_2, y_3, y_4 \rangle$ holds $\rho^{X \times Y \times Z \times W}(x, y) = \rho(x_1, y_1) + \rho(x_2, y_2) + (\rho(x_3, y_3) + \rho(x_4, y_4))$.

The following propositions are true:

(17) Let X be a metric space. Let Y be a metric space. Let Z be a metric space. Let W be a metric space. Let F be a function from $[\![[\![$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W]\!]$, $[\![$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W]\!]]\!]$ into $\mathbb{R}$. Then $F = \rho^{X \times Y \times Z \times W}$ if and only if for all elements x_1, y_1 of the carrier of X and for all elements x_2, y_2 of the carrier of Y and for all elements x_3, y_3 of the carrier of Z and for all elements x_4, y_4 of the carrier of W and for all elements x, y of $[\![$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W]\!]$ such that $x = \langle x_1, x_2, x_3, x_4 \rangle$ and $y = \langle y_1, y_2, y_3, y_4 \rangle$ holds $F(x, y) = \rho(x_1, y_1) + \rho(x_2, y_2) + (\rho(x_3, y_3) + \rho(x_4, y_4))$.

(19)[4] For all elements x, y of $[\![$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W]\!]$ such that $x = \langle x_1, x_2, x_3, x_4 \rangle$ and $y = \langle y_1, y_2, y_3, y_4 \rangle$ holds $\rho^{X \times Y \times Z \times W}(x, y) = 0$ if and only if $x = y$.

(20) For all elements x, y of $[\![$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W]\!]$ such that $x = \langle x_1, x_2, x_3, x_4 \rangle$ and $y = \langle y_1, y_2, y_3, y_4 \rangle$ holds $\rho^{X \times Y \times Z \times W}(x, y) = \rho^{X \times Y \times Z \times W}(y, x)$.

(21) Let x, y, z be elements of $[\![$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W]\!]$. Then if $x = \langle x_1, x_2, x_3, x_4 \rangle$ and $y = \langle y_1, y_2, y_3, y_4 \rangle$ and $z = \langle z_1, z_2, z_3, z_4 \rangle$, then $\rho^{X \times Y \times Z \times W}(x, z) \leq \rho^{X \times Y \times Z \times W}(x, y) + \rho^{X \times Y \times Z \times W}(y, z)$.

[4]The proposition (18) was either repeated or obvious.

Let X, Y, Z, W be metric spaces. The functor $[\!:X, Y, Z, W:\!]$ yielding a metric space is defined as follows:

(Def.8) $[\!:X, Y, Z, W:\!] = \langle [\!:$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W:\!], \rho^{X \times Y \times Z \times W} \rangle$.

Let us consider X, Y, Z, W, and let x, y be elements of $[\!:$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W:\!]$. The functor $\rho(x, y)$ yields a real number and is defined by:

(Def.9) $\rho(x, y) = \rho^{X \times Y \times Z \times W}(x,\, y)$.

One can prove the following propositions:

(22) For all elements x, y of $[\!:$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W:\!]$ holds $\rho(x, y) = \rho^{X \times Y \times Z \times W}(x,\, y)$.

(23) For every metric space X and for every metric space Y and for every metric space Z and for every metric space W holds $\langle [\!:$ the carrier of X, the carrier of Y, the carrier of Z, the carrier of $W:\!], \rho^{X \times Y \times Z \times W} \rangle$ is a metric space.

References

[1] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(**3**):537–541, 1990.

[2] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.

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

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

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

[6] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.

[7] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[8] Stanisława Kanas, Adam Lecko, and Mariusz Startek. Metric spaces. *Formalized Mathematics*, 1(**3**):607–610, 1990.

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

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

[11] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

[12] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

Received September 27, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Submetric Spaces - Part I [1]

Adam Lecko
Technical University of Rzeszów

Mariusz Startek
Technical University of Rzeszów

Summary. Definitions of pseudometric space, nonsymmetric metric space, semimetric space and ultrametric space are introduced. We find some relations between these spaces and prove that every ultrametric space is a metric space. We define the relation *is between*. Moreover we introduce the notions of the open segment and the closed segment.

MML Identifier: `SUB_METR`.

The terminology and notation used here are introduced in the following articles: [8], [2], [3], [1], [6], [4], [7], [9], and [5]. One can prove the following propositions:

(1) For all elements x, y of $\mathbb{R}$ such that $0 \leq x$ and $0 \leq y$ holds $\max(x, y) \leq x + y$.

(2) For every metric space M and for all elements x, y of the carrier of M such that $x \neq y$ holds $0 < \rho(x, y)$.

(3) For every element x of $\{\emptyset\}$ holds $x = \emptyset$.

(4) For all elements x, y of $\{\emptyset\}$ such that $x = y$ holds $\{[\emptyset, \emptyset]\} \mapsto 0(x,\, y) = 0$.

(5) For all elements x, y of $\{\emptyset\}$ such that $x \neq y$ holds $0 < \{[\emptyset, \emptyset]\} \mapsto 0(x,\, y)$.

(6) For all elements x, y of $\{\emptyset\}$ holds $\{[\emptyset, \emptyset]\} \mapsto 0(x,\, y) = \{[\emptyset, \emptyset]\} \mapsto 0(y,\, x)$.

(7) For all elements x, y, z of $\{\emptyset\}$ holds $\{[\emptyset, \emptyset]\} \mapsto 0(x,\, z) \leq \{[\emptyset, \emptyset]\} \mapsto 0(x,\, y) + \{[\emptyset, \emptyset]\} \mapsto 0(y,\, z)$.

(8) For all elements x, y, z of $\{\emptyset\}$ holds $\{[\emptyset, \emptyset]\} \mapsto 0(x,\, z) \leq \max(\{[\emptyset, \emptyset]\} \mapsto 0(x,\, y), \{[\emptyset, \emptyset]\} \mapsto 0(y,\, z))$.

A metric structure is called a pseudo metric space if:

(Def.1) for all elements a, b, c of the carrier of it holds if $a = b$, then $\rho(a, b) = 0$ but $\rho(a, b) = \rho(b, a)$ and $\rho(a, c) \leq \rho(a, b) + \rho(b, c)$.

Next we state four propositions:

[1]Supported by RPBP-III.24.B3

ISSN 0777–4028

(10)[2] For every pseudo metric space M and for all elements a, b of the carrier of M such that $a = b$ holds $\rho(a, b) = 0$.

(11) For every pseudo metric space M and for all elements a, b of the carrier of M holds $\rho(a, b) = \rho(b, a)$.

(12) For every pseudo metric space M and for all elements a, b, c of the carrier of M holds $\rho(a, c) \leq \rho(a, b) + \rho(b, c)$.

(13) For every pseudo metric space M and for all elements a, b of the carrier of M holds $0 \leq \rho(a, b)$.

A metric structure is said to be a semi metric space if:

(Def.2) for all elements a, b of the carrier of it holds if $a = b$, then $\rho(a, b) = 0$ but if $a \neq b$, then $0 < \rho(a, b)$ and $\rho(a, b) = \rho(b, a)$.

One can prove the following four propositions:

(15)[3] For every semi metric space M and for all elements a, b of the carrier of M such that $a = b$ holds $\rho(a, b) = 0$.

(16) For every semi metric space M and for all elements a, b of the carrier of M such that $a \neq b$ holds $0 < \rho(a, b)$.

(17) For every semi metric space M and for all elements a, b of the carrier of M holds $\rho(a, b) = \rho(b, a)$.

(18) For every semi metric space M and for all elements a, b of the carrier of M holds $0 \leq \rho(a, b)$.

A metric structure is called a non-symmetric metric space if:

(Def.3) for all elements a, b, c of the carrier of it holds if $a = b$, then $\rho(a, b) = 0$ but if $a \neq b$, then $0 < \rho(a, b)$ and $\rho(a, c) \leq \rho(a, b) + \rho(b, c)$.

One can prove the following four propositions:

(20)[4] For every non-symmetric metric space M and for all elements a, b of the carrier of M such that $a = b$ holds $\rho(a, b) = 0$.

(21) For every non-symmetric metric space M and for all elements a, b of the carrier of M such that $a \neq b$ holds $0 < \rho(a, b)$.

(22) For every non-symmetric metric space M and for all elements a, b, c of the carrier of M holds $\rho(a, c) \leq \rho(a, b) + \rho(b, c)$.

(23) For every non-symmetric metric space M and for all elements a, b of the carrier of M holds $0 \leq \rho(a, b)$.

A metric structure is said to be a ultra metric space if:

(Def.4) for all elements a, b, c of the carrier of it holds if $a = b$, then $\rho(a, b) = 0$ but if $a \neq b$, then $0 < \rho(a, b)$ and $\rho(a, b) = \rho(b, a)$ and $\rho(a, c) \leq \max(\rho(a, b), \rho(b, c))$.

We now state a number of propositions:

[2]The proposition (9) was either repeated or obvious.
[3]The proposition (14) was either repeated or obvious.
[4]The proposition (19) was either repeated or obvious.

(25)[5] For every ultra metric space M and for all elements a, b of the carrier of M such that $a = b$ holds $\rho(a, b) = 0$.

(26) For every ultra metric space M and for all elements a, b of the carrier of M such that $a \neq b$ holds $0 < \rho(a, b)$.

(27) For every ultra metric space M and for all elements a, b of the carrier of M holds $\rho(a, b) = \rho(b, a)$.

(28) For every ultra metric space M and for all elements a, b, c of the carrier of M holds $\rho(a, c) \leq \max(\rho(a, b), \rho(b, c))$.

(29) For every ultra metric space M and for all elements a, b of the carrier of M holds $0 \leq \rho(a, b)$.

(30) For every metric space M holds M is a pseudo metric space.

(31) For every metric space M holds M is a semi metric space.

(32) For every metric space M holds M is a non-symmetric metric space.

(33) For every ultra metric space M holds M is a metric space.

(34) For every ultra metric space M holds M is a pseudo metric space.

(35) For every ultra metric space M holds M is a semi metric space.

(36) For every ultra metric space M holds M is a non-symmetric metric space.

In the sequel x, y will be arbitrary. Let us consider x, y. Then $\{x, y\}$ is a non-empty set.

The function $(2^2 \rightarrow 0)$ from $[\!:\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}:\!]$ into $\mathbb{R}$ is defined by:

(Def.5) $(2^2 \rightarrow 0) = [\!:\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}:\!] \longmapsto 0$.

Next we state several propositions:

(37) $(2^2 \rightarrow 0) = [\!:\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}:\!] \longmapsto 0$.

(38) For every element x of $\{\emptyset, \{\emptyset\}\}$ holds $x = \emptyset$ or $x = \{\emptyset\}$.

(39) (i) $\langle\emptyset, \emptyset\rangle \in [\!:\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}:\!]$,
(ii) $\langle\emptyset, \{\emptyset\}\rangle \in [\!:\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}:\!]$,
(iii) $\langle\{\emptyset\}, \emptyset\rangle \in [\!:\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}:\!]$,
(iv) $\langle\{\emptyset\}, \{\emptyset\}\rangle \in [\!:\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}:\!]$.

(40) For all elements x, y of $\{\emptyset, \{\emptyset\}\}$ holds $(2^2 \rightarrow 0)(x, y) = 0$.

(41) For all elements x, y of $\{\emptyset, \{\emptyset\}\}$ such that $x = y$ holds $(2^2 \rightarrow 0)(x, y) = 0$.

(42) For all elements x, y of $\{\emptyset, \{\emptyset\}\}$ holds $(2^2 \rightarrow 0)(x, y) = (2^2 \rightarrow 0)(y, x)$.

(43) For all elements x, y, z of $\{\emptyset, \{\emptyset\}\}$ holds $(2^2 \rightarrow 0)(x, z) \leq (2^2 \rightarrow 0)(x, y) + (2^2 \rightarrow 0)(y, z)$.

The pseudo metric space $\ominus$ is defined as follows:

(Def.6) $\ominus = \langle\{\emptyset, \{\emptyset\}\}, (2^2 \rightarrow 0)\rangle$.

The following proposition is true

(44) $\ominus = \langle\{\emptyset, \{\emptyset\}\}, (2^2 \rightarrow 0)\rangle$.

[5]The proposition (24) was either repeated or obvious.

Let S be a metric space, and let p, q, r be elements of the carrier of S. We say that q is between p and r if and only if:

(Def.7) $p \neq q$ and $p \neq r$ and $q \neq r$ and $\rho(p,r) = \rho(p,q) + \rho(q,r)$.

Next we state three propositions:

(47)[6] For every metric space S and for all elements p, q, r of the carrier of S such that q is between p and r holds q is between r and p.

(48) For every metric space S and for all elements p, q, r of the carrier of S such that q is between p and r holds p is not between q and r and r is not between p and q.

(49) For every metric space S and for all elements p, q, r, s of the carrier of S such that q is between p and r and r is between p and s holds q is between p and s and r is between q and s.

Let M be a metric space, and let p, r be elements of the carrier of M. The functor $\mathrm{IntSeg}(p,r)$ yielding a subset of the carrier of M is defined as follows:

(Def.8) $\mathrm{IntSeg}(p,r) = \{q : q$ is between p and $r\}$, where q ranges over elements of the carrier of M.

One can prove the following two propositions:

(50) For every metric space M and for all elements p, r of the carrier of M holds $\mathrm{IntSeg}(p,r) = \{q : q$ is between p and $r\}$, where q ranges over elements of the carrier of M.

(51) For every metric space M and for all elements p, r, x of the carrier of M holds $x \in \mathrm{IntSeg}(p,r)$ if and only if x is between p and r.

Let M be a metric space, and let p, r be elements of the carrier of M. The functor $\mathrm{ClSeg}(p,r)$ yielding a subset of the carrier of M is defined by:

(Def.9) $\mathrm{ClSeg}(p,r) = \{q : q$ is between p and $r\} \cup \{p,r\}$, where q ranges over elements of the carrier of M.

We now state three propositions:

(52) For every metric space M and for all elements p, r of the carrier of M holds $\mathrm{ClSeg}(p,r) = \{q : q$ is between p and $r\} \cup \{p,r\}$, where q ranges over elements of the carrier of M.

(53) For every metric space M and for all elements p, r, x of the carrier of M holds $x \in \mathrm{ClSeg}(p,r)$ if and only if x is between p and r or $x = p$ or $x = r$.

(54) For every metric space M and for all elements p, r of the carrier of M holds $\mathrm{IntSeg}(p,r) \subseteq \mathrm{ClSeg}(p,r)$.

References

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

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

[6] The propositions (45)–(46) were either repeated or obvious.

[3] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[4] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[5] Stanisława Kanas, Adam Lecko, and Mariusz Startek. Metric spaces. *Formalized Mathematics*, 1(**3**):607–610, 1990.
[6] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[7] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[9] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

Received September 27, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

On Pseudometric Spaces [1]

Adam Lecko
Technical University of Rzeszów

Mariusz Startek
Technical University of Rzeszów

Summary. We introduce the equivalence classes in a pseudometric space. Next we prove that the set of the equivalence classes forms the metric space with the special metric defined in the article.

MML Identifier: `METRIC_2`.

The terminology and notation used here have been introduced in the following articles: [9], [4], [13], [12], [10], [8], [2], [3], [1], [14], [7], [11], [5], and [6]. Let M be a metric structure, and let x, y be elements of the carrier of M. The predicate $x \approx y$ is defined by:

(Def.1) $\rho(x, y) = 0$.

Let M be a metric structure, and let x be an element of the carrier of M. The functor $x^{\Box}$ yielding a subset of the carrier of M is defined as follows:

(Def.2) $x^{\Box} = \{y : x \approx y\}$, where y ranges over elements of the carrier of M.

One can prove the following proposition

(2)[2] For every M being a metric structure and for every element x of the carrier of M holds $x^{\Box} = \{y : x \approx y\}$, where y ranges over elements of the carrier of M.

Let M be a metric structure. A subset of the carrier of M is called a $\Box$-equivalence class of M if:

(Def.3) there exists an element x of the carrier of M such that it $= x^{\Box}$.

Next we state a number of propositions:

(4)[3] For every pseudo metric space M and for every element x of the carrier of M holds $x \approx x$.

(5) For every pseudo metric space M and for all elements x, y of the carrier of M such that $x \approx y$ holds $y \approx x$.

---

[1]Supported by RPBP-III.24.B3
[2]The proposition (1) was either repeated or obvious.
[3]The proposition (3) was either repeated or obvious.

ISSN 0777–4028

(6) For every pseudo metric space M and for all elements x, y, z of the carrier of M such that $x \approx y$ and $y \approx z$ holds $x \approx z$.

(7) For every pseudo metric space M and for all elements x, y of the carrier of M holds $y \in x^{\square}$ if and only if $y \approx x$.

(8) For every pseudo metric space M and for all elements x, p, q of the carrier of M such that $p \in x^{\square}$ and $q \in x^{\square}$ holds $p \approx q$.

(9) For every pseudo metric space M and for every element x of the carrier of M holds $x \in x^{\square}$.

(10) For every pseudo metric space M and for all elements x, y of the carrier of M holds $x \in y^{\square}$ if and only if $y \in x^{\square}$.

(11) For every pseudo metric space M and for all elements p, x, y of the carrier of M such that $p \in x^{\square}$ and $x \approx y$ holds $p \in y^{\square}$.

(12) For every pseudo metric space M and for all elements x, y of the carrier of M such that $y \in x^{\square}$ holds $x^{\square} = y^{\square}$.

(13) For every pseudo metric space M and for all elements x, y of the carrier of M holds $x^{\square} = y^{\square}$ if and only if $x \approx y$.

The following propositions are true:

(14) For every pseudo metric space M and for all elements x, y of the carrier of M holds $x^{\square} \cap y^{\square} \neq \emptyset$ if and only if $x \approx y$.

(15) For every pseudo metric space M and for every element x of the carrier of M holds $x^{\square}$ is a non-empty set.

(16) For every pseudo metric space M and for every $\square$-equivalence class V of M holds V is a non-empty set.

(17) For every pseudo metric space M and for all elements x, p, q of the carrier of M such that $p \in x^{\square}$ and $q \in x^{\square}$ holds $\rho(p, q) = 0$.

(18) For every metric space M and for all elements x, y of the carrier of M holds $x \approx y$ if and only if $x = y$.

(19) For every metric space M and for all elements x, y of the carrier of M holds $y \in x^{\square}$ if and only if $y = x$.

One can prove the following two propositions:

(20) For every metric space M and for every element x of the carrier of M holds $x^{\square} = \{x\}$.

(21) For every metric space M and for every subset V of the carrier of M holds V is a $\square$-equivalence class of M if and only if there exists an element x of the carrier of M such that $V = \{x\}$.

Let M be a metric structure. The functor $M^{\square}$ yields a non-empty set and is defined by:

(Def.4) $M^{\square} = \{s : \bigvee_x x^{\square} = s\}$, where s ranges over elements of $2^{\text{the carrier of } M}$, and x ranges over elements of the carrier of M.

One can prove the following proposition

(22) For every M being a metric structure holds $M^{\square} = \{s : \bigvee_x x^{\square} = s\}$, where s ranges over elements of $2^{\text{the carrier of } M}$, and x ranges over elements of the carrier of M.

In the sequel V is arbitrary. The following two propositions are true:

(23) For every M being a metric structure holds $V \in M^{\square}$ if and only if there exists an element x of the carrier of M such that $V = x^{\square}$.

(24) For every M being a metric structure and for every element x of the carrier of M holds $x^{\square} \in M^{\square}$.

We now state the proposition

(26)[4] For every M being a metric structure holds $V \in M^{\square}$ if and only if V is a $\square$-equivalence class of M.

We now state three propositions:

(27) For every metric space M and for every element x of the carrier of M holds $\{x\} \in M^{\square}$.

(28) For every metric space M holds $V \in M^{\square}$ if and only if there exists an element x of the carrier of M such that $V = \{x\}$.

(29) For every pseudo metric space M and for all elements V, Q of $M^{\square}$ and for all elements p_1, p_2, q_1, q_2 of the carrier of M such that $p_1 \in V$ and $q_1 \in Q$ and $p_2 \in V$ and $q_2 \in Q$ holds $\rho(p_1, q_1) = \rho(p_2, q_2)$.

Let M be a pseudo metric space, and let V, Q be elements of $M^{\square}$, and let v be an element of $\mathbb{R}$. We say that the distance between V and Q is v if and only if:

(Def.5) for all elements p, q of the carrier of M such that $p \in V$ and $q \in Q$ holds $\rho(p, q) = v$.

We now state two propositions:

(31)[5] For every pseudo metric space M and for all elements V, Q of $M^{\square}$ and for every element v of $\mathbb{R}$ holds the distance between V and Q is v if and only if there exist elements p, q of the carrier of M such that $p \in V$ and $q \in Q$ and $\rho(p, q) = v$.

(32) For every pseudo metric space M and for all elements V, Q of $M^{\square}$ and for every element v of $\mathbb{R}$ holds the distance between V and Q is v if and only if the distance between Q and V is v.

Let M be a pseudo metric space, and let V, Q be elements of $M^{\square}$. The functor $\rho^{\circ}(V, Q)$ yields a subset of $\mathbb{R}$ and is defined as follows:

(Def.6) $\rho^{\circ}(V, Q) = \{v :$ the distance between V and Q is $v\}$, where v ranges over elements of $\mathbb{R}$.

The following two propositions are true:

[4] The proposition (25) was either repeated or obvious.
[5] The proposition (30) was either repeated or obvious.

(33) For every pseudo metric space M and for all elements V, Q of $M^{\square}$ holds $\rho^{\circ}(V,Q) = \{v :$ the distance between V and Q is v $\}$, where v ranges over elements of $\mathbb{R}$.

(34) For every pseudo metric space M and for all elements V, Q of $M^{\square}$ and for every element v of $\mathbb{R}$ holds $v \in \rho^{\circ}(V,Q)$ if and only if the distance between V and Q is v.

Let M be a pseudo metric space, and let v be an element of $\mathbb{R}$. The functor $\rho_M^{\square\,-1}(v)$ yields a subset of $[\!: M^{\square}, M^{\square} :\!]$ and is defined as follows:

(Def.7) $\rho_M^{\square\,-1}(v) = \{W : \bigvee_{V,Q}[W = \langle V, Q\rangle \wedge$ the distance between V and Q is v $]\}$, where W ranges over elements of $[\!: M^{\square}, M^{\square} :\!]$, and V, Q range over elements of $M^{\square}$.

One can prove the following two propositions:

(35) For every pseudo metric space M and for every element v of $\mathbb{R}$ holds $\rho_M^{\square\,-1}(v) = \{W : \bigvee_{V,Q}[W = \langle V, Q\rangle \wedge$ the distance between V and Q is v $]\}$, where W ranges over elements of $[\!: M^{\square}, M^{\square} :\!]$, and V, Q range over elements of $M^{\square}$.

(36) For every pseudo metric space M and for every element v of $\mathbb{R}$ and for every element W of $[\!: M^{\square}, M^{\square} :\!]$ holds $W \in \rho_M^{\square\,-1}(v)$ if and only if there exist elements V, Q of $M^{\square}$ such that $W = \langle V, Q\rangle$ and the distance between V and Q is v.

Let M be a pseudo metric space. The functor $\rho^{\circ}(M^{\square}, M^{\square})$ yields a subset of $\mathbb{R}$ and is defined by:

(Def.8) $\rho^{\circ}(M^{\square}, M^{\square}) = \{v : \bigvee_{V,Q}$ the distance between V and Q is v $\}$, where v ranges over elements of $\mathbb{R}$, and V, Q range over elements of $M^{\square}$.

The following two propositions are true:

(37) For every pseudo metric space M holds $\rho^{\circ}(M^{\square}, M^{\square}) = \{v : \bigvee_{V,Q}$ the distance between V and Q is v $\}$, where v ranges over elements of $\mathbb{R}$, and V, Q range over elements of $M^{\square}$.

(38) For every pseudo metric space M and for every element v of $\mathbb{R}$ holds $v \in \rho^{\circ}(M^{\square}, M^{\square})$ if and only if there exist elements V, Q of $M^{\square}$ such that the distance between V and Q is v.

Let M be a pseudo metric space. The functor $\mathrm{dom}_1\, \rho_M^{\square}$ yields a subset of $M^{\square}$ and is defined as follows:

(Def.9) $\mathrm{dom}_1\, \rho_M^{\square} = \{V : \bigvee_Q \bigvee_v$ the distance between V and Q is v $\}$, where V ranges over elements of $M^{\square}$, and Q ranges over elements of $M^{\square}$, and v ranges over elements of $\mathbb{R}$.

We now state two propositions:

(39) For every pseudo metric space M holds $\mathrm{dom}_1\, \rho_M^{\square} = \{V : \bigvee_Q \bigvee_v$ the distance between V and Q is v $\}$, where V ranges over elements of $M^{\square}$, and Q ranges over elements of $M^{\square}$, and v ranges over elements of $\mathbb{R}$.

(40) For every pseudo metric space M and for every element V of $M^\square$ holds $V \in \mathrm{dom}_1\, \rho^\square_M$ if and only if there exists an element Q of $M^\square$ and there exists an element v of $\mathbb{R}$ such that the distance between V and Q is v.

Let M be a pseudo metric space. The functor $\mathrm{dom}_2\, \rho^\square_M$ yields a subset of $M^\square$ and is defined by:

(Def.10) $\mathrm{dom}_2\, \rho^\square_M = \{Q : \bigvee_V \bigvee_v$ the distance between V and Q is v $\}$, where Q ranges over elements of $M^\square$, and V ranges over elements of $M^\square$, and v ranges over elements of $\mathbb{R}$.

One can prove the following two propositions:

(41) For every pseudo metric space M holds $\mathrm{dom}_2\, \rho^\square_M = \{Q : \bigvee_V \bigvee_v$ the distance between V and Q is v $\}$, where Q ranges over elements of $M^\square$, and V ranges over elements of $M^\square$, and v ranges over elements of $\mathbb{R}$.

(42) For every pseudo metric space M and for every element Q of $M^\square$ holds $Q \in \mathrm{dom}_2\, \rho^\square_M$ if and only if there exists an element V of $M^\square$ and there exists an element v of $\mathbb{R}$ such that the distance between V and Q is v.

Let M be a pseudo metric space. The functor $\mathrm{dom}\, \rho^\square_M$ yielding a subset of $[\!: M^\square, M^\square :\!]$ is defined as follows:

(Def.11) $\mathrm{dom}\, \rho^\square_M = \{V_1 : \bigvee_{V,Q} \bigvee_v [V_1 = \langle V, Q\rangle \wedge$ the distance between V and Q is v $]\}$, where V_1 ranges over elements of $[\!: M^\square, M^\square :\!]$, and V, Q range over elements of $M^\square$, and v ranges over elements of $\mathbb{R}$.

We now state two propositions:

(43) For every pseudo metric space M holds $\mathrm{dom}\, \rho^\square_M = \{V_1 : \bigvee_{V,Q} \bigvee_v [V_1 = \langle V, Q\rangle \wedge$ the distance between V and Q is v $]\}$, where V_1 ranges over elements of $[\!: M^\square, M^\square :\!]$, and V, Q range over elements of $M^\square$, and v ranges over elements of $\mathbb{R}$.

(44) For every pseudo metric space M and for every element V_1 of $[\!: M^\square, M^\square :\!]$ holds $V_1 \in \mathrm{dom}\, \rho^\square_M$ if and only if there exist elements V, Q of $M^\square$ and there exists an element v of $\mathbb{R}$ such that $V_1 = \langle V, Q\rangle$ and the distance between V and Q is v.

Let M be a pseudo metric space. The functor $\mathrm{graph}\, \rho^\square_M$ yielding a subset of $[\!: M^\square, M^\square, \mathbb{R} :\!]$ is defined by:

(Def.12) $\mathrm{graph}\, \rho^\square_M = \{V_2 : \bigvee_{V,Q} \bigvee_v [V_2 = \langle V, Q, v\rangle \wedge$ the distance between V and Q is v $]\}$, where V_2 ranges over elements of $[\!: M^\square, M^\square, \mathbb{R} :\!]$, and V, Q range over elements of $M^\square$, and v ranges over elements of $\mathbb{R}$.

The following propositions are true:

(45) For every pseudo metric space M holds $\mathrm{graph}\, \rho^\square_M = \{V_2 : \bigvee_{V,Q} \bigvee_v [V_2 = \langle V, Q, v\rangle \wedge$ the distance between V and Q is v $]\}$, where V_2 ranges over elements of $[\!: M^\square, M^\square, \mathbb{R} :\!]$, and V, Q range over elements of $M^\square$, and v ranges over elements of $\mathbb{R}$.

(46) For every pseudo metric space M and for every element V_2 of $[\!: M^\square, M^\square, \mathbb{R} :\!]$ holds $V_2 \in \mathrm{graph}\, \rho^\square_M$ if and only if there exist elements V, Q of

$M^{\square}$ and there exists an element v of $\mathbb{R}$ such that $V_2 = \langle V, Q, v \rangle$ and the distance between V and Q is v.

(47) For every pseudo metric space M holds $\mathrm{dom}_1\, \rho^{\square}_{M} = \mathrm{dom}_2\, \rho^{\square}_{M}$.

(48) For every pseudo metric space M holds graph $\rho^{\square}_{M} \subseteq [\!:\mathrm{dom}_1\, \rho^{\square}_{M}, \mathrm{dom}_2\, \rho^{\square}_{M}, \rho^{\circ}(M^{\square}, M^{\square}):\!]$.

(49) Let M be a pseudo metric space. Then for all elements V, Q of $M^{\square}$ and for all elements p_1, q_1, p_2, q_2 of the carrier of M and for all elements v_1, v_2 of $\mathbb{R}$ such that $p_1 \in V$ and $q_1 \in Q$ and $\rho(p_1, q_1) = v_1$ and $p_2 \in V$ and $q_2 \in Q$ and $\rho(p_2, q_2) = v_2$ holds $v_1 = v_2$.

The following two propositions are true:

(50) For every pseudo metric space M and for all elements V, Q of $M^{\square}$ and for all elements v_1, v_2 of $\mathbb{R}$ such that the distance between V and Q is v_1 and the distance between V and Q is v_2 holds $v_1 = v_2$.

(52)[6] For every pseudo metric space M and for every elements V, Q of $M^{\square}$ there exists an element v of $\mathbb{R}$ such that the distance between V and Q is v.

Let M be a pseudo metric space. The functor $\rho^{\square}_{M}$ yielding a function from $[\!:M^{\square}, M^{\square}:\!]$ into $\mathbb{R}$ is defined as follows:

(Def.13) for all elements V, Q of $M^{\square}$ and for all elements p, q of the carrier of M such that $p \in V$ and $q \in Q$ holds $\rho^{\square}_{M}(V, Q) = \rho(p, q)$.

One can prove the following propositions:

(53) For every pseudo metric space M and for every function F from $[\!:M^{\square}, M^{\square}:\!]$ into $\mathbb{R}$ holds $F = \rho^{\square}_{M}$ if and only if for all elements V, Q of $M^{\square}$ and for all elements p, q of the carrier of M such that $p \in V$ and $q \in Q$ holds $F(V, Q) = \rho(p, q)$.

(54) For every pseudo metric space M and for all elements V, Q of $M^{\square}$ holds $\rho^{\square}_{M}(V, Q) = 0$ if and only if $V = Q$.

(55) For every pseudo metric space M and for all elements V, Q of $M^{\square}$ holds $\rho^{\square}_{M}(V, Q) = \rho^{\square}_{M}(Q, V)$.

(56) For every pseudo metric space M and for all elements V, Q, W of $M^{\square}$ holds $\rho^{\square}_{M}(V, W) \leq \rho^{\square}_{M}(V, Q) + \rho^{\square}_{M}(Q, W)$.

Let M be a pseudo metric space. The functor $M_{/\square}$ yields a metric space and is defined as follows:

(Def.14) $M_{/\square} = \langle M^{\square}, \rho^{\square}_{M} \rangle$.

We now state the proposition

(57) For every pseudo metric space M holds $M_{/\square} = \langle M^{\square}, \rho^{\square}_{M} \rangle$.

References

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

[6] The proposition (51) was either repeated or obvious.

[2] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[3] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[4] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[5] Stanisława Kanas, Adam Lecko, and Mariusz Startek. Metric spaces. *Formalized Mathematics*, 1(**3**):607–610, 1990.
[6] Adam Lecko and Mariusz Startek. Submetric spaces - part I. *Formalized Mathematics*, 2(**2**):199–203, 1991.
[7] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[8] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[9] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[10] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[11] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[12] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[13] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[14] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received September 28, 1990

FORMALIZED MATHEMATICS
Vol.2, No.2, March–April 1991
Université Catholique de Louvain

Real Exponents and Logarithms [1]

Konrad Raczkowski
Warsaw University
Białystok

Andrzej Nędzusiak
Warsaw University
Białystok

Summary. Definitions and properties of the following concepts: root, real exponent and logarithm. Also the number e is defined.

MML Identifier: `POWER`.

The papers [11], [2], [9], [1], [7], [5], [6], [13], [12], [4], [3], [8], and [10] provide the notation and terminology for this paper. For simplicity we follow the rules: a, b, c, d denote real numbers, m, n, m_1, m_2 denote natural numbers, k, l denote integers, and p denotes a rational number. One can prove the following propositions:

(1) If there exists m such that $n = 2 \cdot m$, then $(-a)^n_{\mathbb{N}} = a^n_{\mathbb{N}}$.

(2) If there exists m such that $n = 2 \cdot m + 1$, then $(-a)^n_{\mathbb{N}} = -a^n_{\mathbb{N}}$.

(3) If $a \geq 0$ or there exists m such that $n = 2 \cdot m$, then $a^n_{\mathbb{N}} \geq 0$.

Let us consider n, a. The functor $\sqrt[n]{a}$ yields a real number and is defined by:

(Def.1) (i) $\sqrt[n]{a} = \mathrm{root}_n(a)$ if $a \geq 0$ and $n \geq 1$,

(ii) $\sqrt[n]{a} = -\mathrm{root}_n(-a)$ if $a < 0$ and there exists m such that $n = 2 \cdot m + 1$.

One can prove the following propositions:

(4) For all a, n holds if $a \geq 0$ and $n \geq 1$, then $\sqrt[n]{a} = \mathrm{root}_n(a)$ but if $a < 0$ and there exists m such that $n = 2 \cdot m + 1$, then $\sqrt[n]{a} = -\mathrm{root}_n(-a)$.

(5) If $n \geq 1$ and $a \geq 0$ or there exists m such that $n = 2 \cdot m + 1$, then $\sqrt[n]{a^n_{\mathbb{N}}} = a$ and $\sqrt[n]{a}^n_{\mathbb{N}} = a$.

(6) If $n \geq 1$, then $\sqrt[n]{0} = 0$.

(7) If $n \geq 1$, then $\sqrt[n]{1} = 1$.

(8) If $a \geq 0$ and $n \geq 1$, then $\sqrt[n]{a} \geq 0$.

(9) If there exists m such that $n = 2 \cdot m + 1$, then $\sqrt[n]{-1} = -1$.

(10) $\sqrt[1]{a} = a$.

[1] Supported by RPBP-III.24.C8

ISSN 0777–4028

(11) If there exists m such that $n = 2 \cdot m + 1$, then $\sqrt[n]{a} = -\sqrt[n]{-a}$.

(12) If $n \geq 1$ and $a \geq 0$ and $b \geq 0$ or there exists m such that $n = 2 \cdot m + 1$, then $\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$.

(13) If $a > 0$ and $n \geq 1$ or $a \neq 0$ and there exists m such that $n = 2 \cdot m + 1$, then $\sqrt[n]{\frac{1}{a}} = \frac{1}{\sqrt[n]{a}}$.

(14) If $a \geq 0$ and $b > 0$ and $n \geq 1$ or $b \neq 0$ and there exists m such that $n = 2 \cdot m + 1$, then $\sqrt[n]{\frac{a}{b}} = \frac{\sqrt[n]{a}}{\sqrt[n]{b}}$.

(15) If $a \geq 0$ and $n \geq 1$ and $m \geq 1$ or there exist m_1, m_2 such that $n = 2 \cdot m_1 + 1$ and $m = 2 \cdot m_2 + 1$, then $\sqrt[n]{\sqrt[m]{a}} = \sqrt[n \cdot m]{a}$.

(16) If $a \geq 0$ and $n \geq 1$ and $m \geq 1$ or there exist m_1, m_2 such that $n = 2 \cdot m_1 + 1$ and $m = 2 \cdot m_2 + 1$, then $\sqrt[n]{a} \cdot \sqrt[m]{a} = \sqrt[n \cdot m]{a_{\mathbb{N}}^{n+m}}$.

(17) If $a \leq b$ but $0 \leq a$ and $n \geq 1$ or there exists m such that $n = 2 \cdot m + 1$, then $\sqrt[n]{a} \leq \sqrt[n]{b}$.

(18) If $a < b$ but $a \geq 0$ and $n \geq 1$ or there exists m such that $n = 2 \cdot m + 1$, then $\sqrt[n]{a} < \sqrt[n]{b}$.

(19) If $a \geq 1$ and $n \geq 1$, then $\sqrt[n]{a} \geq 1$ and $a \geq \sqrt[n]{a}$.

(20) If $a \leq -1$ and there exists m such that $n = 2 \cdot m + 1$, then $\sqrt[n]{a} \leq -1$ and $a \leq \sqrt[n]{a}$.

(21) If $a \geq 0$ and $a < 1$ and $n \geq 1$, then $a \leq \sqrt[n]{a}$ and $\sqrt[n]{a} < 1$.

(22) If $a > -1$ and $a \leq 0$ and there exists m such that $n = 2 \cdot m + 1$, then $a \geq \sqrt[n]{a}$ and $\sqrt[n]{a} > -1$.

(23) If $a > 0$ and $n \geq 1$, then $\sqrt[n]{a} - 1 \leq \frac{a-1}{n}$.

(24) For every sequence of real numbers s and for every a such that $a > 0$ and for every n such that $n \geq 1$ holds $s(n) = \sqrt[n]{a}$ holds s is convergent and $\lim s = 1$.

Let us consider a, b. The functor a^b yielding a real number is defined as follows:

(Def.2) (i) $a^b = a_{\mathbb{R}}^b$ if $a > 0$,

(ii) $a^b = 0$ if $a = 0$ and $b > 0$,

(iii) there exists k such that $k = b$ and $a^b = a_{\mathbb{Z}}^k$ if $a < 0$ and b is an integer.

One can prove the following propositions:

(25) Given a, b. Then if $a > 0$, then $a^b = a_{\mathbb{R}}^b$ but if $a = 0$ and $b > 0$, then $a^b = 0$ but if $a < 0$ and b is an integer, then there exists k such that $k = b$ and $a^b = a_{\mathbb{Z}}^k$.

(26) If $a > 0$, then $a^b = a_{\mathbb{R}}^b$.

(27) If $b > 0$, then $0^b = 0$.

(28) If $a < 0$, then $a^k = a_{\mathbb{Z}}^k$.

(29) If $a \neq 0$, then $a^0 = 1$.

(30) $a^1 = a$.

(31) $1^a = 1$.

(32) If $a > 0$, then $a^{b+c} = a^b \cdot a^c$.

(33) If $a > 0$, then $a^{-c} = \frac{1}{a^c}$.

(34) If $a > 0$, then $a^{b-c} = \frac{a^b}{a^c}$.

(35) If $a > 0$ and $b > 0$, then $(a \cdot b)^c = a^c \cdot b^c$.

(36) If $a > 0$ and $b > 0$, then $\frac{a}{b}^c = \frac{a^c}{b^c}$.

(37) If $a > 0$, then $\frac{1}{a}^b = a^{-b}$.

(38) If $a > 0$, then $(a^b)^c = a^{b \cdot c}$.

(39) If $a > 0$, then $a^b > 0$.

(40) If $a > 1$ and $b > 0$, then $a^b > 1$.

(41) If $a > 1$ and $b < 0$, then $a^b < 1$.

(42) If $a > 0$ and $a < b$ and $c > 0$, then $a^c < b^c$.

(43) If $a > 0$ and $a < b$ and $c < 0$, then $a^c > b^c$.

(44) If $a < b$ and $c > 1$, then $c^a < c^b$.

(45) If $a < b$ and $c > 0$ and $c < 1$, then $c^a > c^b$.

(46) If $a \neq 0$, then $a^n = a^n_{\mathbb{N}}$.

(47) If $n \geq 1$, then $a^n = a^n_{\mathbb{N}}$.

(48) If $a \neq 0$, then $a^n = a^n$.

(49) If $n \geq 1$, then $a^n = a^n$.

(50) If $a \neq 0$, then $a^k = a^k_{\mathbb{Z}}$.

(51) If $a > 0$, then $a^p = a^p_{\mathbb{Q}}$.

(52) If $a \geq 0$ and $n \geq 1$, then $a^{\frac{1}{n}} = \sqrt[n]{a}$.

(53) $a^2 = a^{\mathbf{2}}$.

(54) If $a \neq 0$ and there exists l such that $k = 2 \cdot l$, then $(-a)^k = a^k$.

(55) If $a \neq 0$ and there exists l such that $k = 2 \cdot l + 1$, then $(-a)^k = -a^k$.

Next we state two propositions:

(56) If $-1 < a$, then $(1 + a)^n \geq 1 + n \cdot a$.

(57) If $a > 0$ and $a \neq 1$ and $c \neq d$, then $a^c \neq a^d$.

Let us consider a, b. Let us assume that $a > 0$ and $a \neq 1$ and $b > 0$. The functor $\log_a b$ yields a real number and is defined by:

(Def.3) $a^{\log_a b} = b$.

The following propositions are true:

(58) For all a, b, c such that $a > 0$ and $a \neq 1$ and $b > 0$ holds $c = \log_a b$ if and only if $a^c = b$.

(59) If $a > 0$ and $a \neq 1$, then $\log_a 1 = 0$.

(60) If $a > 0$ and $a \neq 1$, then $\log_a a = 1$.

(61) If $a > 0$ and $a \neq 1$ and $b > 0$ and $c > 0$, then $\log_a b + \log_a c = \log_a (b \cdot c)$.

(62) If $a > 0$ and $a \neq 1$ and $b > 0$ and $c > 0$, then $\log_a b - \log_a c = \log_a \frac{b}{c}$.

(63) If $a > 0$ and $a \neq 1$ and $b > 0$, then $\log_a(b^c) = c \cdot \log_a b$.

(64) If $a > 0$ and $a \neq 1$ and $b > 0$ and $b \neq 1$ and $c > 0$, then $\log_a c = \log_a b \cdot \log_b c$.

(65) If $a > 1$ and $b > 0$ and $c > b$, then $\log_a c > \log_a b$.

(66) If $a > 0$ and $a < 1$ and $b > 0$ and $c > b$, then $\log_a c < \log_a b$.

(67) For every sequence of real numbers s such that for every n holds $s(n) = (1 + \frac{1}{n+1})^{n+1}$ holds s is convergent.

The real number e is defined as follows:

(Def.4) for every sequence of real numbers s such that for every n holds $s(n) = (1 + \frac{1}{n+1})^{n+1}$ holds $e = \lim s$.

References

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

[2] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

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

[4] Jarosław Kotowicz. Convergent real sequences. Upper and lower bound of sets of real numbers. *Formalized Mathematics*, 1(**3**):477–481, 1990.

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

[6] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.

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

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

[9] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

[10] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

[11] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

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

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

Received October 1, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Hessenberg Theorem [1]

Eugeniusz Kusak
Warsaw University
Białystok

Wojciech Leończuk
Warsaw University
Białystok

Summary. We prove the Hessenberg theorem which states that every Pappian projective space is Desarguesian.

MML Identifier: `HESSENBE`.

The terminology and notation used in this paper are introduced in the following articles: [7], [1], [2], [3], [4], [5], and [6]. We follow a convention: P_1 denotes a projective space defined in terms of collinearity and a, a', a_1, a_2, a_3, b, b', b_1, b_2, c, c', c_1, c_3, d, d', e, o, p, p_1, p_2, p_3, q, q_1, q_2, q_3, r, s, x, y, z denote elements of the points of P_1. One can prove the following propositions:

(1) If a, b and c are collinear, then b, a and c are collinear.

(2) If a, b and c are collinear, then a, c and b are collinear.

(3) If a, b and c are collinear, then b, c and a are collinear and c, a and b are collinear and b, a and c are collinear and a, c and b are collinear and c, b and a are collinear.

(4) If $a \neq b$ and a, b and c are collinear and a, b and d are collinear, then a, c and d are collinear.

(5) If $p \neq q$ and a, b and p are collinear and a, b and q are collinear and p, q and r are collinear, then a, b and r are collinear.

(6) If $p \neq q$, then there exists r such that p, q and r are not collinear.

(7) There exist q, r such that p, q and r are not collinear.

(8) If a, b and c are not collinear and a, b and b' are collinear and $a \neq b'$, then a, b' and c are not collinear.

(9) If a, b and c are not collinear and a, b and d are collinear and a, c and d are collinear, then $a = d$.

[1]Supported by RPBP.III-24.C6

ISSN 0777–4028

(10) If o, a and d are not collinear and o, d and d' are collinear and a, d and s are collinear and $d \neq d'$ and a', d' and s are collinear and o, a and a' are collinear and $o \neq a'$, then $s \neq d$.

(11) If a, b and c are not collinear and a, b and b' are collinear and a, c and c' are collinear and $a \neq b'$, then $b' \neq c'$.

(12) If a_1, a_2 and a_3 are not collinear and a_1, a_2 and c_3 are collinear and a_2, a_3 and c_1 are collinear and a_1, a_3 and z are collinear and c_1, c_3 and z are collinear and $c_3 \neq a_1$ and $c_3 \neq a_2$ and $c_1 \neq a_2$ and $c_1 \neq a_3$, then $a_1 \neq z$ and $a_3 \neq z$.

(13) If a, b and c are not collinear and a, b and d are collinear and c, e and d are collinear and $e \neq c$ and $d \neq a$, then e, a and c are not collinear.

(14) If p_1, p_2 and q_1 are not collinear and p_1, p_2 and q_2 are collinear and q_1, q_2 and q_3 are collinear and $p_1 \neq q_2$ and $q_2 \neq q_3$, then p_2, p_1 and q_3 are not collinear.

(15) If p_1, p_2 and q_1 are not collinear and p_1, p_2 and p_3 are collinear and q_1, q_2 and p_3 are collinear and $p_3 \neq q_2$ and $p_2 \neq p_3$, then p_3, p_2 and q_2 are not collinear.

(16) If p_1, p_2 and q_1 are not collinear and p_1, p_2 and p_3 are collinear and q_1, q_2 and p_1 are collinear and $p_1 \neq p_3$ and $p_1 \neq q_2$, then p_3, p_1 and q_2 are not collinear.

(17) If $a_1 \neq a_2$ and $b_1 \neq b_2$ and b_1, b_2 and x are collinear and b_1, b_2 and y are collinear and a_1, a_2 and x are collinear and a_1, a_2 and y are collinear and a_1, a_2 and b_1 are not collinear, then $x = y$.

(19)[2] If o, a_1 and a_2 are not collinear and o, a_1 and b_1 are collinear and o, a_2 and b_2 are collinear and $o \neq b_1$ and $o \neq b_2$, then o, b_1 and b_2 are not collinear.

We follow a convention: P_1 denotes a Pappian projective plane defined in terms of collinearity and a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3, o, p_1, p_2, p_3, q_1, q_2, q_3, r_1, r_2, r_3 denote elements of the points of P_1. We now state two propositions:

(20) Suppose that
- (i) $p_2 \neq p_3$,
- (ii) $p_1 \neq p_3$,
- (iii) $q_2 \neq q_3$,
- (iv) $q_1 \neq q_2$,
- (v) $q_1 \neq q_3$,
- (vi) p_1, p_2 and q_1 are not collinear,
- (vii) p_1, p_2 and p_3 are collinear,
- (viii) q_1, q_2 and q_3 are collinear,
- (ix) p_1, q_2 and r_3 are collinear,
- (x) q_1, p_2 and r_3 are collinear,
- (xi) p_1, q_3 and r_2 are collinear,
- (xii) p_3, q_1 and r_2 are collinear,

[2]The proposition (18) was either repeated or obvious.

(xiii) p_2, q_3 and r_1 are collinear,
(xiv) p_3, q_2 and r_1 are collinear.
Then r_1, r_2 and r_3 are collinear.

(21) Suppose that
(i) $o \neq b_1$,
(ii) $a_1 \neq b_1$,
(iii) $o \neq b_2$,
(iv) $a_2 \neq b_2$,
(v) $o \neq b_3$,
(vi) $a_3 \neq b_3$,
(vii) o, a_1 and a_2 are not collinear,
(viii) o, a_1 and a_3 are not collinear,
(ix) o, a_2 and a_3 are not collinear,
(x) a_1, a_2 and c_3 are collinear,
(xi) b_1, b_2 and c_3 are collinear,
(xii) a_2, a_3 and c_1 are collinear,
(xiii) b_2, b_3 and c_1 are collinear,
(xiv) a_1, a_3 and c_2 are collinear,
(xv) b_1, b_3 and c_2 are collinear,
(xvi) o, a_1 and b_1 are collinear,
(xvii) o, a_2 and b_2 are collinear,
(xviii) o, a_3 and b_3 are collinear.
Then c_1, c_2 and c_3 are collinear.

We see that the Pappian projective plane defined in terms of collinearity is a Desarguesian projective plane defined in terms of collinearity.

We see that the Pappian projective space defined in terms of collinearity is a Desarguesian projective space defined in terms of collinearity.

References

[1] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part I. *Formalized Mathematics*, 1(**4**):767–776, 1990.
[2] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part II. *Formalized Mathematics*, 1(**5**):901–907, 1990.
[3] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part III. *Formalized Mathematics*, 1(**5**):909–918, 1990.
[4] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part IV. *Formalized Mathematics*, 1(**5**):919–927, 1990.
[5] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part V. *Formalized Mathematics*, 1(**5**):929–938, 1990.
[6] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part VI. *Formalized Mathematics*, 1(**5**):939–947, 1990.
[7] Wojciech Skaba. The collinearity structure. *Formalized Mathematics*, 1(**4**):657–659, 1990.

Received October 2, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Three-Argument Operations and Four-Argument Operations [1]

Michal Muzalewski
Warsaw University
Białystok

Wojciech Skaba
University of Toruń

Summary. The article contains the definition of three- and four-argument operations. The article is also introduces a few operation related schemes: *FuncEx3D*, *TriOpEx*, *Lambda3D*, *TriOpLambda*, *FuncEx4D*, *QuaOpEx*, *Lambda4D*, *QuaOpLambda*.

MML Identifier: `MULTOP_1`.

The terminology and notation used in this paper have been introduced in the following articles: [4], [1], [2], [5], and [3]. Let f be a function, and let a, b, c be arbitrary. The functor $f(a,\,b,\,c)$ is defined by:

(Def.1) $f(a,\,b,\,c) = f(\langle a,b,c\rangle)$.

We now state the proposition

(1) For every function f and for arbitrary a, b, c holds $f(a,\,b,\,c) = f(\langle a,b,c\rangle)$.

For simplicity we adopt the following rules: A, B, C, D are non-empty sets, a is an element of A, b is an element of B, and c is an element of C. Let us consider A, B, C, D, and let f be a function from $[\!:A,\,B,\,C\,:\!]$ into D, and let us consider a, b, c. Then $f(a,\,b,\,c)$ is an element of D.

We adopt the following rules: X, Y, Z denote sets, T denotes a non-empty set, and x, y, z are arbitrary. One can prove the following propositions:

(2) For all functions f_1, f_2 from $[\!:X,\,Y,\,Z\,:\!]$ into T such that $T \neq \emptyset$ and for all x, y, z such that $x \in X$ and $y \in Y$ and $z \in Z$ holds $f_1(\langle x,y,z\rangle) = f_2(\langle x,y,z\rangle)$ holds $f_1 = f_2$.

(3) For all functions f_1, f_2 from $[\!:A,\,B,\,C\,:\!]$ into D such that for all a, b, c holds $f_1(\langle a,b,c\rangle) = f_2(\langle a,b,c\rangle)$ holds $f_1 = f_2$.

[1] Supported by RPBP.III-24.C6

ISSN 0777–4028

(4) For all functions f_1, f_2 from $[: A, B, C :]$ into D such that for every element a of A and for every element b of B and for every element c of C holds $f_1(a, b, c) = f_2(a, b, c)$ holds $f_1 = f_2$.

Let us consider A. A ternary operation on A is a function from $[: A, A, A :]$ into A.

In this article we present several logical schemes. The scheme *FuncEx3D* concerns a non-empty set $\mathcal{A}$, a non-empty set $\mathcal{B}$, a non-empty set $\mathcal{C}$, a non-empty set $\mathcal{D}$, and a 4-ary predicate $\mathcal{P}$, and states that:

there exists a function f from $[: \mathcal{A}, \mathcal{B}, \mathcal{C} :]$ into $\mathcal{D}$ such that for every element x of $\mathcal{A}$ and for every element y of $\mathcal{B}$ and for every element z of $\mathcal{C}$ holds $\mathcal{P}[x, y, z, f(\langle x, y, z \rangle)]$

provided the following requirements are met:

- for every element x of $\mathcal{A}$ and for every element y of $\mathcal{B}$ and for every element z of $\mathcal{C}$ there exists an element t of $\mathcal{D}$ such that $\mathcal{P}[x, y, z, t]$,
- for every element x of $\mathcal{A}$ and for every element y of $\mathcal{B}$ and for every element z of $\mathcal{C}$ and for all elements t_1, t_2 of $\mathcal{D}$ such that $\mathcal{P}[x, y, z, t_1]$ and $\mathcal{P}[x, y, z, t_2]$ holds $t_1 = t_2$.

The scheme *TriOpEx* concerns a non-empty set $\mathcal{A}$, and a 4-ary predicate $\mathcal{P}$, and states that:

there exists a ternary operation o on $\mathcal{A}$ such that for all elements a, b, c of $\mathcal{A}$ holds $\mathcal{P}[a, b, c, o(a, b, c)]$

provided the parameters meet the following requirements:

- for every elements x, y, z of $\mathcal{A}$ there exists an element t of $\mathcal{A}$ such that $\mathcal{P}[x, y, z, t]$,
- for all elements x, y, z of $\mathcal{A}$ and for all elements t_1, t_2 of $\mathcal{A}$ such that $\mathcal{P}[x, y, z, t_1]$ and $\mathcal{P}[x, y, z, t_2]$ holds $t_1 = t_2$.

The scheme *Lambda3D* concerns a non-empty set $\mathcal{A}$, a non-empty set $\mathcal{B}$, a non-empty set $\mathcal{C}$, a non-empty set $\mathcal{D}$, and a ternary functor $\mathcal{F}$ yielding an element of $\mathcal{D}$ and states that:

there exists a function f from $[: \mathcal{A}, \mathcal{B}, \mathcal{C} :]$ into $\mathcal{D}$ such that for every element x of $\mathcal{A}$ and for every element y of $\mathcal{B}$ and for every element z of $\mathcal{C}$ holds $f(\langle x, y, z \rangle) = \mathcal{F}(x, y, z)$

for all values of the parameters.

The scheme *TriOpLambda* concerns a non-empty set $\mathcal{A}$ and a ternary functor $\mathcal{F}$ yielding an element of $\mathcal{A}$ and states that:

there exists a ternary operation o on $\mathcal{A}$ such that for all elements a, b, c of $\mathcal{A}$ holds $o(a, b, c) = \mathcal{F}(a, b, c)$

for all values of the parameters.

Let f be a function, and let a, b, c, d be arbitrary. The functor $f(a, b, c, d)$ is defined as follows:

(Def.2) $f(a, b, c, d) = f(\langle a, b, c, d \rangle)$.

One can prove the following proposition

(5) For every function f and for arbitrary a, b, c, d holds $f(a, b, c, d) = f(\langle a, b, c, d \rangle)$.

For simplicity we adopt the following rules: A, B, C, D, E will be non-empty sets, a will be an element of A, b will be an element of B, c will be an element of C, and d will be an element of D. Let us consider A, B, C, D, E, and let f be a function from $[: A, B, C, D :]$ into E, and let us consider a, b, c, d. Then $f(a, b, c, d)$ is an element of E.

We adopt the following rules: X, Y, Z, S will be sets, T will be a non-empty set, and x, y, z, s will be arbitrary. The following three propositions are true:

(6) Let f_1, f_2 be functions from $[: X, Y, Z, S :]$ into T. Then if $T \neq \emptyset$ and for all x, y, z, s such that $x \in X$ and $y \in Y$ and $z \in Z$ and $s \in S$ holds $f_1(\langle x, y, z, s\rangle) = f_2(\langle x, y, z, s\rangle)$, then $f_1 = f_2$.

(7) For all functions f_1, f_2 from $[: A, B, C, D :]$ into E such that for all a, b, c, d holds $f_1(\langle a, b, c, d\rangle) = f_2(\langle a, b, c, d\rangle)$ holds $f_1 = f_2$.

(8) For all functions f_1, f_2 from $[: A, B, C, D :]$ into E such that for every element a of A and for every element b of B and for every element c of C and for every element d of D holds $f_1(a, b, c, d) = f_2(a, b, c, d)$ holds $f_1 = f_2$.

Let us consider A. A quadrary operation on A is a function from $[: A, A, A, A :]$ into A.

Now we present four schemes. The scheme *FuncEx4D* concerns a non-empty set $\mathcal{A}$, a non-empty set $\mathcal{B}$, a non-empty set $\mathcal{C}$, a non-empty set $\mathcal{D}$, a non-empty set $\mathcal{E}$, and a 5-ary predicate $\mathcal{P}$, and states that:

there exists a function f from $[: \mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} :]$ into $\mathcal{E}$ such that for every element x of $\mathcal{A}$ and for every element y of $\mathcal{B}$ and for every element z of $\mathcal{C}$ and for every element s of $\mathcal{D}$ holds $\mathcal{P}[x, y, z, s, f(\langle x, y, z, s\rangle)]$

provided the parameters have the following properties:

- for every element x of $\mathcal{A}$ and for every element y of $\mathcal{B}$ and for every element z of $\mathcal{C}$ and for every element s of $\mathcal{D}$ there exists an element t of $\mathcal{E}$ such that $\mathcal{P}[x, y, z, s, t]$,
- for every element x of $\mathcal{A}$ and for every element y of $\mathcal{B}$ and for every element z of $\mathcal{C}$ and for every element s of $\mathcal{D}$ and for all elements t_1, t_2 of $\mathcal{E}$ such that $\mathcal{P}[x, y, z, s, t_1]$ and $\mathcal{P}[x, y, z, s, t_2]$ holds $t_1 = t_2$.

The scheme *QuaOpEx* deals with a non-empty set $\mathcal{A}$, and a 5-ary predicate $\mathcal{P}$, and states that:

there exists a quadrary operation o on $\mathcal{A}$ such that for all elements a, b, c, d of $\mathcal{A}$ holds $\mathcal{P}[a, b, c, d, o(a, b, c, d)]$

provided the parameters meet the following requirements:

- for every elements x, y, z, s of $\mathcal{A}$ there exists an element t of $\mathcal{A}$ such that $\mathcal{P}[x, y, z, s, t]$,
- for all elements x, y, z, s of $\mathcal{A}$ and for all elements t_1, t_2 of $\mathcal{A}$ such that $\mathcal{P}[x, y, z, s, t_1]$ and $\mathcal{P}[x, y, z, s, t_2]$ holds $t_1 = t_2$.

The scheme *Lambda4D* concerns a non-empty set $\mathcal{A}$, a non-empty set $\mathcal{B}$, a non-empty set $\mathcal{C}$, a non-empty set $\mathcal{D}$, a non-empty set $\mathcal{E}$, and a 4-ary functor $\mathcal{F}$ yielding an element of $\mathcal{E}$ and states that:

there exists a function f from $[: \mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} :]$ into $\mathcal{E}$ such that for every element x of $\mathcal{A}$ and for every element y of $\mathcal{B}$ and for every element z of $\mathcal{C}$ and for every element s of $\mathcal{D}$ holds $f(\langle x, y, z, s \rangle) = \mathcal{F}(x, y, z, s)$
for all values of the parameters.

The scheme *QuaOpLambda* deals with a non-empty set $\mathcal{A}$ and a 4-ary functor $\mathcal{F}$ yielding an element of $\mathcal{A}$ and states that:

there exists a quadrary operation o on $\mathcal{A}$ such that for all elements a, b, c, d of $\mathcal{A}$ holds $o(a, b, c, d) = \mathcal{F}(a, b, c, d)$
for all values of the parameters.

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] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[4] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[5] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

Received October 2, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Incidence Projective Spaces

Wojciech Leończuk[1]
Warsaw University
Białystok

Krzysztof Prażmowski[2]
Warsaw University
Białystok

Summary. A basis for investigations on incidence projective spaces. With every projective space defined in terms of collinearity relation we associate the incidence structure consisting of points and lines of the given space. We introduce the general notion of projective space defined in terms of incidence and define several properties of such structures (like satisfability of the Desargues Axiom and conditions on the dimension).

MML Identifier: `INCPROJ`.

The papers [7], [8], [6], [1], [2], [3], [4], and [5] provide the notation and terminology for this paper. We consider projective incidence structures which are systems

⟨points, lines, an incidence⟩,

where the points constitute a non-empty set, the lines constitute a non-empty set, and the incidence is a relation between the points and the lines.

We see that the projective space defined in terms of collinearity is a proper collinearity space.

For simplicity we follow a convention: C_1 will be a proper collinearity space, x, y will be arbitrary, Y will be a set, and B will be an element of $2^{\text{the points of } C_1}$. Let us consider C_1. We see that the line of C_1 is an element of $2^{\text{the points of } C_1}$.

Let us consider C_1. The functor $L(C_1)$ yielding a non-empty set is defined by:

(Def.1) $L(C_1) = \{B : B \text{ is a line of } C_1\}$.

We now state two propositions:

(1) $L(C_1) = \{B : B \text{ is a line of } C_1\}$.

(2) For every x holds x is a line of C_1 if and only if x is an element of $L(C_1)$.

[1]Supported by RPBP.III-24.C6
[2]Supported by RPBP.III-24.C2

ISSN 0777–4028

Let us consider C_1. The functor $\mathbf{I}_{C_1}$ yields a relation between the points of C_1 and $L(C_1)$ and is defined by:

(Def.2) for all x, y holds $\langle x, y\rangle \in \mathbf{I}_{C_1}$ if and only if $x \in$ the points of C_1 and $y \in L(C_1)$ and there exists Y such that $y = Y$ and $x \in Y$.

Let us consider C_1. The functor Inc-ProjSp(C_1) yields a projective incidence structure and is defined by:

(Def.3) Inc-ProjSp$(C_1) = \langle$ the points of $C_1, L(C_1), \mathbf{I}_{C_1}\rangle$.

Next we state four propositions:

(3) Inc-ProjSp$(C_1) = \langle$ the points of $C_1, L(C_1), \mathbf{I}_{C_1}\rangle$.

(4) For every C_1 holds the points of Inc-ProjSp(C_1) = the points of C_1 and the lines of Inc-ProjSp(C_1) = $L(C_1)$ and the incidence of Inc-ProjSp$(C_1) = \mathbf{I}_{C_1}$.

(5) For every x holds x is a line of C_1 if and only if x is an element of the lines of Inc-ProjSp(C_1).

(6) For every x holds x is an element of the points of Inc-ProjSp(C_1) if and only if x is an element of the points of C_1.

For simplicity we adopt the following rules: a, b, c, p, q, s will be elements of the points of Inc-ProjSp(C_1), P, Q, S will be elements of the lines of Inc-ProjSp(C_1), P' will be a line of C_1, and a', b', c', p' will be elements of the points of C_1. Let I_1 be a projective incidence structure, and let s be an element of the points of I_1, and let S be an element of the lines of I_1. The predicate $s \mid S$ is defined as follows:

(Def.4) $\langle s, S\rangle \in$ the incidence of I_1.

One can prove the following propositions:

(7) $s \mid S$ if and only if $\langle s, S\rangle \in \mathbf{I}_{C_1}$.

(8) If $p = p'$ and $P = P'$, then $p \mid P$ if and only if $p' \in P'$.

(9) There exist a', b', c' such that $a' \neq b'$ and $b' \neq c'$ and $c' \neq a'$.

(10) For every a' there exists b' such that $a' \neq b'$.

(11) If $p \mid P$ and $q \mid P$ and $p \mid Q$ and $q \mid Q$, then $p = q$ or $P = Q$.

(12) For every p, q there exists P such that $p \mid P$ and $q \mid P$.

(13) If $a = a'$ and $b = b'$ and $c = c'$, then a', b' and c' are collinear if and only if there exists P such that $a \mid P$ and $b \mid P$ and $c \mid P$.

(14) There exist p, P such that $p \nmid P$.

For simplicity we follow the rules: C_1 is a projective space defined in terms of collinearity, a, b, c, d, p, q are elements of the points of Inc-ProjSp(C_1), P, Q, S, M, N are elements of the lines of Inc-ProjSp(C_1), and a', b', c', d', p' are elements of the points of C_1. One can prove the following propositions:

(15) For every P there exist a, b, c such that $a \neq b$ and $b \neq c$ and $c \neq a$ and $a \mid P$ and $b \mid P$ and $c \mid P$.

(16) Suppose that

(i) $a \mid M$,

(ii) $b \mid M$,
(iii) $c \mid N$,
(iv) $d \mid N$,
(v) $p \mid M$,
(vi) $p \mid N$,
(vii) $a \mid P$,
(viii) $c \mid P$,
(ix) $b \mid Q$,
(x) $d \mid Q$,
(xi) $p \nmid P$,
(xii) $p \nmid Q$,
(xiii) $M \neq N$.

Then there exists q such that $q \mid P$ and $q \mid Q$.

(17) If for every a', b', c', d' there exists p' such that a', b' and p' are collinear and c', d' and p' are collinear, then for every M, N there exists q such that $q \mid M$ and $q \mid N$.

(18) If there exist elements p, p_1, r, r_1 of the points of C_1 such that for no element s of the points of C_1 holds p, p_1 and s are collinear and r, r_1 and s are collinear, then there exist M, N such that for no q holds $q \mid M$ and $q \mid N$.

(19) Suppose for every elements p, p_1, q, q_1, r_2 of the points of C_1 there exist elements r, r_1 of the points of C_1 such that p, q and r are collinear and p_1, q_1 and r_1 are collinear and r_2, r and r_1 are collinear. Then for every a, M, N there exist b, c, S such that $a \mid S$ and $b \mid S$ and $c \mid S$ and $b \mid M$ and $c \mid N$.

We now define two new predicates. Let x, y, z be arbitrary. We say that x, y, z are mutually different if and only if:

(Def.5) $x \neq y$ and $y \neq z$ and $z \neq x$.

Let u be arbitrary. We say that x, y, z, u are mutually different if and only if:

(Def.6) $x \neq y$ and $y \neq z$ and $z \neq x$ and $u \neq x$ and $u \neq y$ and $u \neq z$.

We now define two new predicates. Let C_2 be a projective incidence structure, and let a, b be elements of the points of C_2, and let M be an element of the lines of C_2. The predicate $a, b \mid M$ is defined as follows:

(Def.7) $a \mid M$ and $b \mid M$.

Let c be an element of the points of C_2. The predicate $a, b, c \mid M$ is defined by:

(Def.8) $a \mid M$ and $b \mid M$ and $c \mid M$.

We now state three propositions:

(20) Suppose that

(i) for all elements p_1, r_2, q, r_1, q_1, p, r of the points of C_1 such that p_1, r_2 and q are collinear and r_1, q_1 and q are collinear and p_1, r_1 and p are collinear and r_2, q_1 and p are collinear and p_1, q_1 and r are collinear and r_2, r_1 and r are collinear and p, q and r are collinear holds p_1, r_2 and q_1

are collinear or p_1, r_2 and r_1 are collinear or p_1, r_1 and q_1 are collinear or r_2, r_1 and q_1 are collinear.

Let p, q, r, s, a, b, c be elements of the points of Inc-ProjSp(C_1). Let L, Q, R, S, A, B, C be elements of the lines of Inc-ProjSp(C_1). Suppose that

(ii) $q \nmid L$,
(iii) $r \nmid L$,
(iv) $p \nmid Q$,
(v) $s \nmid Q$,
(vi) $p \nmid R$,
(vii) $r \nmid R$,
(viii) $q \nmid S$,
(ix) $s \nmid S$,
(x) $a, p, s \mid L$,
(xi) $a, q, r \mid Q$,
(xii) $b, q, s \mid R$,
(xiii) $b, p, r \mid S$,
(xiv) $c, p, q \mid A$,
(xv) $c, r, s \mid B$,
(xvi) $a, b \mid C$.

Then $c \nmid C$.

(21) Suppose that

(i) for all elements o, p_1, p_2, p_3, q_1, q_2, q_3, r_1, r_2, r_3 of the points of C_1 such that $o \neq q_1$ and $p_1 \neq q_1$ and $o \neq q_2$ and $p_2 \neq q_2$ and $o \neq q_3$ and $p_3 \neq q_3$ and o, p_1 and p_2 are not collinear and o, p_1 and p_3 are not collinear and o, p_2 and p_3 are not collinear and p_1, p_2 and r_3 are collinear and q_1, q_2 and r_3 are collinear and p_2, p_3 and r_1 are collinear and q_2, q_3 and r_1 are collinear and p_1, p_3 and r_2 are collinear and q_1, q_3 and r_2 are collinear and o, p_1 and q_1 are collinear and o, p_2 and q_2 are collinear and o, p_3 and q_3 are collinear holds r_1, r_2 and r_3 are collinear.

Let o, b_1, a_1, b_2, a_2, b_3, a_3, r, s, t be elements of the points of Inc-ProjSp(C_1). Let C_3, C_4, C_5, A_1, A_2, A_3, B_1, B_2, B_3 be elements of the lines of Inc-ProjSp(C_1). Suppose that

(ii) $o, b_1, a_1 \mid C_3$,
(iii) $o, a_2, b_2 \mid C_4$,
(iv) $o, a_3, b_3 \mid C_5$,
(v) $a_3, a_2, t \mid A_1$,
(vi) $a_3, r, a_1 \mid A_2$,
(vii) $a_2, s, a_1 \mid A_3$,
(viii) $t, b_2, b_3 \mid B_1$,
(ix) $b_1, r, b_3 \mid B_2$,
(x) $b_1, s, b_2 \mid B_3$,
(xi) C_3, C_4, C_5 are mutually different,
(xii) $o \neq a_1$,
(xiii) $o \neq a_2$,

(xiv) $o \neq a_3$,
(xv) $o \neq b_1$,
(xvi) $o \neq b_2$,
(xvii) $o \neq b_3$,
(xviii) $a_1 \neq b_1$,
(xix) $a_2 \neq b_2$,
(xx) $a_3 \neq b_3$.

Then there exists an element O of the lines of Inc-ProjSp(C_1) such that $r, s, t \mid O$.

(22) Suppose that

(i) for all elements o, p_1, p_2, p_3, q_1, q_2, q_3, r_1, r_2, r_3 of the points of C_1 such that $o \neq p_2$ and $o \neq p_3$ and $p_2 \neq p_3$ and $p_1 \neq p_2$ and $p_1 \neq p_3$ and $o \neq q_2$ and $o \neq q_3$ and $q_2 \neq q_3$ and $q_1 \neq q_2$ and $q_1 \neq q_3$ and o, p_1 and q_1 are not collinear and o, p_1 and p_2 are collinear and o, p_1 and p_3 are collinear and o, q_1 and q_2 are collinear and o, q_1 and q_3 are collinear and p_1, q_2 and r_3 are collinear and q_1, p_2 and r_3 are collinear and p_1, q_3 and r_2 are collinear and p_3, q_1 and r_2 are collinear and p_2, q_3 and r_1 are collinear and p_3, q_2 and r_1 are collinear holds r_1, r_2 and r_3 are collinear.

Let o, a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3 be elements of the points of Inc-ProjSp(C_1). Let A_1, A_2, A_3, B_1, B_2, B_3, C_3, C_4, C_5 be elements of the lines of Inc-ProjSp(C_1). Suppose that

(ii) o, a_1, a_2, a_3 are mutually different,
(iii) o, b_1, b_2, b_3 are mutually different,
(iv) $A_3 \neq B_3$,
(v) $o \mid A_3$,
(vi) $o \mid B_3$,
(vii) $a_2, b_3, c_1 \mid A_1$,
(viii) $a_3, b_1, c_2 \mid B_1$,
(ix) $a_1, b_2, c_3 \mid C_3$,
(x) $a_1, b_3, c_2 \mid A_2$,
(xi) $a_3, b_2, c_1 \mid B_2$,
(xii) $a_2, b_1, c_3 \mid C_4$,
(xiii) $b_1, b_2, b_3 \mid A_3$,
(xiv) $a_1, a_2, a_3 \mid B_3$,
(xv) $c_1, c_2 \mid C_5$.

Then $c_3 \mid C_5$.

A projective incidence structure is called a projective space defined in terms of incidence if:

(Def.9) (i) for all elements p, q of the points of it and for all elements P, Q of the lines of it such that $p \mid P$ and $q \mid P$ and $p \mid Q$ and $q \mid Q$ holds $p = q$ or $P = Q$,

(ii) for every elements p, q of the points of it there exists an element P of the lines of it such that $p \mid P$ and $q \mid P$,

(iii) there exists an element p of the points of it and there exists an element P of the lines of it such that $p \nmid P$,

(iv) for every element P of the lines of it there exist elements a, b, c of the points of it such that $a \neq b$ and $b \neq c$ and $c \neq a$ and $a \mid P$ and $b \mid P$ and $c \mid P$,

(v) for all elements a, b, c, d, p, q of the points of it and for all elements M, N, P, Q of the lines of it such that $a \mid M$ and $b \mid M$ and $c \mid N$ and $d \mid N$ and $p \mid M$ and $p \mid N$ and $a \mid P$ and $c \mid P$ and $b \mid Q$ and $d \mid Q$ and $p \nmid P$ and $p \nmid Q$ and $M \neq N$ there exists an element q of the points of it such that $q \mid P$ and $q \mid Q$.

Let C_1 be a projective space defined in terms of collinearity.

Then Inc-ProjSp(C_1) is a projective space defined in terms of incidence.

A projective space defined in terms of incidence is 2-dimensional if:

(Def.10) for every elements M, N of the lines of it there exists an element q of the points of it such that $q \mid M$ and $q \mid N$.

A projective space defined in terms of incidence is at least 3-dimensional if:

(Def.11) there exist elements M, N of the lines of it such that for no element q of the points of it holds $q \mid M$ and $q \mid N$.

A projective space defined in terms of incidence is at most 3-dimensional if:

(Def.12) for every element a of the points of it and for every elements M, N of the lines of it there exist elements b, c of the points of it and there exists an element S of the lines of it such that $a \mid S$ and $b \mid S$ and $c \mid S$ and $b \mid M$ and $c \mid N$.

A projective space defined in terms of incidence is 3-dimensional if:

(Def.13) it is at most 3-dimensional and it is at least 3-dimensional.

A projective space defined in terms of incidence is Fanoian if:

(Def.14) Let p, q, r, s, a, b, c be elements of the points of it . Let L, Q, R, S, A, B, C be elements of the lines of it . Suppose that

(i) $q \nmid L$,
(ii) $r \nmid L$,
(iii) $p \nmid Q$,
(iv) $s \nmid Q$,
(v) $p \nmid R$,
(vi) $r \nmid R$,
(vii) $q \nmid S$,
(viii) $s \nmid S$,
(ix) $a, p, s \mid L$,
(x) $a, q, r \mid Q$,
(xi) $b, q, s \mid R$,
(xii) $b, p, r \mid S$,
(xiii) $c, p, q \mid A$,
(xiv) $c, r, s \mid B$,

(xv) $a, b \mid C$.
Then $c \nmid C$.

A projective space defined in terms of incidence is Desarguesian if:

(Def.15) Let o, b_1, a_1, b_2, a_2, b_3, a_3, r, s, t be elements of the points of it . Let C_3, C_4, C_5, A_1, A_2, A_3, B_1, B_2, B_3 be elements of the lines of it . Suppose that

(i) $o, b_1, a_1 \mid C_3$,
(ii) $o, a_2, b_2 \mid C_4$,
(iii) $o, a_3, b_3 \mid C_5$,
(iv) $a_3, a_2, t \mid A_1$,
(v) $a_3, r, a_1 \mid A_2$,
(vi) $a_2, s, a_1 \mid A_3$,
(vii) $t, b_2, b_3 \mid B_1$,
(viii) $b_1, r, b_3 \mid B_2$,
(ix) $b_1, s, b_2 \mid B_3$,
(x) C_3, C_4, C_5 are mutually different,
(xi) $o \neq a_1$,
(xii) $o \neq a_2$,
(xiii) $o \neq a_3$,
(xiv) $o \neq b_1$,
(xv) $o \neq b_2$,
(xvi) $o \neq b_3$,
(xvii) $a_1 \neq b_1$,
(xviii) $a_2 \neq b_2$,
(xix) $a_3 \neq b_3$.

Then there exists an element O of the lines of it such that $r, s, t \mid O$.

A projective space defined in terms of incidence is Pappian if:

(Def.16) Let o, a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3 be elements of the points of it . Let A_1, A_2, A_3, B_1, B_2, B_3, C_3, C_4, C_5 be elements of the lines of it . Suppose that

(i) o, a_1, a_2, a_3 are mutually different,
(ii) o, b_1, b_2, b_3 are mutually different,
(iii) $A_3 \neq B_3$,
(iv) $o \mid A_3$,
(v) $o \mid B_3$,
(vi) $a_2, b_3, c_1 \mid A_1$,
(vii) $a_3, b_1, c_2 \mid B_1$,
(viii) $a_1, b_2, c_3 \mid C_3$,
(ix) $a_1, b_3, c_2 \mid A_2$,
(x) $a_3, b_2, c_1 \mid B_2$,
(xi) $a_2, b_1, c_3 \mid C_4$,
(xii) $b_1, b_2, b_3 \mid A_3$,
(xiii) $a_1, a_2, a_3 \mid B_3$,
(xiv) $c_1, c_2 \mid C_5$.

Then $c_3 \mid C_5$.

References

[1] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part I. *Formalized Mathematics*, 1(**4**):767–776, 1990.
[2] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part III. *Formalized Mathematics*, 1(**5**):909–918, 1990.
[3] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part IV. *Formalized Mathematics*, 1(**5**):919–927, 1990.
[4] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part V. *Formalized Mathematics*, 1(**5**):929–938, 1990.
[5] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces - part VI. *Formalized Mathematics*, 1(**5**):939–947, 1990.
[6] Wojciech Skaba. The collinearity structure. *Formalized Mathematics*, 1(**4**):657–659, 1990.
[7] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[8] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received October 4, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

One-Dimensional Congruence of Segments, Basic Facts and Midpoint Relation [1]

Barbara Konstanta
Siedlce Agricultural and Pedagogical University

Urszula Kowieska
Siedlce Agricultural and Pedagogical University

Grzegorz Lewandowski
Siedlce Agricultural and Pedagogical University

Krzysztof Prażmowski
Warsaw University
Białystok

Summary. We study the theory of one-dimensional congruence of segments. The theory is characterized by a suitable formal axiom system; as a model of this system one can take the structure obtained from any weak directed geometrical bundle, with the congruence interpreted as in the case of "classical" vectors. Preliminary consequences of our axiom system are proved, basic relations of maximal distance and of midpoint are defined, and several fundamental properties of them are established.

MML Identifier: `AFVECT01`.

The papers [8], [2], [3], [10], [7], [4], [1], [5], [6], and [9] provide the terminology and notation for this paper. In the sequel A_1 will be a weak affine vector space. Let us consider A_1, and let a, b, c, d be elements of the points of A_1. The predicate $a, b \Leftrightarrow c, d$ is defined as follows:

(Def.1) $a, b \Rrightarrow c, d$ or $a, b \Rrightarrow d, c$.

An affine structure is called a weak segment-congruence space if:

(Def.2) (i) there exist elements a, b of the points of it such that $a \neq b$,

(ii) for all elements a, b of the points of it holds $a, b \Rrightarrow b, a$,

[1]Supported by RPBP.III-24.C3

ISSN 0777–4028

(iii) for all elements a, b of the points of it such that $a, b \Rrightarrow a, a$ holds $a = b$,

(iv) for all elements a, b, c, d, p, q of the points of it such that $a, b \Rrightarrow p, q$ and $c, d \Rrightarrow p, q$ holds $a, b \Rrightarrow c, d$,

(v) for every elements a, c of the points of it there exists an element b of the points of it such that $a, b \Rrightarrow b, c$,

(vi) for all elements a, a', b, b', p of the points of it such that $a \neq a'$ and $b \neq b'$ and $p, a \Rrightarrow p, a'$ and $p, b \Rrightarrow p, b'$ holds $a, b \Rrightarrow a', b'$,

(vii) for all elements a, b of the points of it holds $a = b$ or there exists an element c of the points of it such that $a \neq c$ and $a, b \Rrightarrow b, c$ or there exist elements p, p' of the points of it such that $p \neq p'$ and $a, b \Rrightarrow p, p'$ and $a, p \Rrightarrow p, b$ and $a, p' \Rrightarrow p', b$,

(viii) for all elements a, b, b', p, p', c of the points of it such that $a, b \Rrightarrow b, c$ and $b, b' \Rrightarrow p, p'$ and $b, p \Rrightarrow p, b'$ and $b, p' \Rrightarrow p', b'$ holds $a, b' \Rrightarrow b', c$,

(ix) for all elements a, b, b', c of the points of it such that $a \neq c$ and $b \neq b'$ and $a, b \Rrightarrow b, c$ and $a, b' \Rrightarrow b', c$ there exist elements p, p' of the points of it such that $p \neq p'$ and $b, b' \Rrightarrow p, p'$ and $b, p \Rrightarrow p, b'$ and $b, p' \Rrightarrow p', b'$,

(x) for all elements a, b, c, p, p', q, q' of the points of it such that $a, b \Rrightarrow p, p'$ and $a, c \Rrightarrow q, q'$ and $a, p \Rrightarrow p, b$ and $a, q \Rrightarrow q, c$ and $a, p' \Rrightarrow p', b$ and $a, q' \Rrightarrow q', c$ there exist elements r, r' of the points of it such that $b, c \Rrightarrow r, r'$ and $b, r \Rrightarrow r, c$ and $b, r' \Rrightarrow r', c$.

We adopt the following rules: A_1 is a weak segment-congruence space and a, b, b', b'', c, d, p, p' are elements of the points of A_1. Let us consider A_1, and let a, b, c, d be elements of the points of A_1. The predicate $a, b \Leftrightarrow c, d$ is defined by:

(Def.3) $a, b \Rrightarrow c, d$.

We now state several propositions:

(1) $a, b \Leftrightarrow a, b$.

(2) If $a, b \Leftrightarrow c, d$, then $c, d \Leftrightarrow a, b$.

(3) If $a, b \Leftrightarrow c, d$, then $a, b \Leftrightarrow d, c$.

(4) If $a, b \Leftrightarrow c, d$, then $b, a \Leftrightarrow c, d$.

(5) For all a, b holds $a, a \Leftrightarrow b, b$.

(6) If $a, b \Leftrightarrow c, c$, then $a = b$.

(7) If $a, b \Leftrightarrow p, p'$ and $p, p' \Leftrightarrow b, c$ and $a, b \Leftrightarrow b, c$ and $a, p \Leftrightarrow p, b$ and $a, p' \Leftrightarrow p', b$, then $a = c$.

(8) If $a, b \Leftrightarrow a, b'$ and $a, b' \Leftrightarrow a, b''$ and $a, b \Leftrightarrow a, b''$, then $b = b'$ or $b = b''$ or $b' = b''$.

Let us consider A_1, a, b. We say that a, b are in a maximal distance if and only if:

(Def.4) there exist p, p' such that $p \neq p'$ and $a, b \Leftrightarrow p, p'$ and $a, p \Leftrightarrow p, b$ and $a, p' \Leftrightarrow p', b$.

Let us consider A_1, a, b, c. We say that b is a midpoint of a, c if and only if:

(Def.5) $a = b$ and $b = c$ and $a = c$ or $a = c$ and a, b are in a maximal distance or $a \neq c$ and $a, b \Leftrightarrow b, c$.

Next we state three propositions:

(11)[2] If $a \neq b$ and a, b are not in a maximal distance, then there exists c such that $a \neq c$ and $a, b \Leftrightarrow b, c$.

(12) If a, b are in a maximal distance and $a, b \Leftrightarrow b, c$, then $a = c$.

(13) If a, b are in a maximal distance, then $a \neq b$.

References

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

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

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

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

[5] Grzegorz Lewandowski and Krzysztof Prażmowski. A construction of an abstract space of congruence of vectors. *Formalized Mathematics*, 1(**4**):685–688, 1990.

[6] Grzegorz Lewandowski, Krzysztof Prażmowski, and Bożena Lewandowska. Directed geometrical bundles and their analytical representation. *Formalized Mathematics*, 2(**1**):135–141, 1991.

[7] Henryk Oryszczyszyn and Krzysztof Prażmowski. Analytical ordered affine spaces. *Formalized Mathematics*, 1(**3**):601–605, 1990.

[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[9] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

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

Received October 4, 1990

[2] The propositions (9)–(10) were either repeated or obvious.

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Algebra of Normal Forms

Andrzej Trybulec
Warsaw University
Białystok

Summary. We mean by a normal form a finite set of ordered pairs of subsets of a fixed set that fulfils two conditions: elements of it consist of disjoint sets and elements of it are incomparable w.r.t. inclusion. The underlying set corresponds to a set of propositional variables but is arbitrary. The correspodents to a normal form of a formula, e.g. a disjunctive normal form, is as follows. The normal form is the set of disjuncts and a disjunct is an ordered pair consisting of the sets of propositional variables that occur in the non-negated and negated disjunct. The requirement that the element of a normal form consists of disjoint sets means that contradictory disjuncts have been removed, and the second condition means that the absorption law has been used to shorten the normal form. We construct a lattice $\langle \mathbb{N}, \sqcup, \sqcap \rangle$, where $a \sqcup b = \mu(a \cup b)$ and $a \sqcap b = \mu c$, c being the set of all pairs $\langle X_1 \cup Y_1, X_2 \cup Y_2 \rangle$, $\langle X_1, X_2 \rangle \in a$ and $\langle Y_1, Y_2 \rangle \in b$, which consist of disjoint sets. μa denotes here the set of all minimal, w.r.t. inclusion, elements of a. We prove that the lattice of normal forms over a set defined in this way is distributive and that $\emptyset$ is the minimal element of it.

MML Identifier: `NORMFORM`.

The terminology and notation used here have been introduced in the following articles: [8], [9], [3], [4], [1], [5], [2], [6], [10], [7], and [11]. In the sequel A, B, C, D will be sets. We now state two propositions:

(1) If $A \subseteq B$ and $C \subseteq D$ and B misses D, then A misses C.

(2) If $A \setminus B \subseteq C$, then $A \subseteq B \cup C$.

In the sequel A, B will denote Boolean domains and x, y will denote elements of $[\!: A, B :\!]$. We now define five new constructions. Let us consider A, B, x, y. The predicate $x \subseteq y$ is defined by:

(Def.1) $\quad x_{\mathbf{1}} \subseteq y_{\mathbf{1}}$ and $x_{\mathbf{2}} \subseteq y_{\mathbf{2}}$.

The functor $x \cup y$ yielding an element of $[\!: A, B :\!]$ is defined as follows:

(Def.2) $\quad x \cup y = \langle x_{\mathbf{1}} \cup y_{\mathbf{1}}, x_{\mathbf{2}} \cup y_{\mathbf{2}} \rangle$.

The functor $x \cap y$ yielding an element of $[\!: A, B :\!]$ is defined as follows:

ISSN 0777–4028

(Def.3) $x \cap y = \langle x_{\mathbf{1}} \cap y_{\mathbf{1}}, x_{\mathbf{2}} \cap y_{\mathbf{2}} \rangle$.

The functor $x \setminus y$ yields an element of $[\!: A, B :\!]$ and is defined as follows:

(Def.4) $x \setminus y = \langle x_{\mathbf{1}} \setminus y_{\mathbf{1}}, x_{\mathbf{2}} \setminus y_{\mathbf{2}} \rangle$.

The functor $x \dot{-} y$ yields an element of $[\!: A, B :\!]$ and is defined as follows:

(Def.5) $x \dot{-} y = \langle x_{\mathbf{1}} \dot{-} y_{\mathbf{1}}, x_{\mathbf{2}} \dot{-} y_{\mathbf{2}} \rangle$.

In the sequel X will be a set and a, b, c will be elements of $[\!: A, B :\!]$. We now state a number of propositions:

(3) $a \subseteq a$.

(4) If $a \subseteq b$ and $b \subseteq a$, then $a = b$.

(5) If $a \subseteq b$ and $b \subseteq c$, then $a \subseteq c$.

(6) $a \cup b = \langle a_{\mathbf{1}} \cup b_{\mathbf{1}}, a_{\mathbf{2}} \cup b_{\mathbf{2}} \rangle$.

(7) $a \cap b = \langle a_{\mathbf{1}} \cap b_{\mathbf{1}}, a_{\mathbf{2}} \cap b_{\mathbf{2}} \rangle$.

(8) $a \setminus b = \langle a_{\mathbf{1}} \setminus b_{\mathbf{1}}, a_{\mathbf{2}} \setminus b_{\mathbf{2}} \rangle$.

(9) $a \dot{-} b = \langle a_{\mathbf{1}} \dot{-} b_{\mathbf{1}}, a_{\mathbf{2}} \dot{-} b_{\mathbf{2}} \rangle$.

(10) $(a \cup b)_{\mathbf{1}} = a_{\mathbf{1}} \cup b_{\mathbf{1}}$ and $(a \cup b)_{\mathbf{2}} = a_{\mathbf{2}} \cup b_{\mathbf{2}}$.

(11) $(a \cap b)_{\mathbf{1}} = a_{\mathbf{1}} \cap b_{\mathbf{1}}$ and $(a \cap b)_{\mathbf{2}} = a_{\mathbf{2}} \cap b_{\mathbf{2}}$.

(12) $(a \setminus b)_{\mathbf{1}} = a_{\mathbf{1}} \setminus b_{\mathbf{1}}$ and $(a \setminus b)_{\mathbf{2}} = a_{\mathbf{2}} \setminus b_{\mathbf{2}}$.

(13) $(a \dot{-} b)_{\mathbf{1}} = a_{\mathbf{1}} \dot{-} b_{\mathbf{1}}$ and $(a \dot{-} b)_{\mathbf{2}} = a_{\mathbf{2}} \dot{-} b_{\mathbf{2}}$.

(14) $a \cup a = a$.

(15) $a \cup b = b \cup a$.

(16) $a \cup b \cup c = a \cup (b \cup c)$.

(17) $a \cap a = a$.

(18) $a \cap b = b \cap a$.

(19) $a \cap b \cap c = a \cap (b \cap c)$.

(20) $a \cap (b \cup c) = a \cap b \cup a \cap c$.

(21) $a \cup b \cap a = a$.

(22) $a \cap (b \cup a) = a$.

(24)[1] $a \cup b \cap c = (a \cup b) \cap (a \cup c)$.

(25) If $a \subseteq c$ and $b \subseteq c$, then $a \cup b \subseteq c$.

(26) $a \subseteq a \cup b$ and $b \subseteq a \cup b$.

(27) If $a = a \cup b$, then $b \subseteq a$.

(28) If $a \subseteq b$, then $c \cup a \subseteq c \cup b$ and $a \cup c \subseteq b \cup c$.

(29) $(a \setminus b) \cup b = a \cup b$.

(30) If $a \setminus b \subseteq c$, then $a \subseteq b \cup c$.

(31) If $a \subseteq b \cup c$, then $a \setminus c \subseteq b$.

In the sequel a will be an element of $[\!: \operatorname{Fin} X, \operatorname{Fin} X :\!]$. Let A be a set. The functor $\operatorname{FinUnion}_A$ yields a binary operation on $[\!: \operatorname{Fin} A, \operatorname{Fin} A :\!]$ and is defined by:

[1]The proposition (23) was either repeated or obvious.

(Def.6) for all elements x, y of $[:\mathrm{Fin}\,A, \mathrm{Fin}\,A:]$ holds $\mathrm{FinUnion}_A(x, y) = x \cup y$.

In the sequel A will denote a set. Let X be a non-empty set, and let A be a set, and let B be an element of $\mathrm{Fin}\,X$, and let f be a function from X into $[:\mathrm{Fin}\,A, \mathrm{Fin}\,A:]$. The functor $\mathrm{FinUnion}(B, f)$ yields an element of $[:\mathrm{Fin}\,A, \mathrm{Fin}\,A:]$ and is defined as follows:

(Def.7) $\mathrm{FinUnion}(B, f) = \mathrm{FinUnion}_A \text{-} \sum_B f$.

The following propositions are true:

(32) $\mathrm{FinUnion}_A$ is idempotent.

(33) $\mathrm{FinUnion}_A$ is commutative.

(34) $\mathrm{FinUnion}_A$ is associative.

(35) For every non-empty set X and for every function f from X into $[:\mathrm{Fin}\,A, \mathrm{Fin}\,A:]$ and for every element B of $\mathrm{Fin}\,X$ and for every element x of X such that $x \in B$ holds $f(x) \subseteq \mathrm{FinUnion}(B, f)$.

(36) $\langle 0_A, 0_A \rangle$ is a unity w.r.t. $\mathrm{FinUnion}_A$.

(37) $\mathrm{FinUnion}_A$ has a unity.

(38) $\mathbf{1}_{\mathrm{FinUnion}_A} = \langle 0_A, 0_A \rangle$.

(39) For every element x of $[:\mathrm{Fin}\,A, \mathrm{Fin}\,A:]$ holds $\mathbf{1}_{\mathrm{FinUnion}_A} \subseteq x$.

(40) For every non-empty set X and for every function f from X into $[:\mathrm{Fin}\,A, \mathrm{Fin}\,A:]$ and for every element B of $\mathrm{Fin}\,X$ and for every element c of $[:\mathrm{Fin}\,A, \mathrm{Fin}\,A:]$ such that for every element x of X such that $x \in B$ holds $f(x) \subseteq c$ holds $\mathrm{FinUnion}(B, f) \subseteq c$.

(41) For every non-empty set X and for every element B of $\mathrm{Fin}\,X$ and for all functions f, g from X into $[:\mathrm{Fin}\,A, \mathrm{Fin}\,A:]$ such that $f \restriction B = g \restriction B$ holds $\mathrm{FinUnion}(B, f) = \mathrm{FinUnion}(B, g)$.

Let us consider X. The functor $\mathrm{DP}(X)$ yields a non-empty subset of $[:\mathrm{Fin}\,X, \mathrm{Fin}\,X:]$ and is defined as follows:

(Def.8) $\mathrm{DP}(X) = \{a : a_{\mathbf{1}} \text{ misses } a_{\mathbf{2}}\}$.

The following proposition is true

(42) For every element y of $[:\mathrm{Fin}\,X, \mathrm{Fin}\,X:]$ holds $y \in \mathrm{DP}(X)$ if and only if $y_{\mathbf{1}} \cap y_{\mathbf{2}} = \emptyset$.

In the sequel x, y will denote elements of $[:\mathrm{Fin}\,X, \mathrm{Fin}\,X:]$ and a, b will denote elements of $\mathrm{DP}(X)$. We now state several propositions:

(43) If $y \in \mathrm{DP}(X)$ and $x \in \mathrm{DP}(X)$, then $y \cup x \in \mathrm{DP}(X)$ if and only if $y_{\mathbf{1}} \cap x_{\mathbf{2}} \cup x_{\mathbf{1}} \cap y_{\mathbf{2}} = \emptyset$.

(44) $a_{\mathbf{1}} \cap a_{\mathbf{2}} = \emptyset$.

(45) If $x \subseteq b$, then x is an element of $\mathrm{DP}(X)$.

(46) For no arbitrary x holds $x \in a_{\mathbf{1}}$ and $x \in a_{\mathbf{2}}$.

(47) If $a \cup b \notin \mathrm{DP}(X)$, then there exists an element p of X such that $p \in a_{\mathbf{1}}$ and $p \in b_{\mathbf{2}}$ or $p \in b_{\mathbf{1}}$ and $p \in a_{\mathbf{2}}$.

(48) $a_{\mathbf{1}}$ misses $a_{\mathbf{2}}$.

(49) If $x_{\mathbf{1}}$ misses $x_{\mathbf{2}}$, then x is an element of $\mathrm{DP}(X)$.

(50) For all sets V, W such that $V \subseteq a_{\mathbf{1}}$ and $W \subseteq a_{\mathbf{2}}$ holds $\langle V, W\rangle$ is an element of $\mathrm{DP}(X)$.

In this article we present several logical schemes. The scheme *LambdaX* concerns a non-empty set $\mathcal{A}$, a non-empty set $\mathcal{B}$, a non-empty subset $\mathcal{C}$ of $\mathcal{A}$, and a unary functor $\mathcal{F}$ yielding an element of $\mathcal{C}$ and states that:

there exists a function f from $\mathcal{B}$ into $\mathcal{C}$ such that for every element x of $\mathcal{B}$ holds $f(x) = \mathcal{F}(x)$

for all values of the parameters.

The scheme *BinOpLambdaX* deals with a non-empty set $\mathcal{A}$, a non-empty subset $\mathcal{B}$ of $\mathcal{A}$, and a binary functor $\mathcal{F}$ yielding an element of $\mathcal{B}$ and states that:

there exists a binary operation o on $\mathcal{B}$ such that for all elements a, b of $\mathcal{B}$ holds $o(a, b) = \mathcal{F}(a, b)$

for all values of the parameters.

For simplicity we follow a convention: A will be a set, x will be an element of $[\!:\mathrm{Fin}\,A, \mathrm{Fin}\,A:\!]$, a, b, c, s, t will be elements of $\mathrm{DP}(A)$, and B, C, D will be elements of $\mathrm{Fin}\,\mathrm{DP}(A)$. Let us consider A. The normal forms over A yields a non-empty subset of $\mathrm{Fin}\,\mathrm{DP}(A)$ and is defined as follows:

(Def.9) the normal forms over $A = \{B : a \in B \wedge b \in B \wedge a \subseteq b \Rightarrow a = b\}$.

In the sequel K, L, M are elements of the normal forms over A. Next we state three propositions:

(51) $\emptyset \in$ the normal forms over A.

(52) If $B \in$ the normal forms over A and $a \in B$ and $b \in B$ and $a \subseteq b$, then $a = b$.

(53) If for all a, b such that $a \in B$ and $b \in B$ and $a \subseteq b$ holds $a = b$, then $B \in$ the normal forms over A.

We now define two new functors. Let us consider A, B. The functor μB yielding an element of the normal forms over A is defined by:

(Def.10) $\mu B = \{t : s \in B \wedge s \subseteq t \Leftrightarrow s = t\}$.

Let us consider C. The functor $B \frown C$ yielding an element of $\mathrm{Fin}\,\mathrm{DP}(A)$ is defined as follows:

(Def.11) $B \frown C = \mathrm{DP}(A) \cap \{s \cup t : s \in B \wedge t \in C\}$.

The following propositions are true:

(54) $B \frown C = \mathrm{DP}(A) \cap \{s \cup t : s \in B \wedge t \in C\}$.

(55) If $x \in B \frown C$, then there exist b, c such that $b \in B$ and $c \in C$ and $x = b \cup c$.

(56) If $b \in B$ and $c \in C$ and $b \cup c \in \mathrm{DP}(A)$, then $b \cup c \in B \frown C$.

(57) If $b \in B$ and $c \in C$ and $a = b \cup c$, then $a \in B \frown C$.

(58) If $a \in \mu B$, then $a \in B$ but if $b \in B$ and $b \subseteq a$, then $b = a$.

(59) If $a \in \mu B$, then $a \in B$.

(60) If $a \in \mu B$ and $b \in B$ and $b \subseteq a$, then $b = a$.

(61) If $a \in B$ and for every b such that $b \in B$ and $b \subseteq a$ holds $b = a$, then $a \in \mu B$.

We now define two new functors. Let us consider A. The functor $\sqcup_A$ yields a binary operation on the normal forms over A and is defined by:

(Def.12) $\sqcup_A(K, L) = \mu(K \cup L)$.

The functor $\sqcap_A$ yielding a binary operation on the normal forms over A is defined by:

(Def.13) $\sqcap_A(K, L) = \mu(K \frown L)$.

One can prove the following propositions:

(62) $\sqcup_A(K, L) = \mu(K \cup L)$.

(63) $\sqcap_A(K, L) = \mu(K \frown L)$.

Let A be a non-empty set, and let B be a non-empty subset of A, and let O be a binary operation on B, and let a, b be elements of B. Then $O(a, b)$ is an element of B.

One can prove the following propositions:

(64) $\mu B \subseteq B$.

(65) If $b \in B$, then there exists c such that $c \subseteq b$ and $c \in \mu B$.

(66) $\mu K = K$.

(67) $\mu(B \cup C) \subseteq \mu B \cup C$.

(68) $\mu(\mu B \cup C) = \mu(B \cup C)$.

(69) $\mu(B \cup \mu C) = \mu(B \cup C)$.

(70) If $B \subseteq C$, then $B \frown D \subseteq C \frown D$.

(71) $\mu(B \frown C) \subseteq \mu B \frown C$.

(72) $B \frown C = C \frown B$.

(73) If $B \subseteq C$, then $D \frown B \subseteq D \frown C$.

(74) $\mu(\mu B \frown C) = \mu(B \frown C)$.

(75) $\mu(B \frown \mu C) = \mu(B \frown C)$.

(76) $K \frown (L \frown M) = K \frown L \frown M$.

(77) $K \frown (L \cup M) = K \frown L \cup K \frown M$.

(78) $B \subseteq B \frown B$.

(79) $\mu(K \frown K) = \mu K$.

Let us consider A. The lattice of normal forms over A yields a lower bound lattice and is defined as follows:

(Def.14) the lattice of normal forms over $A = \langle$the normal forms over $A, \sqcup_A, \sqcap_A\rangle$.

The following propositions are true:

(80) The lattice of normal forms over $A = \langle$the normal forms over $A, \sqcup_A, \sqcap_A\rangle$.

(81) The lattice of normal forms over A is a distributive lattice.

(82) The carrier of the lattice of normal forms over $A =$ the normal forms over A.

(83) The join operation of the lattice of normal forms over $A = \sqcup_A$.

(84) The meet operation of the lattice of normal forms over $A = \sqcap_A$.

(85) $\emptyset$ is an element of the carrier of the lattice of normal forms over A.

(86) $\perp_{\text{The lattice of normal forms over } A} = \emptyset$.

(87) The join operation of the lattice of normal forms over A has a unity.

References

[1] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 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] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

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

[7] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.

[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[9] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

[10] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.

[11] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

Received October 5, 1990

FORMALIZED MATHEMATICS
Vol.2, No.2, March–April 1991
Université Catholique de Louvain

Ordered Rings - Part I

Michał Muzalewski
Warsaw University
Białystok

Lesław W. Szczerba
Siedlce University

Summary. This series of papers is devoted to the notion of the ordered ring, and one of its most important cases: the notion of ordered field. It follows the results of [5]. The idea of the notion of order in the ring is based on that of positive cone i.e. the set of positive elements. Positive cone has to contain at least squares of all elements, and has to be closed under sum and product. Therefore the key notions of this theory are that of square, sum of squares, product of squares, etc. and finally elements generated from squares by means of sums and products. Part I contains definitions of all those key notions and inclusions between them.

MML Identifier: `O_RING_1`.

The papers [1], [2], [6], [3], and [4] provide the notation and terminology for this paper. For simplicity we adopt the following convention: i, j, k, n will be natural numbers, R will be a field structure, x, y will be scalars of R, and f will be a finite sequence of elements of the carrier of R. Let us consider R, f, k. Let us assume that $0 \neq k$ and $k \leq \operatorname{len} f$. The functor $f \circ k$ yields a scalar of R and is defined by:

(Def.1) $f \circ k = f(k)$.

Let us consider R, x. The functor $x^{\mathbf{2}}$ yields a scalar of R and is defined as follows:

(Def.2) $x^{\mathbf{2}} = x \cdot x$.

Let us consider R, x. We say that x is a square if and only if:

(Def.3) there exists a scalar y of R such that $x = y^{\mathbf{2}}$.

Let us consider R, f. We say that f is a sequence of sums of squares if and only if:

(Def.4) $\operatorname{len} f \neq 0$ and $f \circ 1$ is a square and for every n such that $n \neq 0$ and $n < \operatorname{len} f$ there exists y such that y is a square and $f \circ (n+1) = f \circ n + y$.

Let us consider R, x. We say that x is a sum of squares if and only if:

ISSN 0777–4028

(Def.5) there exists f such that f is a sequence of sums of squares and $x = f \circ \operatorname{len} f$.

Let us consider R, f. We say that f is a sequence of products of squares if and only if:

(Def.6) $\operatorname{len} f \neq 0$ and $f \circ 1$ is a square and for every n such that $n \neq 0$ and $n < \operatorname{len} f$ there exists y such that y is a square and $f \circ (n+1) = f \circ n \cdot y$.

Let us consider R, x. We say that x is a product of squares if and only if:

(Def.7) there exists f such that f is a sequence of products of squares and $x = f \circ \operatorname{len} f$.

Let us consider R, f. We say that f is a sequence of sums of products of squares if and only if:

(Def.8) $\operatorname{len} f \neq 0$ and $f \circ 1$ is a product of squares and for every n such that $n \neq 0$ and $n < \operatorname{len} f$ there exists y such that y is a product of squares and $f \circ (n+1) = f \circ n + y$.

Let us consider R, x. We say that x is a sum of products of squares if and only if:

(Def.9) there exists f such that f is a sequence of sums of products of squares and $x = f \circ \operatorname{len} f$.

Let us consider R, f. We say that f is a sequence of amalgams of squares if and only if:

(Def.10) (i) $\operatorname{len} f \neq 0$,

(ii) for every n such that $n \neq 0$ and $n \leq \operatorname{len} f$ holds $f \circ n$ is a product of squares or there exist i, j such that $f \circ n = f \circ i \cdot f \circ j$ and $i \neq 0$ and $i < n$ and $j \neq 0$ and $j < n$.

Let us consider R, x. We say that x is a amalgam of squares if and only if:

(Def.11) there exists f such that f is a sequence of amalgams of squares and $x = f \circ \operatorname{len} f$.

Let us consider R, f. We say that f is a sequence of sums of amalgams of squares if and only if:

(Def.12) $\operatorname{len} f \neq 0$ and $f \circ 1$ is a amalgam of squares and for every n such that $n \neq 0$ and $n < \operatorname{len} f$ there exists y such that y is a amalgam of squares and $f \circ (n+1) = f \circ n + y$.

Let us consider R, x. We say that x is a sum of amalgams of squares if and only if:

(Def.13) there exists f such that f is a sequence of sums of amalgams of squares and $x = f \circ \operatorname{len} f$.

Let us consider R, f. We say that f is a generation from squares if and only if:

(Def.14) (i) $\operatorname{len} f \neq 0$,

(ii) for every n such that $n \neq 0$ and $n \leq \operatorname{len} f$ holds $f \circ n$ is a amalgam of squares or there exist i, j such that $f \circ n = f \circ i \cdot f \circ j$ or $f \circ n = f \circ i + f \circ j$ but $i \neq 0$ and $i < n$ and $j \neq 0$ and $j < n$.

Let us consider R, x. We say that x is generated from squares if and only if:

(Def.15) there exists f such that f is a generation from squares and $x = f \circ \operatorname{len} f$.

The following propositions are true:

(1) If x is a square, then x is a sum of squares and x is a product of squares and x is a sum of products of squares and x is a amalgam of squares and x is a sum of amalgams of squares and x is generated from squares.

(2) If x is a sum of squares, then x is a sum of products of squares and x is a sum of amalgams of squares and x is generated from squares.

(3) If x is a product of squares, then x is a sum of products of squares and x is a amalgam of squares and x is a sum of amalgams of squares and x is generated from squares.

(4) If x is a sum of products of squares, then x is a sum of amalgams of squares and x is generated from squares.

(5) If x is a amalgam of squares, then x is a sum of amalgams of squares and x is generated from squares.

(6) If x is a sum of amalgams of squares, then x is generated from squares.

References

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

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

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

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

[5] Wanda Szmielew. *From Affine to Euclidean Geometry.* Volume 27, PWN – D.Reidel Publ. Co., Warszawa – Dordrecht, 1983.

[6] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

Received October 11, 1990

FORMALIZED MATHEMATICS
Vol.2, No.2, March–April 1991
Université Catholique de Louvain

Ordered Rings - Part II

Michał Muzalewski
Warsaw University
Białystok

Lesław W. Szczerba
Siedlce University

Summary. This series of papers is devoted to the notion of the ordered ring, and one of its most important cases: the notion of ordered field. It follows the results of [6]. The idea of the notion of order in the ring is based on that of positive cone i.e. the set of positive elements. Positive cone has to contain at least squares of all elements, and has to be closed under sum and product. Therefore the key notions of this theory are that of square, sum of squares, product of squares, etc. and finally elements generated from squares by means of sums and products. Part II contains the classification of sums of such elements.

MML Identifier: O_RING_2.

The terminology and notation used here are introduced in the following articles: [1], [2], [7], [3], [4], and [5]. In the sequel R is a field structure and x, y are scalars of R. One can prove the following propositions:

(1) If x is a square and y is a square or x is a sum of squares and y is a square, then $x+y$ is a sum of squares.

(2) If x is a sum of products of squares and y is a square or x is a sum of products of squares and y is a product of squares, then $x+y$ is a sum of products of squares.

(3) If x is a amalgam of squares and y is a product of squares or x is a amalgam of squares and y is a amalgam of squares or x is a sum of amalgams of squares and y is a square or x is a sum of amalgams of squares and y is a product of squares or x is a sum of amalgams of squares and y is a amalgam of squares, then $x+y$ is a sum of amalgams of squares.

(4) If x is a square and y is a sum of squares or x is a square and y is a product of squares or x is a square and y is a sum of products of squares or x is a square and y is a amalgam of squares or x is a square and y is a sum of amalgams of squares or x is a square and y is generated from squares, then $x+y$ is generated from squares.

ISSN 0777–4028

(5) If x is a sum of squares and y is a sum of squares or x is a sum of squares and y is a product of squares or x is a sum of squares and y is a sum of products of squares or x is a sum of squares and y is a amalgam of squares or x is a sum of squares and y is a sum of amalgams of squares or x is a sum of squares and y is generated from squares, then $x + y$ is generated from squares.

(6) If x is a product of squares and y is a square or x is a product of squares and y is a sum of squares or x is a product of squares and y is a product of squares or x is a product of squares and y is a sum of products of squares or x is a product of squares and y is a amalgam of squares or x is a product of squares and y is a sum of amalgams of squares or x is a product of squares and y is generated from squares, then $x + y$ is generated from squares.

(7) If x is a sum of products of squares and y is a sum of squares or x is a sum of products of squares and y is a sum of products of squares or x is a sum of products of squares and y is a amalgam of squares or x is a sum of products of squares and y is a sum of amalgams of squares or x is a sum of products of squares and y is generated from squares, then $x + y$ is generated from squares.

(8) If x is a amalgam of squares and y is a square or x is a amalgam of squares and y is a sum of squares or x is a amalgam of squares and y is a sum of products of squares or x is a amalgam of squares and y is a sum of amalgams of squares or x is a amalgam of squares and y is generated from squares, then $x + y$ is generated from squares.

(9) If x is a sum of amalgams of squares and y is a sum of squares or x is a sum of amalgams of squares and y is a sum of products of squares or x is a sum of amalgams of squares and y is a sum of amalgams of squares or x is a sum of amalgams of squares and y is generated from squares, then $x + y$ is generated from squares.

(10) If x is generated from squares and y is a square or x is generated from squares and y is a sum of squares or x is generated from squares and y is a product of squares or x is generated from squares and y is a sum of products of squares or x is generated from squares and y is a amalgam of squares or x is generated from squares and y is a sum of amalgams of squares or x is generated from squares and y is generated from squares, then $x + y$ is generated from squares.

References

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

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

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

[4] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[5] Michał Muzalewski and Lesław W. Szczerba. Ordered rings - part I. *Formalized Mathematics*, 2(**2**):243–245, 1991.
[6] Wanda Szmielew. *From Affine to Euclidean Geometry.* Volume 27, PWN – D.Reidel Publ. Co., Warszawa – Dordrecht, 1983.
[7] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

Received October 11, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Ordered Rings - Part III

Michał Muzalewski
Warsaw University
Białystok

Lesław W. Szczerba
Siedlce University

Summary. This series of papers is devoted to the notion of the ordered ring, and one of its most important cases: the notion of ordered field. It follows the results of [6]. The idea of the notion of order in the ring is based on that of positive cone i.e. the set of positive elements. Positive cone has to contain at least squares of all elements, and has to be closed under sum and product. Therefore the key notions of this theory are that of square, sum of squares, product of squares, etc. and finally elements generated from squares by means of sums and products. Part III contains the classification of products of such elements.

MML Identifier: `O_RING_3`.

The papers [1], [2], [7], [3], [4], and [5] provide the terminology and notation for this paper. In the sequel R will denote a field structure and x, y will denote scalars of R. Next we state a number of propositions:

(1) If x is a square and y is a square, then $x \cdot y$ is a product of squares.

(2) If x is a product of squares and y is a square, then $x \cdot y$ is a product of squares.

(3) If x is a square and y is a product of squares or x is a square and y is a amalgam of squares, then $x \cdot y$ is a amalgam of squares.

(4) If x is a product of squares and y is a product of squares or x is a product of squares and y is a amalgam of squares, then $x \cdot y$ is a amalgam of squares.

(5) If x is a amalgam of squares and y is a square or x is a amalgam of squares and y is a product of squares or x is a amalgam of squares and y is a amalgam of squares, then $x \cdot y$ is a amalgam of squares.

(6) If x is a square and y is a sum of squares or x is a square and y is a sum of products of squares or x is a square and y is a sum of amalgams of squares or x is a square and y is generated from squares, then $x \cdot y$ is generated from squares.

ISSN 0777–4028

(7) If x is a sum of squares and y is a square or x is a sum of squares and y is a sum of squares or x is a sum of squares and y is a product of squares or x is a sum of squares and y is a sum of products of squares or x is a sum of squares and y is a amalgam of squares or x is a sum of squares and y is a sum of amalgams of squares or x is a sum of squares and y is generated from squares, then $x \cdot y$ is generated from squares.

(8) If x is a product of squares and y is a sum of squares or x is a product of squares and y is a sum of products of squares or x is a product of squares and y is a sum of amalgams of squares or x is a product of squares and y is generated from squares, then $x \cdot y$ is generated from squares.

(9) If x is a sum of products of squares and y is a square or x is a sum of products of squares and y is a sum of squares or x is a sum of products of squares and y is a product of squares or x is a sum of products of squares and y is a sum of products of squares or x is a sum of products of squares and y is a amalgam of squares or x is a sum of products of squares and y is a sum of amalgams of squares or x is a sum of products of squares and y is generated from squares, then $x \cdot y$ is generated from squares.

(10) If x is a amalgam of squares and y is a sum of squares or x is a amalgam of squares and y is a sum of products of squares or x is a amalgam of squares and y is a sum of amalgams of squares or x is a amalgam of squares and y is generated from squares, then $x \cdot y$ is generated from squares.

(11) If x is a sum of amalgams of squares and y is a square or x is a sum of amalgams of squares and y is a sum of squares or x is a sum of amalgams of squares and y is a product of squares or x is a sum of amalgams of squares and y is a sum of products of squares or x is a sum of amalgams of squares and y is a amalgam of squares or x is a sum of amalgams of squares and y is a sum of amalgams of squares or x is a sum of amalgams of squares and y is generated from squares, then $x \cdot y$ is generated from squares.

(12) If x is generated from squares and y is a square or x is generated from squares and y is a sum of squares or x is generated from squares and y is a product of squares or x is generated from squares and y is a sum of products of squares or x is generated from squares and y is a amalgam of squares or x is generated from squares and y is a sum of amalgams of squares or x is generated from squares and y is generated from squares, then $x \cdot y$ is generated from squares.

References

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

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

[3] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[4] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[5] Michał Muzalewski and Lesław W. Szczerba. Ordered rings - part I. *Formalized Mathematics*, 2(**2**):243–245, 1991.
[6] Wanda Szmielew. *From Affine to Euclidean Geometry.* Volume 27, PWN – D.Reidel Publ. Co., Warszawa – Dordrecht, 1983.
[7] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

Received October 11, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

N-Tuples and Cartesian Products for n=5 [1]

Michał Muzalewski
Warsaw University
Białystok

Wojciech Skaba
University of Toruń

Summary. This article defines ordered n-tuples, projections and Cartesian products for n=5. We prove many theorems concerning the basic properties of the n-tuples and Cartesian products that may be utilized in several further, more challenging applications. A few of these theorems are a strightforward consequence of the regularity axiom. The article originated as an upgrade of the article [5].

MML Identifier: `MCART_2`.

The notation and terminology used in this paper are introduced in the following articles: [4], [3], [6], [2], [1], and [5]. For simplicity we follow a convention: v will be arbitrary, x_1, x_2, x_3, x_4, x_5 will be arbitrary, y_1, y_2, y_3, y_4, y_5 will be arbitrary, z will be arbitrary, X, X_1, X_2, X_3, X_4, X_5 will denote sets, Y, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7 will denote sets, Z will denote a set, x_6 will denote an element of X_1, x_7 will denote an element of X_2, x_8 will denote an element of X_3, and x_9 will denote an element of X_4. We now state two propositions:

(1) If $X \neq \emptyset$, then there exists Y such that $Y \in X$ and for all Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 such that $Y_1 \in Y_2$ and $Y_2 \in Y_3$ and $Y_3 \in Y_4$ and $Y_4 \in Y_5$ and $Y_5 \in Y_6$ and $Y_6 \in Y$ holds Y_1 misses X.

(2) If $X \neq \emptyset$, then there exists Y such that $Y \in X$ and for all Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7 such that $Y_1 \in Y_2$ and $Y_2 \in Y_3$ and $Y_3 \in Y_4$ and $Y_4 \in Y_5$ and $Y_5 \in Y_6$ and $Y_6 \in Y_7$ and $Y_7 \in Y$ holds Y_1 misses X.

Let us consider x_1, x_2, x_3, x_4, x_5. The functor $\langle x_1, x_2, x_3, x_4, x_5 \rangle$ is defined as follows:

(Def.1) $\langle x_1, x_2, x_3, x_4, x_5 \rangle = \langle \langle x_1, x_2, x_3, x_4 \rangle, x_5 \rangle$.

One can prove the following propositions:

(3) $\langle x_1, x_2, x_3, x_4, x_5 \rangle = \langle \langle \langle \langle x_1, x_2 \rangle, x_3 \rangle, x_4 \rangle, x_5 \rangle$.

(4) $\langle x_1, x_2, x_3, x_4, x_5 \rangle = \langle \langle x_1, x_2, x_3, x_4 \rangle, x_5 \rangle$.

[1] Supported by RPBP.III-24.C6

ISSN 0777–4028

(5) $\langle x_1, x_2, x_3, x_4, x_5\rangle = \langle\langle x_1, x_2, x_3\rangle, x_4, x_5\rangle$.

(6) $\langle x_1, x_2, x_3, x_4, x_5\rangle = \langle\langle x_1, x_2\rangle, x_3, x_4, x_5\rangle$.

(7) If $\langle x_1, x_2, x_3, x_4, x_5\rangle = \langle y_1, y_2, y_3, y_4, y_5\rangle$, then $x_1 = y_1$ and $x_2 = y_2$ and $x_3 = y_3$ and $x_4 = y_4$ and $x_5 = y_5$.

(8) If $X \neq \emptyset$, then there exists v such that $v \in X$ and for no x_1, x_2, x_3, x_4, x_5 holds $x_1 \in X$ or $x_2 \in X$ but $v = \langle x_1, x_2, x_3, x_4, x_5\rangle$.

Let us consider X_1, X_2, X_3, X_4, X_5. The functor $[: X_1, X_2, X_3, X_4, X_5 :]$ yields a set and is defined as follows:

(Def.2) $[: X_1, X_2, X_3, X_4, X_5 :] = [: [: X_1, X_2, X_3, X_4 :], X_5 :]$.

The following propositions are true:

(9) $[: X_1, X_2, X_3, X_4, X_5 :] = [: [: [: [: X_1, X_2 :], X_3 :], X_4 :], X_5 :]$.

(10) $[: X_1, X_2, X_3, X_4, X_5 :] = [: [: X_1, X_2, X_3, X_4 :], X_5 :]$.

(11) $[: X_1, X_2, X_3, X_4, X_5 :] = [: [: X_1, X_2, X_3 :], X_4, X_5 :]$.

(12) $[: X_1, X_2, X_3, X_4, X_5 :] = [: [: X_1, X_2 :], X_3, X_4, X_5 :]$.

(13) $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$ if and only if $[: X_1, X_2, X_3, X_4, X_5 :] \neq \emptyset$.

(14) Suppose $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$. Then if $[: X_1, X_2, X_3, X_4, X_5 :] = [: Y_1, Y_2, Y_3, Y_4, Y_5 :]$, then $X_1 = Y_1$ and $X_2 = Y_2$ and $X_3 = Y_3$ and $X_4 = Y_4$ and $X_5 = Y_5$.

(15) If $[: X_1, X_2, X_3, X_4, X_5 :] \neq \emptyset$ and $[: X_1, X_2, X_3, X_4, X_5 :] = [: Y_1, Y_2, Y_3, Y_4, Y_5 :]$, then $X_1 = Y_1$ and $X_2 = Y_2$ and $X_3 = Y_3$ and $X_4 = Y_4$ and $X_5 = Y_5$.

(16) If $[: X, X, X, X, X :] = [: Y, Y, Y, Y, Y :]$, then $X = Y$.

In the sequel x_{10} will be an element of X_5. We now state the proposition

(17) If $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$, then for every element x of $[: X_1, X_2, X_3, X_4, X_5 :]$ there exist x_6, x_7, x_8, x_9, x_{10} such that $x = \langle x_6, x_7, x_8, x_9, x_{10}\rangle$.

We now define five new functors. Let us consider X_1, X_2, X_3, X_4, X_5. Let us assume that $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$. Let x be an element of $[: X_1, X_2, X_3, X_4, X_5 :]$. The functor $x_{\mathbf{1}}$ yields an element of X_1 and is defined as follows:

(Def.3) if $x = \langle x_1, x_2, x_3, x_4, x_5\rangle$, then $x_{\mathbf{1}} = x_1$.

The functor $x_{\mathbf{2}}$ yields an element of X_2 and is defined as follows:

(Def.4) if $x = \langle x_1, x_2, x_3, x_4, x_5\rangle$, then $x_{\mathbf{2}} = x_2$.

The functor $x_{\mathbf{3}}$ yielding an element of X_3 is defined as follows:

(Def.5) if $x = \langle x_1, x_2, x_3, x_4, x_5\rangle$, then $x_{\mathbf{3}} = x_3$.

The functor $x_{\mathbf{4}}$ yielding an element of X_4 is defined as follows:

(Def.6) if $x = \langle x_1, x_2, x_3, x_4, x_5\rangle$, then $x_{\mathbf{4}} = x_4$.

The functor $x_{\mathbf{5}}$ yields an element of X_5 and is defined by:

(Def.7) if $x = \langle x_1, x_2, x_3, x_4, x_5\rangle$, then $x_{\mathbf{5}} = x_5$.

One can prove the following propositions:

(18) Suppose $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$. Then for every element x of $[\!: X_1, X_2, X_3, X_4, X_5 :\!]$ and for all x_1, x_2, x_3, x_4, x_5 such that $x = \langle x_1, x_2, x_3, x_4, x_5 \rangle$ holds $x_{\mathbf{1}} = x_1$ and $x_{\mathbf{2}} = x_2$ and $x_{\mathbf{3}} = x_3$ and $x_{\mathbf{4}} = x_4$ and $x_{\mathbf{5}} = x_5$.

(19) If $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$, then for every element x of $[\!: X_1, X_2, X_3, X_4, X_5 :\!]$ holds $x = \langle x_{\mathbf{1}}, x_{\mathbf{2}}, x_{\mathbf{3}}, x_{\mathbf{4}}, x_{\mathbf{5}} \rangle$.

(20) Suppose $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$. Let x be an element of $[\!: X_1, X_2, X_3, X_4, X_5 :\!]$. Then $x_{\mathbf{1}} = x\,\mathbf{qua}\,any_{\mathbf{1111}}$ and $x_{\mathbf{2}} = x\,\mathbf{qua}\,any_{\mathbf{1112}}$ and $x_{\mathbf{3}} = x\,\mathbf{qua}\,any_{\mathbf{112}}$ and $x_{\mathbf{4}} = x\,\mathbf{qua}\,any_{\mathbf{12}}$ and $x_{\mathbf{5}} = x\,\mathbf{qua}\,any_{\mathbf{2}}$.

(21) If $X_1 \subseteq [\!: X_1, X_2, X_3, X_4, X_5 :\!]$ or $X_1 \subseteq [\!: X_2, X_3, X_4, X_5, X_1 :\!]$ or $X_1 \subseteq [\!: X_3, X_4, X_5, X_1, X_2 :\!]$ or $X_1 \subseteq [\!: X_4, X_5, X_1, X_2, X_3 :\!]$ or $X_1 \subseteq [\!: X_5, X_1, X_2, X_3, X_4 :\!]$, then $X_1 = \emptyset$.

(22) If $[\!: X_1, X_2, X_3, X_4, X_5 :\!]$ meets $[\!: Y_1, Y_2, Y_3, Y_4, Y_5 :\!]$, then X_1 meets Y_1 and X_2 meets Y_2 and X_3 meets Y_3 and X_4 meets Y_4 and X_5 meets Y_5.

(23) $[\!: \{x_1\}, \{x_2\}, \{x_3\}, \{x_4\}, \{x_5\} :\!] = \{\langle x_1, x_2, x_3, x_4, x_5 \rangle\}$.

For simplicity we adopt the following rules: A_1 is a subset of X_1, A_2 is a subset of X_2, A_3 is a subset of X_3, A_4 is a subset of X_4, A_5 is a subset of X_5, and x is an element of $[\!: X_1, X_2, X_3, X_4, X_5 :\!]$. One can prove the following propositions:

(24) Suppose $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$. Then for all x_1, x_2, x_3, x_4, x_5 such that $x = \langle x_1, x_2, x_3, x_4, x_5 \rangle$ holds $x_{\mathbf{1}} = x_1$ and $x_{\mathbf{2}} = x_2$ and $x_{\mathbf{3}} = x_3$ and $x_{\mathbf{4}} = x_4$ and $x_{\mathbf{5}} = x_5$.

(25) If $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$ and for all $x_6, x_7, x_8, x_9, x_{10}$ such that $x = \langle x_6, x_7, x_8, x_9, x_{10} \rangle$ holds $y_1 = x_6$, then $y_1 = x_{\mathbf{1}}$.

(26) If $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$ and for all $x_6, x_7, x_8, x_9, x_{10}$ such that $x = \langle x_6, x_7, x_8, x_9, x_{10} \rangle$ holds $y_2 = x_7$, then $y_2 = x_{\mathbf{2}}$.

(27) If $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$ and for all $x_6, x_7, x_8, x_9, x_{10}$ such that $x = \langle x_6, x_7, x_8, x_9, x_{10} \rangle$ holds $y_3 = x_8$, then $y_3 = x_{\mathbf{3}}$.

(28) If $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$ and for all $x_6, x_7, x_8, x_9, x_{10}$ such that $x = \langle x_6, x_7, x_8, x_9, x_{10} \rangle$ holds $y_4 = x_9$, then $y_4 = x_{\mathbf{4}}$.

(29) If $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$ and for all $x_6, x_7, x_8, x_9, x_{10}$ such that $x = \langle x_6, x_7, x_8, x_9, x_{10} \rangle$ holds $y_5 = x_{10}$, then $y_5 = x_{\mathbf{5}}$.

(30) If $z \in [\!: X_1, X_2, X_3, X_4, X_5 :\!]$, then there exist x_1, x_2, x_3, x_4, x_5 such that $x_1 \in X_1$ and $x_2 \in X_2$ and $x_3 \in X_3$ and $x_4 \in X_4$ and $x_5 \in X_5$ and $z = \langle x_1, x_2, x_3, x_4, x_5 \rangle$.

(31) $\langle x_1, x_2, x_3, x_4, x_5\rangle \in [: X_1, X_2, X_3, X_4, X_5 :]$ if and only if $x_1 \in X_1$ and $x_2 \in X_2$ and $x_3 \in X_3$ and $x_4 \in X_4$ and $x_5 \in X_5$.

(32) If for every z holds $z \in Z$ if and only if there exist x_1, x_2, x_3, x_4, x_5 such that $x_1 \in X_1$ and $x_2 \in X_2$ and $x_3 \in X_3$ and $x_4 \in X_4$ and $x_5 \in X_5$ and $z = \langle x_1, x_2, x_3, x_4, x_5\rangle$, then $Z = [: X_1, X_2, X_3, X_4, X_5 :]$.

(33) Suppose $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$ and $X_5 \neq \emptyset$ and $Y_1 \neq \emptyset$ and $Y_2 \neq \emptyset$ and $Y_3 \neq \emptyset$ and $Y_4 \neq \emptyset$ and $Y_5 \neq \emptyset$. Let x be an element of $[: X_1, X_2, X_3, X_4, X_5 :]$. Then for every element y of $[: Y_1, Y_2, Y_3, Y_4, Y_5 :]$ such that $x = y$ holds $x_{\mathbf{1}} = y_{\mathbf{1}}$ and $x_{\mathbf{2}} = y_{\mathbf{2}}$ and $x_{\mathbf{3}} = y_{\mathbf{3}}$ and $x_{\mathbf{4}} = y_{\mathbf{4}}$ and $x_{\mathbf{5}} = y_{\mathbf{5}}$.

(34) For every element x of $[: X_1, X_2, X_3, X_4, X_5 :]$ such that $x \in [: A_1, A_2, A_3, A_4, A_5 :]$ holds $x_{\mathbf{1}} \in A_1$ and $x_{\mathbf{2}} \in A_2$ and $x_{\mathbf{3}} \in A_3$ and $x_{\mathbf{4}} \in A_4$ and $x_{\mathbf{5}} \in A_5$.

(35) If $X_1 \subseteq Y_1$ and $X_2 \subseteq Y_2$ and $X_3 \subseteq Y_3$ and $X_4 \subseteq Y_4$ and $X_5 \subseteq Y_5$, then $[: X_1, X_2, X_3, X_4, X_5 :] \subseteq [: Y_1, Y_2, Y_3, Y_4, Y_5 :]$.

Let us consider X_1, X_2, X_3, X_4, X_5, A_1, A_2, A_3, A_4, A_5. Then $[: A_1, A_2, A_3, A_4, A_5 :]$ is a subset of $[: X_1, X_2, X_3, X_4, X_5 :]$.

The following three propositions are true:

(36) If $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$, then for every element x_{11} of $[: X_1, X_2 :]$ there exists an element x_6 of X_1 and there exists an element x_7 of X_2 such that $x_{11} = \langle x_6, x_7\rangle$.

(37) If $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$, then for every element x_{11} of $[: X_1, X_2, X_3 :]$ there exist x_6, x_7, x_8 such that $x_{11} = \langle x_6, x_7, x_8\rangle$.

(38) If $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$ and $X_3 \neq \emptyset$ and $X_4 \neq \emptyset$, then for every element x_{11} of $[: X_1, X_2, X_3, X_4 :]$ there exist x_6, x_7, x_8, x_9 such that $x_{11} = \langle x_6, x_7, x_8, x_9\rangle$.

References

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

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

[3] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[4] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[5] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

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

Received October 13, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Ternary Fields [1]

Michał Muzalewski
Warsaw University
Białystok

Wojciech Skaba
University of Toruń

Summary. The article contains part 3 of the set of papers concerning the theory of algebraic structures, based on the book [11] pp. 13-15 (pages 6-8 for English edition).

First the basic structure (F, 0, 1, T) is defined, where T is a ternary operation on F (three-argument operations have been introduced in the article [9]). Following it, the basic axioms of a Ternary Field are displayed, the mode is defined and its existence proved. The basic properties of a Ternary Field are also contemplated there.

MML Identifier: `ALGSTR_3`.

The articles [13], [12], [3], [4], [1], [2], [6], [5], [7], [8], [10], and [9] provide the notation and terminology for this paper. We consider ternary field structures which are systems

⟨a carrier, a zero, a unity, a operation⟩,

where the carrier is a non-empty set, the zero is an element of the carrier, the unity is an element of the carrier, and the operation is a ternary operation on the carrier.

In the sequel F denotes a ternary field structure. Let us consider F. A scalar of F is an element of the carrier of F.

In the sequel a, b, c are scalars of F. Let us consider F, a, b, c. The functor $\mathrm{T}(a, b, c)$ yields a scalar of F and is defined by:

(Def.1) $\mathrm{T}(a, b, c) =$ (the operation of F)(a, b, c).

Let us consider F. The functor 0_F yielding a scalar of F is defined as follows:

(Def.2) $0_F =$ the zero of F.

Let us consider F. The functor 1_F yields a scalar of F and is defined by:

(Def.3) $1_F =$ the unity of F.

The ternary operation $\mathrm{T}_{\mathbb{R}}$ on $\mathbb{R}$ is defined as follows:

[1] Supported by RPBP.III-24.C6

ISSN 0777–4028

(Def.4) for all real numbers a, b, c holds $\mathrm{T}_{\mathbb{R}}(a, b, c) = a \cdot b + c$.

The ternary field structure $\mathbb{R}_{\mathrm{t}}$ is defined by:

(Def.5) $\mathbb{R}_{\mathrm{t}} = \langle \mathbb{R}, 0, 1, \mathrm{T}_{\mathbb{R}} \rangle$.

Let a, b, c be scalars of $\mathbb{R}_{\mathrm{t}}$. The functor $\mathrm{T}^e(a, b, c)$ yields a scalar of $\mathbb{R}_{\mathrm{t}}$ and is defined by:

(Def.6) $\mathrm{T}^e(a, b, c) =$ (the operation of $\mathbb{R}_{\mathrm{t}}$)(a, b, c).

We now state several propositions:

(1) For every scalar a of $\mathbb{R}_{\mathrm{t}}$ holds a is a real number.

(2) For every real number a holds a is a scalar of $\mathbb{R}_{\mathrm{t}}$.

(3) For all real numbers u, u', v, v' such that $u \neq u'$ there exists a real number x such that $u \cdot x + v = u' \cdot x + v'$.

(5)[2] For all scalars u, a, v of $\mathbb{R}_{\mathrm{t}}$ and for all real numbers z, x, y such that $u = z$ and $a = x$ and $v = y$ holds $\mathrm{T}(u, a, v) = z \cdot x + y$.

(6) $0 = 0_{\mathbb{R}_{\mathrm{t}}}$.

(7) $1 = 1_{\mathbb{R}_{\mathrm{t}}}$.

A ternary field structure is called a ternary field if:

(Def.7) (i) $0_{\mathrm{it}} \neq 1_{\mathrm{it}}$,

(ii) for every scalar a of it holds $\mathrm{T}(a, 1_{\mathrm{it}}, 0_{\mathrm{it}}) = a$,

(iii) for every scalar a of it holds $\mathrm{T}(1_{\mathrm{it}}, a, 0_{\mathrm{it}}) = a$,

(iv) for all scalars a, b of it holds $\mathrm{T}(a, 0_{\mathrm{it}}, b) = b$,

(v) for all scalars a, b of it holds $\mathrm{T}(0_{\mathrm{it}}, a, b) = b$,

(vi) for every scalars u, a, b of it there exists a scalar v of it such that $\mathrm{T}(u, a, v) = b$,

(vii) for all scalars u, a, v, v' of it such that $\mathrm{T}(u, a, v) = \mathrm{T}(u, a, v')$ holds $v = v'$,

(viii) for all scalars a, a' of it such that $a \neq a'$ for every scalars b, b' of it there exist scalars u, v of it such that $\mathrm{T}(u, a, v) = b$ and $\mathrm{T}(u, a', v) = b'$,

(ix) for all scalars u, u' of it such that $u \neq u'$ for every scalars v, v' of it there exists a scalar a of it such that $\mathrm{T}(u, a, v) = \mathrm{T}(u', a, v')$,

(x) for all scalars a, a', u, u', v, v' of it such that $\mathrm{T}(u, a, v) = \mathrm{T}(u', a, v')$ and $\mathrm{T}(u, a', v) = \mathrm{T}(u', a', v')$ holds $a = a'$ or $u = u'$.

We adopt the following convention: F is a ternary field and a, a', b, c, x, x', u, u', v, v' are scalars of F. We now state several propositions:

(8) If $a \neq a'$ and $\mathrm{T}(u, a, v) = \mathrm{T}(u', a, v')$ and $\mathrm{T}(u, a', v) = \mathrm{T}(u', a', v')$, then $u = u'$ and $v = v'$.

(9) For every a, b, c there exists x such that $\mathrm{T}(a, b, x) = c$.

(10) If $\mathrm{T}(a, b, x) = \mathrm{T}(a, b, x')$, then $x = x'$.

(11) If $a \neq 0_F$, then for every b, c there exists x such that $\mathrm{T}(a, x, b) = c$.

(12) If $a \neq 0_F$ and $\mathrm{T}(a, x, b) = \mathrm{T}(a, x', b)$, then $x = x'$.

(13) If $a \neq 0_F$, then for every b, c there exists x such that $\mathrm{T}(x, a, b) = c$.

[2]The proposition (4) was either repeated or obvious.

(14) If $a \neq 0_F$ and $\mathrm{T}(x, a, b) = \mathrm{T}(x', a, b)$, then $x = x'$.

References

[1] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 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] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[6] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[7] Michał Muzalewski. Midpoint algebras. *Formalized Mathematics*, 1(**3**):483–488, 1990.
[8] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.
[9] Michal Muzalewski and Wojciech Skaba. Three-argument operations and four-argument operations. *Formalized Mathematics*, 2(**2**):221–224, 1991.
[10] Wojciech Skaba and Michał Muzalewski. From double loops to fields. *Formalized Mathematics*, 2(**1**):185–191, 1991.
[11] Wanda Szmielew. *From Affine to Euclidean Geometry*. Volume 27, PWN – D.Reidel Publ. Co., Warszawa – Dordrecht, 1983.
[12] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[13] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

Received October 15, 1990

FORMALIZED MATHEMATICS
Vol.2, No.2, March–April 1991
Université Catholique de Louvain

The σ-additive Measure Theory

Józef Białas
University of Łódź

Summary. The article contains a definition and basic properties of a σ-additive, nonnegative measure, with values in $\overline{\mathbb{R}}$, the enlarged set of real numbers, where $\overline{\mathbb{R}}$ denotes set $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ - by [11]. We present definitions of σ-field of sets, σ-additive measure, measurable sets, measure zero sets and the basic theorems describing relationships between the notions mentioned above. The work is the third part of the series of articles concerning the Lebesgue measure theory.

MML Identifier: `MEASURE1`.

The papers [13], [12], [7], [8], [5], [6], [1], [10], [2], [9], [3], and [4] provide the terminology and notation for this paper. One can prove the following four propositions:

(1) For all sets X, Y holds $\bigcup\{X, Y, \emptyset\} = \bigcup\{X, Y\}$.

(2) For every natural number n holds $n = 0$ or $n = 1$ or $1 < n$.

(4)[1] For all *Real numbers* x, y, s, t such that $0_{\overline{\mathbb{R}}} \leq x$ and $0_{\overline{\mathbb{R}}} \leq s$ and $x \leq y$ and $s \leq t$ holds $x + s \leq y + t$.

(5) For all *Real numbers* x, y, z such that $0_{\overline{\mathbb{R}}} \leq y$ and $0_{\overline{\mathbb{R}}} \leq z$ and $x = y + z$ and $y < +\infty$ holds $z = x - y$.

Let X be a set. A set is called a non-empty family of subsets of X if:

(Def.1) it $\neq \emptyset$ and for an arbitrary A such that $A \in$ it holds $A \in 2^X$.

One can prove the following propositions:

(6) For every set X and for every subset A of X holds $\{A\}$ is a non-empty family of subsets of X.

(7) For every set X and for all subsets A, B of X holds $\{A, B\}$ is a non-empty family of subsets of X.

(8) For every set X and for all subsets A, B, C of X holds $\{A, B, C\}$ is a non-empty family of subsets of X.

[1]The proposition (3) was either repeated or obvious.

ISSN 0777–4028

(9) For every set X holds $\{\emptyset\}$ is a non-empty family of subsets of X.

(10) For every set X holds $\{\emptyset, X\}$ is a non-empty family of subsets of X.

(12)[2] For every set X holds 2^X is a non-empty family of subsets of X.

The scheme *DomsetFamEx* concerns a set $\mathcal{A}$, and a unary predicate $\mathcal{P}$, and states that:

there exists a non-empty family F of subsets of $\mathcal{A}$ such that for every set B holds $B \in F$ if and only if $B \subseteq \mathcal{A}$ and $\mathcal{P}[B]$

provided the following condition is satisfied:

- there exists a set B such that $B \subseteq \mathcal{A}$ and $\mathcal{P}[B]$.

Let X be a set, and let S be a non-empty family of subsets of X. The functor $X \setminus S$ yielding a non-empty family of subsets of X is defined as follows:

(Def.2) for every set A holds $A \in X \setminus S$ if and only if there exists a set B such that $B \in S$ and $A = X \setminus B$.

We now state three propositions:

(13) For every set X and for every non-empty family S of subsets of X and for every set A holds $A \in X \setminus S$ if and only if there exists a set B such that $B \in S$ and $A = X \setminus B$.

(14) For every set X and for every non-empty family S of subsets of X holds $S = X \setminus (X \setminus S)$.

(15) For every set X and for every non-empty family S of subsets of X holds $\bigcap S = X \setminus \bigcup(X \setminus S)$ and $\bigcup S = X \setminus \bigcap(X \setminus S)$.

Let X be a set. A non-empty family of subsets of X is said to be a field of subsets of X if:

(Def.3) for every set A such that $A \in$ it holds $X \setminus A \in$ it and for all sets A, B such that $A \in$ it and $B \in$ it holds $A \cup B \in$ it.

The following propositions are true:

(17)[3] For every set X and for every field S of subsets of X holds $S = X \setminus S$.

(18) For every set X and for an arbitrary M holds M is a field of subsets of X if and only if there exists a non-empty family S of subsets of X such that $M = S$ and for every set A such that $A \in S$ holds $X \setminus A \in S$ and for all sets A, B such that $A \in S$ and $B \in S$ holds $A \cup B \in S$.

(19) For every set X and for every non-empty family S of subsets of X holds S is a field of subsets of X if and only if for every set A such that $A \in S$ holds $X \setminus A \in S$ and for all sets A, B such that $A \in S$ and $B \in S$ holds $A \cap B \in S$.

(20) For every set X and for every field S of subsets of X and for all sets A, B such that $A \in S$ and $B \in S$ holds $A \setminus B \in S$.

(21) For every set X and for every field S of subsets of X holds $\emptyset \in S$ and $X \in S$.

---

[2]The proposition (11) was either repeated or obvious.

[3]The proposition (16) was either repeated or obvious.

Let X be a set, and let S be a non-empty family of subsets of X, and let F be a function from S into $\overline{\mathbb{R}}$, and let A be an element of S. Then $F(A)$ is a *Real number.*

Let F be a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$, and let n be a natural number. Then $F(n)$ is a *Real number.*

Let X be a set, and let S be a non-empty family of subsets of X, and let F be a function from S into $\overline{\mathbb{R}}$. We say that F is non-negative if and only if:

(Def.4) for every element A of S holds $0_{\overline{\mathbb{R}}} \leq F(A)$.

We now state the proposition

(23)[4] For every set X and for every field S of subsets of X there exists a function M from S into $\overline{\mathbb{R}}$ such that M is non-negative and $M(\emptyset) = 0_{\overline{\mathbb{R}}}$ and for all elements A, B of S such that $A \cap B = \emptyset$ holds $M(A \cup B) = M(A) + M(B)$.

Let X be a set, and let S be a field of subsets of X. A function from S into $\overline{\mathbb{R}}$ is called a measure on S if:

(Def.5) it is non-negative and $\mathrm{it}(\emptyset) = 0_{\overline{\mathbb{R}}}$ and for all elements A, B of S such that $A \cap B = \emptyset$ holds $\mathrm{it}(A \cup B) = \mathrm{it}(A) + \mathrm{it}(B)$.

Next we state two propositions:

(25)[5] For every set X and for every field S of subsets of X and for every measure M on S and for all elements A, B of S such that $A \subseteq B$ holds $M(A) \leq M(B)$.

(26) For every set X and for every field S of subsets of X and for every measure M on S and for all elements A, B of S such that $A \subseteq B$ and $M(A) < +\infty$ holds $M(B \setminus A) = M(B) - M(A)$.

Let X be a set, and let S be a field of subsets of X, and let A, B be elements of S. Then $A \cup B$ is an element of S.

Let X be a set, and let S be a field of subsets of X, and let A, B be elements of S. Then $A \cap B$ is an element of S.

Let X be a set, and let S be a field of subsets of X, and let A, B be elements of S. Then $A \setminus B$ is an element of S.

The following proposition is true

(27) For every set X and for every field S of subsets of X and for every measure M on S and for all elements A, B of S holds $M(A \cup B) \leq M(A) + M(B)$.

Let X be a set, and let S be a field of subsets of X, and let M be a measure on S, and let A be a set. We say that A is measurable w.r.t. M if and only if:

(Def.6) $A \in S$.

The following proposition is true

[4]The proposition (22) was either repeated or obvious.
[5]The proposition (24) was either repeated or obvious.

(29)[6] For every set X and for every field S of subsets of X and for every measure M on S holds $\emptyset$ is measurable w.r.t. M and X is measurable w.r.t. M and for all sets A, B such that A is measurable w.r.t. M and B is measurable w.r.t. M holds $X \setminus A$ is measurable w.r.t. M and $A \cup B$ is measurable w.r.t. M and $A \cap B$ is measurable w.r.t. M.

Let X be a set, and let S be a field of subsets of X, and let M be a measure on S. An element of S is called a set of measure zero w.r.t. M if:

(Def.7) $M(\mathrm{it}) = 0_{\overline{\mathbb{R}}}$.

The following propositions are true:

(31)[7] For every set X and for every field S of subsets of X and for every measure M on S and for every element A of S and for every set B of measure zero w.r.t. M such that $A \subseteq B$ holds A is a set of measure zero w.r.t. M.

(32) For every set X and for every field S of subsets of X and for every measure M on S and for all sets A, B of measure zero w.r.t. M holds $A \cup B$ is a set of measure zero w.r.t. M and $A \cap B$ is a set of measure zero w.r.t. M and $A \setminus B$ is a set of measure zero w.r.t. M.

(33) For every set X and for every field S of subsets of X and for every measure M on S and for every element A of S and for every set B of measure zero w.r.t. M holds $M(A \cup B) = M(A)$ and $M(A \cap B) = 0_{\overline{\mathbb{R}}}$ and $M(A \setminus B) = M(A)$.

(34) For every set X and for every subset A of X there exists a function F from $\mathbb{N}$ into 2^X such that $\operatorname{rng} F = \{A\}$.

(35) For every set X and for every subset A of X there exists a function F from $\mathbb{N}$ into $\{A\}$ such that for every natural number n holds $F(n) = A$.

Let X be a set. A non-empty family of subsets of X is said to be a denumerable family of subsets of X if:

(Def.8) there exists a function F from $\mathbb{N}$ into 2^X such that $\mathrm{it} = \operatorname{rng} F$.

We now state several propositions:

(37)[8] For every set X and for every denumerable family S of subsets of X there exists a function F from $\mathbb{N}$ into 2^X such that $S = \operatorname{rng} F$.

(38) For every set X and for every subsets A, B, C of X there exists a function F from $\mathbb{N}$ into 2^X such that $\operatorname{rng} F = \{A, B, C\}$ and $F(0) = A$ and $F(1) = B$ and for every natural number n such that $1 < n$ holds $F(n) = C$.

(39) For every set X and for all subsets A, B of X holds $\{A, B, \emptyset\}$ is a denumerable family of subsets of X.

[6]The proposition (28) was either repeated or obvious.
[7]The proposition (30) was either repeated or obvious.
[8]The proposition (36) was either repeated or obvious.

(40) For every set X and for every subsets A, B of X there exists a function F from $\mathbb{N}$ into 2^X such that $\operatorname{rng} F = \{A, B\}$ and $F(0) = A$ and for every natural number n such that $0 < n$ holds $F(n) = B$.

(41) For every set X and for all subsets A, B of X holds $\{A, B\}$ is a denumerable family of subsets of X.

(42) For every set X and for every denumerable family S of subsets of X holds $X \setminus S$ is a denumerable family of subsets of X.

Let X be a set. A non-empty family of subsets of X is said to be a σ-field of subsets of X if:

(Def.9) for every set A such that $A \in$ it holds $X \setminus A \in$ it and for every denumerable family M of subsets of X such that $M \subseteq$ it holds $\bigcup M \in$ it.

One can prove the following propositions:

(44)[9] For every set X and for every non-empty family S of subsets of X such that S is a σ-field of subsets of X holds S is a field of subsets of X.

(45) For every set X and for every σ-field S of subsets of X holds $\emptyset \in S$ and $X \in S$.

(46) For every set X and for every σ-field S of subsets of X and for all sets A, B such that $A \in S$ and $B \in S$ holds $A \cup B \in S$ and $A \cap B \in S$.

(47) For every set X and for every σ-field S of subsets of X and for all sets A, B such that $A \in S$ and $B \in S$ holds $A \setminus B \in S$.

(48) For every set X and for every σ-field S of subsets of X holds $S = X \setminus S$.

(49) For every set X and for every non-empty family S of subsets of X holds S is a σ-field of subsets of X if and only if for every set A such that $A \in S$ holds $X \setminus A \in S$ and for every denumerable family M of subsets of X such that $M \subseteq S$ holds $\bigcap M \in S$.

Let X be a set, and let S be a σ-field of subsets of X. A function from $\mathbb{N}$ into S is said to be a sequence of separated subsets of S if:

(Def.10) for all natural numbers n, m such that $n \neq m$ holds $\mathrm{it}(n) \cap \mathrm{it}(m) = \emptyset$.

We now state the proposition

(51)[10] For every set X and for every σ-field S of subsets of X and for every function F from $\mathbb{N}$ into S and for every function M from S into $\overline{\mathbb{R}}$ holds $M \cdot F$ is a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$.

Let X be a set, and let S be a σ-field of subsets of X, and let F be a function from $\mathbb{N}$ into S. Then $\operatorname{rng} F$ is a non-empty family of subsets of X.

Let X be a set, and let S be a σ-field of subsets of X, and let F be a function from $\mathbb{N}$ into S, and let M be a function from S into $\overline{\mathbb{R}}$. Then $M \cdot F$ is a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$.

Next we state several propositions:

[9] The proposition (43) was either repeated or obvious.
[10] The proposition (50) was either repeated or obvious.

(52) For every set X and for every σ-field S of subsets of X and for every function F from $\mathbb{N}$ into S holds $\operatorname{rng} F$ is a denumerable family of subsets of X.

(53) For every set X and for every σ-field S of subsets of X and for every function F from $\mathbb{N}$ into S holds $\bigcup \operatorname{rng} F$ is an element of S.

(54) For every set X and for every σ-field S of subsets of X and for every function F from $\mathbb{N}$ into S and for every function M from S into $\overline{\mathbb{R}}$ such that M is non-negative holds $M \cdot F$ is non-negative.

(55) For every set X and for every σ-field S of subsets of X and for every *Real numbers* a, b there exists a function M from S into $\overline{\mathbb{R}}$ such that for every element A of S holds if $A = \emptyset$, then $M(A) = a$ but if $A \neq \emptyset$, then $M(A) = b$.

(56) For every set X and for every σ-field S of subsets of X there exists a function M from S into $\overline{\mathbb{R}}$ such that for every element A of S holds if $A = \emptyset$, then $M(A) = 0_{\overline{\mathbb{R}}}$ but if $A \neq \emptyset$, then $M(A) = +\infty$.

(57) For every set X and for every σ-field S of subsets of X there exists a function M from S into $\overline{\mathbb{R}}$ such that for every element A of S holds $M(A) = 0_{\overline{\mathbb{R}}}$.

(58) For every set X and for every σ-field S of subsets of X there exists a function M from S into $\overline{\mathbb{R}}$ such that M is non-negative and $M(\emptyset) = 0_{\overline{\mathbb{R}}}$ and for every sequence F of separated subsets of S holds $\sum(M \cdot F) = M(\bigcup \operatorname{rng} F)$.

Let X be a set, and let S be a σ-field of subsets of X. A function from S into $\overline{\mathbb{R}}$ is said to be a σ-measure on S if:

(Def.11) it is non-negative and $\operatorname{it}(\emptyset) = 0_{\overline{\mathbb{R}}}$ and for every sequence F of separated subsets of S holds $\sum(\operatorname{it} \cdot F) = \operatorname{it}(\bigcup \operatorname{rng} F)$.

Let X be a set. We see that the σ-field of subsets of X is a field of subsets of X.

One can prove the following propositions:

(60)[11] For every set X and for every σ-field S of subsets of X and for every σ-measure M on S holds M is a measure on S.

(61) For every set X and for every σ-field S of subsets of X and for every σ-measure M on S and for all elements A, B of S such that $A \cap B = \emptyset$ holds $M(A \cup B) = M(A) + M(B)$.

(62) For every set X and for every σ-field S of subsets of X and for every σ-measure M on S and for all elements A, B of S such that $A \subseteq B$ holds $M(A) \leq M(B)$.

(63) For every set X and for every σ-field S of subsets of X and for every σ-measure M on S and for all elements A, B of S such that $A \subseteq B$ and $M(A) < +\infty$ holds $M(B \setminus A) = M(B) - M(A)$.

[11]The proposition (59) was either repeated or obvious.

(64) For every set X and for every σ-field S of subsets of X and for every σ-measure M on S and for all elements A, B of S holds $M(A \cup B) \leq M(A) + M(B)$.

Let X be a set, and let S be a σ-field of subsets of X, and let M be a σ-measure on S, and let A be a set. We say that A is measurable w.r.t. M if and only if:

(Def.12) $A \in S$.

Next we state two propositions:

(66)[12] For every set X and for every σ-field S of subsets of X and for every σ-measure M on S holds $\emptyset$ is measurable w.r.t. M and X is measurable w.r.t. M and for all sets A, B such that A is measurable w.r.t. M and B is measurable w.r.t. M holds $X \setminus A$ is measurable w.r.t. M and $A \cup B$ is measurable w.r.t. M and $A \cap B$ is measurable w.r.t. M.

(67) For every set X and for every σ-field S of subsets of X and for every σ-measure M on S and for every denumerable family T of subsets of X such that for every set A such that $A \in T$ holds A is measurable w.r.t. M holds $\bigcup T$ is measurable w.r.t. M and $\bigcap T$ is measurable w.r.t. M.

Let X be a set, and let S be a σ-field of subsets of X, and let M be a σ-measure on S. An element of S is called a set of measure zero w.r.t. M if:

(Def.13) $M(\mathrm{it}) = 0_{\overline{\mathbb{R}}}$.

Next we state three propositions:

(69)[13] For every set X and for every σ-field S of subsets of X and for every σ-measure M on S and for every element A of S and for every set B of measure zero w.r.t. M such that $A \subseteq B$ holds A is a set of measure zero w.r.t. M.

(70) For every set X and for every σ-field S of subsets of X and for every σ-measure M on S and for all sets A, B of measure zero w.r.t. M holds $A \cup B$ is a set of measure zero w.r.t. M and $A \cap B$ is a set of measure zero w.r.t. M and $A \setminus B$ is a set of measure zero w.r.t. M.

(71) For every set X and for every σ-field S of subsets of X and for every σ-measure M on S and for every element A of S and for every set B of measure zero w.r.t. M holds $M(A \cup B) = M(A)$ and $M(A \cap B) = 0_{\overline{\mathbb{R}}}$ and $M(A \setminus B) = M(A)$.

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] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):163–171, 1991.

[12] The proposition (65) was either repeated or obvious.
[13] The proposition (68) was either repeated or obvious.

[4] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.
[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] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[10] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[11] R. Sikorski. *Rachunek różniczkowy i całkowy - funkcje wielu zmiennych.* PWN - Warszawa, 1968.
[12] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[13] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

Received October 15, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Incidence Projective Space (a reduction theorem in a plane) [1]

Eugeniusz Kusak
Warsaw University
Białystok

Wojciech Leończuk
Warsaw University
Białystok

Summary. The article begins with basic facts concernig arbitrary projective spaces. Further we are concerned with Fano projective spaces (we prove it has a rank of at least four). Finally we confine ourselves to Desarguesian planes; we define the notion of perspectivity and we prove the reduction theorem for projectivities with concurrent axes.

MML Identifier: `PROJRED1`.

The articles [6], [8], [5], [7], [9], [10], [4], [3], [1], and [2] provide the terminology and notation for this paper. We adopt the following convention: I_1 will be a projective space defined in terms of incidence, a, b, c, d, p, q, o, r, s will be elements of the points of I_1, and A, B, C, P, Q will be elements of the lines of I_1. We now state a number of propositions:

(1) There exists a such that $a \nmid A$.

(2) There exists A such that $a \nmid A$.

(3) If $A \neq B$, then there exist a, b such that $a \mid A$ and $a \nmid B$ and $b \mid B$ and $b \nmid A$.

(4) If $a \neq b$, then there exist A, B such that $a \mid A$ and $a \nmid B$ and $b \mid B$ and $b \nmid A$.

(5) There exist A, B, C such that $a \mid A$ and $a \mid B$ and $a \mid C$ and $A \neq B$ and $B \neq C$ and $C \neq A$.

(6) There exists a such that $a \nmid A$ and $a \nmid B$.

(7) There exists a such that $a \mid A$.

(8) If $a \mid A$ and $b \mid A$, then there exists c such that $c \mid A$ and $c \neq a$ and $c \neq b$.

[1]Supported by RPBP.III-24.C6

ISSN 0777–4028

(9) There exists A such that $a \nmid A$ and $b \nmid A$.

(10) If $A \neq B$ and $o \mid A$ and $o \mid B$ and $p \mid A$ and $p \neq o$ and $q \mid B$, then $p \neq q$.

(11) If $o \neq a$ and $o \neq b$ and $A \neq B$ and $o \mid A$ and $o \mid B$ and $a \mid A$ and $a \mid C$ and $b \mid B$ and $b \mid C$, then $A \neq C$.

(12) Suppose $o \mid A$ and $o \mid B$ and $A \neq B$ and $a \mid A$ and $o \neq a$ and $b \mid B$ and $c \mid B$ and $b \neq c$ and $a \mid P$ and $b \mid P$ and $a \mid Q$ and $c \mid Q$. Then $P \neq Q$.

(13) If $a, b, c \mid A$, then $a, c, b \mid A$ and $b, a, c \mid A$ and $b, c, a \mid A$ and $c, a, b \mid A$ and $c, b, a \mid A$.

(14) Let I_1 be a Desarguesian projective space defined in terms of incidence. Let o, b_1, a_1, b_2, a_2, b_3, a_3, r, s, t be elements of the points of I_1. Let C_1, C_2, C_3, A_1, A_2, A_3, B_1, B_2, B_3 be elements of the lines of I_1. Suppose that

(i) $o, b_1, a_1 \mid C_1$,
(ii) $o, a_2, b_2 \mid C_2$,
(iii) $o, a_3, b_3 \mid C_3$,
(iv) $a_3, a_2, t \mid A_1$,
(v) $a_3, r, a_1 \mid A_2$,
(vi) $a_2, s, a_1 \mid A_3$,
(vii) $t, b_2, b_3 \mid B_1$,
(viii) $b_1, r, b_3 \mid B_2$,
(ix) $b_1, s, b_2 \mid B_3$,
(x) C_1, C_2, C_3 are mutually different,
(xi) $o \neq a_3$,
(xii) $o \neq b_1$,
(xiii) $o \neq b_2$,
(xiv) $a_2 \neq b_2$.

Then there exists an element O of the lines of I_1 such that $r, s, t \mid O$.

(15) Suppose there exist A, a, b, c, d such that $a \mid A$ and $b \mid A$ and $c \mid A$ and $d \mid A$ and a, b, c, d are mutually different. Then for every B there exist p, q, r, s such that $p \mid B$ and $q \mid B$ and $r \mid B$ and $s \mid B$ and p, q, r, s are mutually different.

We follow a convention: I_1 will be a Fanoian projective space defined in terms of incidence, a, b, c, d, p, q, r, s will be elements of the points of I_1, and A, B, C, D, L, Q, R, S will be elements of the lines of I_1. The following propositions are true:

(16) There exist p, q, r, s, a, b, c, A, B, C, Q, L, R, S, D such that $q \nmid L$ and $r \nmid L$ and $p \nmid Q$ and $s \nmid Q$ and $p \nmid R$ and $r \nmid R$ and $q \nmid S$ and $s \nmid S$ and $a, p, s \mid L$ and $a, q, r \mid Q$ and $b, q, s \mid R$ and $b, p, r \mid S$ and $c, p, q \mid A$ and $c, r, s \mid B$ and $a, b \mid C$ and $c \nmid C$.

(17) There exist a, A, B, C, D such that $a \mid A$ and $a \mid B$ and $a \mid C$ and $a \mid D$ and A, B, C, D are mutually different.

(18) There exist a, b, c, d, A such that $a \mid A$ and $b \mid A$ and $c \mid A$ and $d \mid A$ and a, b, c, d are mutually different.

(19) There exist p, q, r, s such that $p \mid B$ and $q \mid B$ and $r \mid B$ and $s \mid B$ and p, q, r, s are mutually different.

We follow a convention: I_1 will denote a Desarguesian 2-dimensional projective space defined in terms of incidence, c, p, q, x, y will denote elements of the points of I_1, and K, L, R, X will denote elements of the lines of I_1. Let us consider I_1, K, L, p. Let us assume that $p \nmid K$ and $p \nmid L$. The functor $\pi_p(K \to L)$ yields a partial function from the points of I_1 to the points of I_1 and is defined as follows:

(Def.1) $\operatorname{dom} \pi_p(K \to L) \subseteq$ the points of I_1 and for every x holds $x \in \operatorname{dom} \pi_p(K \to L)$ if and only if $x \mid K$ and for all x, y such that $x \mid K$ and $y \mid L$ holds $\pi_p(K \to L)(x) = y$ if and only if there exists X such that $p \mid X$ and $x \mid X$ and $y \mid X$.

One can prove the following propositions:

(20) Suppose $p \nmid K$ and $p \nmid L$. Then
(i) $\operatorname{dom} \pi_p(K \to L) \subseteq$ the points of I_1,
(ii) for every x holds $x \in \operatorname{dom} \pi_p(K \to L)$ if and only if $x \mid K$,
(iii) for all x, y such that $x \mid K$ and $y \mid L$ holds $\pi_p(K \to L)(x) = y$ if and only if there exists X such that $p \mid X$ and $x \mid X$ and $y \mid X$.

(21) If $p \nmid K$, then for every x such that $x \mid K$ holds $\pi_p(K \to K)(x) = x$.

(22) If $p \nmid K$ and $p \nmid L$ and $x \mid K$, then $\pi_p(K \to L)(x)$ is an element of the points of I_1.

(23) If $p \nmid K$ and $p \nmid L$ and $x \mid K$ and $y = \pi_p(K \to L)(x)$, then $y \mid L$.

(24) If $p \nmid K$ and $p \nmid L$ and $y \in \operatorname{rng} \pi_p(K \to L)$, then $y \mid L$.

(25) Suppose $p \nmid K$ and $p \nmid L$ and $q \nmid L$ and $q \nmid R$. Then $\operatorname{dom}(\pi_q(L \to R) \cdot \pi_p(K \to L)) = \operatorname{dom} \pi_p(K \to L)$ and $\operatorname{rng}(\pi_q(L \to R) \cdot \pi_p(K \to L)) = \operatorname{rng} \pi_q(L \to R)$.

(26) Let a_1, b_1, a_2, b_2 be elements of the points of I_1. Then if $p \nmid K$ and $p \nmid L$ and $a_1 \mid K$ and $b_1 \mid K$ and $\pi_p(K \to L)(a_1) = a_2$ and $\pi_p(K \to L)(b_1) = b_2$ and $a_2 = b_2$, then $a_1 = b_1$.

(27) If $p \nmid K$ and $p \nmid L$ and $x \mid K$ and $x \mid L$, then $\pi_p(K \to L)(x) = x$.

We now state the proposition

(28) Suppose $p \nmid K$ and $p \nmid L$ and $q \nmid L$ and $q \nmid R$ and $c \mid K$ and $c \mid L$ and $c \mid R$ and $K \neq R$. Then there exists an element o of the points of I_1 such that $o \nmid K$ and $o \nmid R$ and $\pi_q(L \to R) \cdot \pi_p(K \to L) = \pi_o(K \to R)$.

References

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

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

[3] Wojciech Leończuk and Krzysztof Prażmowski. Incidence projective spaces. *Formalized Mathematics*, 2(**2**):225–232, 1991.

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

[5] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[6] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[7] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[8] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[9] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[10] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received October 16, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Groups, Rings, Left- and Right-Modules [1]

Michał Muzalewski
Warsaw University
Białystok

Wojciech Skaba
University of Toruń

Summary. The notion of group was defined as a group structure introduced in the article [6]. The article contains the basic properties of groups, rings, left- and right-modules of an associative ring.

MML Identifier: `MOD_1`.

The articles [11], [10], [13], [3], [1], [12], [9], [4], [2], [5], [6], [7], and [8] provide the notation and terminology for this paper. A group structure is called a group if:

(Def.1) for all elements x, y, z of it holds $x+y+z = x+(y+z)$ and $x+0_{\rm it} = x$ and $x+-x = 0_{\rm it}$.

In the sequel G denotes a group structure and x, y denote elements of G. We see that the Abelian group is a group.

Let us consider G, x, y. The functor $x -' y$ yielding an element of G is defined by:

(Def.2) $x -' y = x + -y$.

In the sequel G denotes a group and u, v, w denote elements of G. One can prove the following propositions:

(1) $(-v) + v = 0_G$.

(2) $0_G + v = v$.

(3) $v + w = 0_G$ if and only if $-v = w$.

(4) $-0_G = 0_G$.

(5) (i) $-(v + w) = (-w) -' v$,

(ii) $- - v = v$,

(iii) $-((-v) + w) = (-w) + v$,

(iv) $-(v -' w) = w -' v$,

[1]Supported by RPBP.III-24.C6

ISSN 0777–4028

(v) $-((-v) -' w) = w + v$,
(vi) $u -' (v + w) = u -' w -' v$.

(6) $0_G -' v = -v$ and $v -' 0_G = v$.

In the sequel G denotes an Abelian group and u, v, w denote elements of G. The following four propositions are true:

(7) (i) $-(v + w) = (-w) - v$,
(ii) $- - v = v$,
(iii) $-((-v) + w) = (-w) + v$,
(iv) $-(v - w) = w - v$,
(v) $-((-v) - w) = w + v$,
(vi) $u - (v + w) = u - w - v$.

(8) $0_G - v = -v$ and $v - 0_G = v$.

(9) $(-u) - v = (-v) - u$ and $(-u) + v = v - u$ and $u - v = (-v) + u$ and $u - v - w = u - w - v$.

(10) (i) $-(v + w) = (-v) - w$,
(ii) $-((-v) + w) = v - w$,
(iii) $-(v - w) = (-v) + w$,
(iv) $-((-v) - w) = v + w$,
(v) $u - (v + w) = u - v - w$.

For simplicity we adopt the following convention: R will denote an associative ring, a, b will denote scalars of R, V will denote a left module over R, and v, w will denote vectors of V. We now state several propositions:

(11) $-(a - b) = (-a) + b$.

(12) $a + 0_R = a$ and $0_R + a = a$.

(13) If $a = 0_R$ or $b = 0_R$, then $a \cdot b = 0_R$.

(14) $(-1_R) \cdot a = -a$ and $a \cdot -1_R = -a$.

(15) $a = 0_R$ if and only if $-a = 0_R$.

(16) $v + -v = \Theta_V$ and $(-v) + v = \Theta_V$.

(17) $-\Theta_V = \Theta_V$.

(18) $v + w = \Theta_V$ if and only if $-v = w$.

(19) $\Theta_V + v = v$ and $v + \Theta_V = v$ and $\Theta_V - v = -v$ and $v - \Theta_V = v$.

In the sequel x, y denote scalars of R. Next we state several propositions:

(20) $0_R \cdot v = \Theta_V$ and $(-1_R) \cdot v = -v$ and $x \cdot (\Theta_V) = \Theta_V$.

(21) $-x \cdot v = (-x) \cdot v$ and $w - x \cdot v = w + (-x) \cdot v$.

(22) $x \cdot -v = -x \cdot v$.

(23) $x \cdot (v - w) = x \cdot v - x \cdot w$.

(24) $v - x \cdot (y \cdot w) = v - x \cdot y \cdot w$.

In the sequel F will be a skew field, x will be a scalar of F, V will be a left module over F, and v will be a vector of V. The following two propositions are true:

(25) $x \cdot v = \Theta_V$ if and only if $x = 0_F$ or $v = \Theta_V$.

(26) If $x \neq 0_F$, then $x^{-1} \cdot (x \cdot v) = v$.

We adopt the following rules: V will denote a left module over R and v, v_1, v_2, u, w will denote vectors of V. The following propositions are true:

(27) $v - v = \Theta_V$.

(28) (i) $- - v = v$,
(ii) $-(v + w) = (-v) + -w$,
(iii) $-((-v) + w) = v + -w$,
(iv) $-(v + w) = (-v) - w$,
(v) $-(v - w) = (-v) + w$,
(vi) $-((-v) + w) = v - w$,
(vii) $-((-v) - w) = v + w$.

(29) $(u + v) - w = u + (v - w)$.

(30) $v = v_1 + v_2$ if and only if $v_1 = v - v_2$.

(31) $v - (u - w) = (v - u) + w$.

(32) If $v + u = v$ or $u + v = v$, then $u = \Theta_V$.

In the sequel R denotes an associative ring, V denotes a right module over R, and v, w denote vectors of V. We now state four propositions:

(33) $v + -v = \Theta_V$ and $(-v) + v = \Theta_V$.

(34) $-\Theta_V = \Theta_V$.

(35) $v + w = \Theta_V$ if and only if $-v = w$.

(36) $\Theta_V + v = v$ and $v + \Theta_V = v$ and $\Theta_V - v = -v$ and $v - \Theta_V = v$.

In the sequel x, y are scalars of R. We now state several propositions:

(37) $v \cdot 0_R = \Theta_V$ and $v \cdot -1_R = -v$ and $(\Theta_V) \cdot x = \Theta_V$.

(38) $-v \cdot x = v \cdot -x$ and $w - v \cdot x = w + v \cdot -x$.

(39) $(-v) \cdot x = -v \cdot x$.

(40) $(v - w) \cdot x = v \cdot x - w \cdot x$.

(41) $v - w \cdot y \cdot x = v - w \cdot (y \cdot x)$.

In the sequel F denotes a skew field, x denotes a scalar of F, V denotes a right module over F, and v denotes a vector of V. One can prove the following two propositions:

(42) $v \cdot x = \Theta_V$ if and only if $x = 0_F$ or $v = \Theta_V$.

(43) If $x \neq 0_F$, then $v \cdot x \cdot x^{-1} = v$.

We follow the rules: V will denote a right module over R and v, v_1, v_2, u, w will denote vectors of V. The following propositions are true:

(44) $v - v = \Theta_V$.

(45) (i) $- - v = v$,
(ii) $-(v + w) = (-v) + -w$,
(iii) $-((-v) + w) = v + -w$,
(iv) $-(v + w) = (-v) - w$,
(v) $-(v - w) = (-v) + w$,
(vi) $-((-v) + w) = v - w$,

(vii) $-((-v) - w) = v + w$.

(46) $(u + v) - w = u + (v - w)$.

(47) $v = v_1 + v_2$ if and only if $v_1 = v - v_2$.

(48) $v - (u - w) = (v - u) + w$.

(49) If $v + u = v$ or $u + v = v$, then $u = \Theta_V$.

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] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[6] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[7] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[8] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.
[9] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[10] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[11] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[12] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[13] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received October 22, 1990

FORMALIZED MATHEMATICS
Vol.2, No.2, March–April 1991
Université Catholique de Louvain

Finite Sums of Vectors in Left Module over Associative Ring [1]

Michał Muzalewski
Warsaw University
Białystok

Wojciech Skaba
University of Toruń

Summary. Definition of a finite sequence of the vectors of Left Module over Associative Ring and some theorems concerning these sums. Written as a generalization of the article [11].

MML Identifier: LMOD_1.

The terminology and notation used here have been introduced in the following papers: [10], [3], [2], [4], [6], [12], [9], [5], [1], [7], and [8]. For simplicity we adopt the following convention: x is arbitrary, R is an associative ring, a is a scalar of R, V is a left module over R, and v, v_1, v_2, w, u are vectors of V. Let us consider R, V, x. The predicate $x \in V$ is defined by:

(Def.1) $x \in$ the carrier of the carrier of V.

The following two propositions are true:

(1) $x \in V$ if and only if $x \in$ the carrier of the carrier of V.

(2) $v \in V$.

We adopt the following convention: F, G, H will denote finite sequences of elements of the carrier of the carrier of V, f will denote a function from $\mathbb{N}$ into the carrier of the carrier of V, and i, j, k, n will denote natural numbers. Let us consider R, V, F. The functor $\sum F$ yielding a vector of V is defined by:

(Def.2) there exists f such that $\sum F = f(\operatorname{len} F)$ and $f(0) = \Theta_V$ and for all j, v such that $j < \operatorname{len} F$ and $v = F(j+1)$ holds $f(j+1) = f(j) + v$.

One can prove the following propositions:

(3) If there exists f such that $u = f(\operatorname{len} F)$ and $f(0) = \Theta_V$ and for all j, v such that $j < \operatorname{len} F$ and $v = F(j+1)$ holds $f(j+1) = f(j) + v$, then $u = \sum F$.

[1]Supported by RPBP.III-24.C6

ISSN 0777–4028

(4) There exists f such that $\sum F = f(\operatorname{len} F)$ and $f(0) = \Theta_V$ and for all j, v such that $j < \operatorname{len} F$ and $v = F(j+1)$ holds $f(j+1) = f(j) + v$.

(5) If $k \in \operatorname{Seg} n$ and $\operatorname{len} F = n$, then $F(k)$ is a vector of V.

(6) If $\operatorname{len} F = \operatorname{len} G + 1$ and $G = F \restriction \operatorname{Seg} \operatorname{len} G$ and $v = F(\operatorname{len} F)$, then $\sum F = \sum G + v$.

(7) $\sum(F \frown G) = \sum F + \sum G$.

(8) If $\operatorname{len} F = \operatorname{len} G$ and $\operatorname{len} F = \operatorname{len} H$ and for every k such that $k \in \operatorname{Seg} \operatorname{len} F$ holds $H(k) = \pi_k F + \pi_k G$, then $\sum H = \sum F + \sum G$.

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

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

(11) If $\operatorname{len} F = \operatorname{len} G$ and for all k, v such that $k \in \operatorname{Seg} \operatorname{len} F$ and $v = G(k)$ holds $F(k) = -v$, then $\sum F = -\sum G$.

(12) If $\operatorname{len} F = \operatorname{len} G$ and for every k such that $k \in \operatorname{Seg} \operatorname{len} F$ holds $G(k) = -\pi_k F$, then $\sum G = -\sum F$.

(13) If $\operatorname{len} F = \operatorname{len} G$ and $\operatorname{len} F = \operatorname{len} H$ and for every k such that $k \in \operatorname{Seg} \operatorname{len} F$ holds $H(k) = \pi_k F - \pi_k G$, then $\sum H = \sum F - \sum G$.

(14) If $\operatorname{rng} F = \operatorname{rng} G$ and F is one-to-one and G is one-to-one, then $\sum F = \sum G$.

(15) For all F, G and for every permutation f of $\operatorname{dom} F$ such that $\operatorname{len} F = \operatorname{len} G$ and for every i such that $i \in \operatorname{dom} G$ holds $G(i) = F(f(i))$ holds $\sum F = \sum G$.

(16) For every permutation f of $\operatorname{dom} F$ such that $G = F \cdot f$ holds $\sum F = \sum G$.

(17) $\sum \varepsilon_{\text{the carrier of the carrier of } V} = \Theta_V$.

(18) $\sum\langle v \rangle = v$.

(19) $\sum\langle v, u \rangle = v + u$.

(20) $\sum\langle v, u, w \rangle = v + u + w$.

(21) $a \cdot \sum \varepsilon_{\text{the carrier of the carrier of } V} = \Theta_V$.

(22) $a \cdot \sum\langle v \rangle = a \cdot v$.

(23) $a \cdot \sum\langle v, u \rangle = a \cdot v + a \cdot u$.

(24) $a \cdot \sum\langle v, u, w \rangle = a \cdot v + a \cdot u + a \cdot w$.

(25) $-\sum \varepsilon_{\text{the carrier of the carrier of } V} = \Theta_V$.

(26) $-\sum\langle v \rangle = -v$.

(27) $-\sum\langle v, u \rangle = (-v) - u$.

(28) $-\sum\langle v, u, w \rangle = (-v) - u - w$.

(29) $\sum\langle v, w \rangle = \sum\langle w, v \rangle$.

(30) $\sum\langle v, w \rangle = \sum\langle v \rangle + \sum\langle w \rangle$.

(31) $\sum\langle \Theta_V, \Theta_V \rangle = \Theta_V$.

(32) $\sum\langle \Theta_V, v \rangle = v$ and $\sum\langle v, \Theta_V \rangle = v$.

(33) $\sum\langle v,-v\rangle = \Theta_V$ and $\sum\langle -v,v\rangle = \Theta_V$.

We now state a number of propositions:

(34) $\sum\langle v,-w\rangle = v-w$ and $\sum\langle -w,v\rangle = v-w$.

(35) $\sum\langle -v,-w\rangle = -(v+w)$ and $\sum\langle -w,-v\rangle = -(v+w)$.

(36) $\sum\langle u,v,w\rangle = \sum\langle u\rangle + \sum\langle v\rangle + \sum\langle w\rangle$.

(37) $\sum\langle u,v,w\rangle = \sum\langle u,v\rangle + w$.

(38) $\sum\langle u,v,w\rangle = \sum\langle v,w\rangle + u$.

(39) $\sum\langle u,v,w\rangle = \sum\langle u,w\rangle + v$.

(40) $\sum\langle u,v,w\rangle = \sum\langle u,w,v\rangle$.

(41) $\sum\langle u,v,w\rangle = \sum\langle v,u,w\rangle$.

(42) $\sum\langle u,v,w\rangle = \sum\langle v,w,u\rangle$.

(43) $\sum\langle u,v,w\rangle = \sum\langle w,u,v\rangle$.

(44) $\sum\langle u,v,w\rangle = \sum\langle w,v,u\rangle$.

(45) $\sum\langle \Theta_V,\Theta_V,\Theta_V\rangle = \Theta_V$.

(46) $\sum\langle \Theta_V,\Theta_V,v\rangle = v$ and $\sum\langle \Theta_V,v,\Theta_V\rangle = v$ and $\sum\langle v,\Theta_V,\Theta_V\rangle = v$.

(47) $\sum\langle \Theta_V,u,v\rangle = u+v$ and $\sum\langle u,v,\Theta_V\rangle = u+v$ and $\sum\langle u,\Theta_V,v\rangle = u+v$.

(48) If $\operatorname{len} F = 0$, then $\sum F = \Theta_V$.

(49) If $\operatorname{len} F = 1$, then $\sum F = F(1)$.

(50) If $\operatorname{len} F = 2$ and $v_1 = F(1)$ and $v_2 = F(2)$, then $\sum F = v_1 + v_2$.

(51) If $\operatorname{len} F = 3$ and $v_1 = F(1)$ and $v_2 = F(2)$ and $v = F(3)$, then $\sum F = v_1 + v_2 + v$.

References

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

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 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] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

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

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

[8] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.

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

[10] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[11] Wojciech A. Trybulec. Finite sums of vectors in vector space. *Formalized Mathematics*, 1(**5**):851–854, 1990.

[12] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

Received October 22, 1990

FORMALIZED MATHEMATICS
Vol.2, No.2, March–April 1991
Université Catholique de Louvain

Submodules and Cosets of Submodules in Left Module over Associative Ring [1]

Michał Muzalewski
Warsaw University
Białystok

Wojciech Skaba
University of Toruń

Summary. Notions of Submodules in Left Module over Associative Ring and Cosets of Submodules in Left Module over Associative Ring. A few basic theorems related to these notions are proved. This article originated as a generalization of the article [12].

MML Identifier: `LMOD_2`.

The notation and terminology used here are introduced in the following articles: [8], [2], [14], [13], [10], [11], [7], [1], [3], [9], [4], [6], and [5]. For simplicity we follow a convention: x will be arbitrary, R will be an associative ring, a will be a scalar of R, V, X, Y will be left modules over R, and u, v, v_1, v_2 will be vectors of V. Let us consider R, V. A subset of V is a subset of the carrier of the carrier of V.

In the sequel V_1, V_2, V_3 will denote subsets of V. Let us consider R, V, V_1. We say that V_1 is linearly closed if and only if:

(Def.1) for all v, u such that $v \in V_1$ and $u \in V_1$ holds $v + u \in V_1$ and for all a, v such that $v \in V_1$ holds $a \cdot v \in V_1$.

We now state a number of propositions:

(1) If for all v, u such that $v \in V_1$ and $u \in V_1$ holds $v + u \in V_1$ and for all a, v such that $v \in V_1$ holds $a \cdot v \in V_1$, then V_1 is linearly closed.

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

(3) If V_1 is linearly closed, then for all a, v such that $v \in V_1$ holds $a \cdot v \in V_1$.

(4) If $V_1 \neq \emptyset$ and V_1 is linearly closed, then $\Theta_V \in V_1$.

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

[1]Supported by RPBP.III-24.C6

ISSN 0777–4028

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

(7) $\{\Theta_V\}$ is linearly closed.

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

(9) 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.

(10) If V_1 is linearly closed and V_2 is linearly closed, then $V_1 \cap V_2$ is linearly closed.

Let us consider R, V. A left module over R is called a submodule of V if:

(Def.2) the carrier of the carrier of it $\subseteq$ the carrier of the carrier of V and the zero of the carrier of it = the zero of the carrier of V and the addition of the carrier of it = (the addition of the carrier of V) $\restriction$ [: the carrier of the carrier of it, the carrier of the carrier of it :] and the left multiplication of it = (the left multiplication of V) $\restriction$ [: the carrier of R, the carrier of the carrier of it :].

We now state the proposition

(11) If the carrier of the carrier of $X \subseteq$ the carrier of the carrier of V and the zero of the carrier of $X =$ the zero of the carrier of V and the addition of the carrier of $X =$ (the addition of the carrier of V) $\restriction$ [: the carrier of the carrier of X, the carrier of the carrier of X :] and the left multiplication of $X =$ (the left multiplication of V) $\restriction$ [: the carrier of R, the carrier of the carrier of X :], then X is a submodule of V.

We follow a convention: W, W_1, W_2 denote submodules of V and w, w_1, w_2 denote vectors of W. The following propositions are true:

(12) The carrier of the carrier of $W \subseteq$ the carrier of the carrier of V.

(13) The zero of the carrier of $W =$ the zero of the carrier of V.

(14) The addition of the carrier of $W =$ (the addition of the carrier of V) $\restriction$ [: the carrier of the carrier of W, the carrier of the carrier of W :].

(15) The left multiplication of $W =$ (the left multiplication of V) $\restriction$ [: the carrier of R, the carrier of the carrier of W :].

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

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

(18) w is a vector of V.

(19) $\Theta_W = \Theta_V$.

(20) $\Theta_{W_1} = \Theta_{W_2}$.

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

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

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

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

(25) $\Theta_V \in W$.

(26) $\Theta_{W_1} \in W_2$.

(27) $\Theta_W \in V$.

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

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

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

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

(32) V is a submodule of V.

(33) If V is a submodule of X and X is a submodule of V, then $V = X$.

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

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

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

(37) If the carrier of the carrier of $W_1 =$ the carrier of the carrier of W_2, then $W_1 = W_2$.

(38) If for every v holds $v \in W_1$ if and only if $v \in W_2$, then $W_1 = W_2$.

(39) If the carrier of the carrier of $W =$ the carrier of the carrier of V, then $W = V$.

(40) If for every v holds $v \in W$, then $W = V$.

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

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

Let us consider R, V. The functor $\mathbf{0}_V$ yields a submodule of V and is defined as follows:

(Def.3) the carrier of the carrier of $\mathbf{0}_V = \{\Theta_V\}$.

Let us consider R, V. The functor Ω_V yielding a submodule of V is defined by:

(Def.4) $\Omega_V = V$.

The following propositions are true:

(43) The carrier of the carrier of $\mathbf{0}_V = \{\Theta_V\}$.

(44) If the carrier of the carrier of $W = \{\Theta_V\}$, then $W = \mathbf{0}_V$.

(45) $\Omega_V = V$.

(46) $x \in \mathbf{0}_V$ if and only if $x = \Theta_V$.

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

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

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

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

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

(52) W is a submodule of Ω_V.

(53) V is a submodule of Ω_V.

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

(Def.5) $v + W = \{v + u : u \in W\}$.

Let us consider R, V, W. A subset of V is said to be a coset of W if:

(Def.6) there exists v such that it $= v + W$.

In the sequel B, C are cosets of W. One can prove the following propositions:

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

(55) There exists v such that $C = v + W$.

(56) If $V_1 = v + W$, then V_1 is a coset of W.

(57) $x \in v + W$ if and only if there exists u such that $u \in W$ and $x = v + u$.

(58) $\Theta_V \in v + W$ if and only if $v \in W$.

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

(60) $\Theta_V + W =$ the carrier of the carrier of W.

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

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

(63) $\Theta_V \in v + W$ if and only if $v + W =$ the carrier of the carrier of W.

(64) $v \in W$ if and only if $v + W =$ the carrier of the carrier of W.

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

(66) $u \in W$ if and only if $v + W = v + u + W$.

(67) $u \in W$ if and only if $v + W = (v - u) + W$.

(68) $v \in u + W$ if and only if $u + W = v + W$.

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

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

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

(72) $u + v \in v + W$ if and only if $u \in W$.

(73) $v - u \in v + W$ if and only if $u \in W$.

(74) $u \in v + W$ if and only if there exists v_1 such that $v_1 \in W$ and $u = v + v_1$.

(75) $u \in v + W$ if and only if there exists v_1 such that $v_1 \in W$ and $u = v - v_1$.

(76) There exists v such that $v_1 \in v + W$ and $v_2 \in v + W$ if and only if $v_1 - v_2 \in W$.

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

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

(79) $v + W_1 = v + W_2$ if and only if $W_1 = W_2$.

(80) If $v + W_1 = u + W_2$, then $W_1 = W_2$.

In the sequel C_1 denotes a coset of W_1 and C_2 denotes a coset of W_2. Next we state a number of propositions:

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

(82) C is linearly closed if and only if $C =$ the carrier of the carrier of W.

(83) If $C_1 = C_2$, then $W_1 = W_2$.

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

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

(86) The carrier of the carrier of W is a coset of W.

(87) The carrier of the carrier of V is a coset of Ω_V.

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

(89) $\Theta_V \in C$ if and only if $C =$ the carrier of the carrier of W.

(90) $u \in C$ if and only if $C = u + W$.

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

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

(93) There exists C such that $v_1 \in C$ and $v_2 \in C$ if and only if $v_1 - v_2 \in W$.

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

References

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

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

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

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

[5] Michał Muzalewski and Wojciech Skaba. Finite sums of vectors in left module over associative ring. *Formalized Mathematics*, 2(**2**):279–282, 1991.

[6] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.

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

[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[9] Wojciech A. Trybulec. Finite sums of vectors in vector space. *Formalized Mathematics*, 1(**5**):851–854, 1990.

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

[11] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.

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

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

[14] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

Received October 22, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Operations on Submodules in Left Module over Associative Ring [1]

Michał Muzalewski
Warsaw University
Białystok

Wojciech Skaba
University of Toruń

Summary. Definition of sum, direct sum and intersection of submodules. We prove a number of theorems related to these notions. This article originated as a generalization of the article [10].

MML Identifier: `LMOD_3`.

The terminology and notation used here are introduced in the following papers: [1], [12], [14], [9], [8], [13], [2], [11], [7], [3], [4], [5], and [6]. For simplicity we adopt the following rules: R denotes an associative ring, V denotes a left module over R, W, W_1, W_2, W_3 denote submodules of V, u, u_1, u_2, v, v_1, v_2 denote vectors of V, and x is arbitrary. Let us consider R, V, W_1, W_2. The functor $W_1 + W_2$ yields a submodule of V and is defined by:

(Def.1) the carrier of the carrier of $W_1 + W_2 = \{v + u : v \in W_1 \wedge u \in W_2\}$.

Let us consider R, V, W_1, W_2. The functor $W_1 \cap W_2$ yielding a submodule of V is defined by:

(Def.2) the carrier of the carrier of $W_1 \cap W_2 =$ (the carrier of the carrier of W_1)$\cap$ (the carrier of the carrier of W_2).

One can prove the following propositions:

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

(2) If the carrier of the carrier of $W = \{v + u : v \in W_1 \wedge u \in W_2\}$, then $W = W_1 + W_2$.

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

(4) If the carrier of the carrier of $W =$ (the carrier of the carrier of W_1)$\cap$ (the carrier of the carrier of W_2), then $W = W_1 \cap W_2$.

[1] Supported by RPBP.III-24.C6

ISSN 0777–4028

(5) $x \in W_1 + W_2$ if and only if there exist v_1, v_2 such that $v_1 \in W_1$ and $v_2 \in W_2$ and $x = v_1 + v_2$.

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

(7) $x \in W_1 \cap W_2$ if and only if $x \in W_1$ and $x \in W_2$.

(8) $W + W = W$.

(9) $W_1 + W_2 = W_2 + W_1$.

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

(11) W_1 is a submodule of $W_1 + W_2$ and W_2 is a submodule of $W_1 + W_2$.

(12) W_1 is a submodule of W_2 if and only if $W_1 + W_2 = W_2$.

(13) $\mathbf{0}_V + W = W$ and $W + \mathbf{0}_V = W$.

(14) $\mathbf{0}_V + \Omega_V = V$ and $\Omega_V + \mathbf{0}_V = V$.

(15) $\Omega_V + W = V$ and $W + \Omega_V = V$.

(16) $\Omega_V + \Omega_V = V$.

(17) $W \cap W = W$.

(18) $W_1 \cap W_2 = W_2 \cap W_1$.

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

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

(21) W_1 is a submodule of W_2 if and only if $W_1 \cap W_2 = W_1$.

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

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

(24) If W_1 is a submodule of W_2 and W_1 is a submodule of W_3, then W_1 is a submodule of $W_2 \cap W_3$.

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

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

(27) $\Omega_V \cap W = W$ and $W \cap \Omega_V = W$.

(28) $\Omega_V \cap \Omega_V = V$.

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

(30) $W_1 \cap W_2 + W_2 = W_2$.

(31) $W_1 \cap (W_1 + W_2) = W_1$.

One can prove the following propositions:

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

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

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

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

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

(37) $W_1 + W_2 = W_2$ if and only if $W_1 \cap W_2 = W_1$.

(38) If W_1 is a submodule of W_2, then $W_1 + W_3$ is a submodule of $W_2 + W_3$.

(39) If W_1 is a submodule of W_2, then W_1 is a submodule of $W_2 + W_3$.

(40) If W_1 is a submodule of W_3 and W_2 is a submodule of W_3, then W_1+W_2 is a submodule of W_3.

(41) There exists W such that the carrier of the carrier of $W =$ (the carrier of the carrier of W_1)$\cup$ (the carrier of 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 R, V. The functor $\mathrm{Sub}(V)$ yields a non-empty set and is defined by:

(Def.3) for every x holds $x \in \mathrm{Sub}(V)$ if and only if x is a submodule of V.

In the sequel D denotes a non-empty set. One can prove the following three propositions:

(42) If for every x holds $x \in D$ if and only if x is a submodule of V, then $D = \mathrm{Sub}(V)$.

(43) $x \in \mathrm{Sub}(V)$ if and only if x is a submodule of V.

(44) $V \in \mathrm{Sub}(V)$.

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

(Def.4) $V = W_1 + W_2$ and $W_1 \cap W_2 = \mathbf{0}_V$.

One can prove the following two propositions:

(46)[2] If V is the direct sum of W_1 and W_2, then V is the direct sum of W_2 and W_1.

(47) V is the direct sum of $\mathbf{0}_V$ and Ω_V and V is the direct sum of Ω_V and $\mathbf{0}_V$.

In the sequel C_1 will denote a coset of W_1 and C_2 will denote a coset of W_2. Next we state several propositions:

(48) If $C_1 \cap C_2 \neq \emptyset$, then $C_1 \cap C_2$ is a coset of $W_1 \cap W_2$.

(49) V is the direct sum of W_1 and W_2 if and only if for every C_1, C_2 there exists v such that $C_1 \cap C_2 = \{v\}$.

(50) $W_1 + W_2 = V$ if and only if for every v there exist v_1, v_2 such that $v_1 \in W_1$ and $v_2 \in W_2$ and $v = v_1 + v_2$.

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

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

In the sequel t will be an element of $[\!:$ the carrier of the carrier of V, the carrier of the carrier of $V :\!]$. Let us consider R, V, v, W_1, W_2. Let us assume that V is the direct sum of W_1 and W_2. The functor $v \lhd (W_1, W_2)$ yielding an

[2]The proposition (45) was either repeated or obvious.

element of $[\!:$ the carrier of the carrier of V, the carrier of the carrier of $V\,:\!]$ is defined as follows:

(Def.5) $v = (v \lhd (W_1, W_2))_{\mathbf{1}} + (v \lhd (W_1, W_2))_{\mathbf{2}}$ and $(v \lhd (W_1, W_2))_{\mathbf{1}} \in W_1$ and $(v \lhd (W_1, W_2))_{\mathbf{2}} \in W_2$.

The following propositions are true:

(53) If V is the direct sum of W_1 and W_2 and $t_{\mathbf{1}} + t_{\mathbf{2}} = v$ and $t_{\mathbf{1}} \in W_1$ and $t_{\mathbf{2}} \in W_2$, then $t = v \lhd (W_1, W_2)$.

(54) If V is the direct sum of W_1 and W_2, then $(v \lhd (W_1, W_2))_{\mathbf{1}} + (v \lhd (W_1, W_2))_{\mathbf{2}} = v$.

(55) If V is the direct sum of W_1 and W_2, then $(v \lhd (W_1, W_2))_{\mathbf{1}} \in W_1$.

(56) If V is the direct sum of W_1 and W_2, then $(v \lhd (W_1, W_2))_{\mathbf{2}} \in W_2$.

(57) If V is the direct sum of W_1 and W_2, then $(v \lhd (W_1, W_2))_{\mathbf{1}} = (v \lhd (W_2, W_1))_{\mathbf{2}}$.

(58) If V is the direct sum of W_1 and W_2, then $(v \lhd (W_1, W_2))_{\mathbf{2}} = (v \lhd (W_2, W_1))_{\mathbf{1}}$.

In the sequel A_1, A_2 will denote elements of $\mathrm{Sub}(V)$. Let us consider R, V. The functor $\mathrm{SubJoin}\,V$ yields a binary operation on $\mathrm{Sub}(V)$ and is defined as follows:

(Def.6) 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 R, V. The functor $\mathrm{SubMeet}\,V$ yielding a binary operation on $\mathrm{Sub}(V)$ is defined as follows:

(Def.7) for all A_1, A_2, W_1, W_2 such that $A_1 = W_1$ and $A_2 = W_2$ holds $(\mathrm{SubMeet}\,V)(A_1,\, A_2) = W_1 \cap W_2$.

In the sequel o is a binary operation on $\mathrm{Sub}(V)$. Next we state several propositions:

(59) If $A_1 = W_1$ and $A_2 = W_2$, then $\mathrm{SubJoin}\,V(A_1,\, A_2) = W_1 + W_2$.

(60) If for all A_1, A_2, W_1, W_2 such that $A_1 = W_1$ and $A_2 = W_2$ holds $o(A_1,\, A_2) = W_1 + W_2$, then $o = \mathrm{SubJoin}\,V$.

(61) If $A_1 = W_1$ and $A_2 = W_2$, then $\mathrm{SubMeet}\,V(A_1,\, A_2) = W_1 \cap W_2$.

(62) If for all A_1, A_2, W_1, W_2 such that $A_1 = W_1$ and $A_2 = W_2$ holds $o(A_1,\, A_2) = W_1 \cap W_2$, then $o = \mathrm{SubMeet}\,V$.

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

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

(65) $\langle \mathrm{Sub}(V), \mathrm{SubJoin}\,V, \mathrm{SubMeet}\,V \rangle$ is an upper bound lattice.

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

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

References

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

[2] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[3] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[4] Michał Muzalewski and Wojciech Skaba. Finite sums of vectors in left module over associative ring. *Formalized Mathematics*, 2(**2**):279–282, 1991.
[5] Michał Muzalewski and Wojciech Skaba. Submodules and cosets of submodules in left module over associative ring. *Formalized Mathematics*, 2(**2**):283–287, 1991.
[6] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.
[7] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[9] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[10] Wojciech A. Trybulec. Operations on subspaces in vector space. *Formalized Mathematics*, 1(**5**):871–876, 1990.
[11] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[12] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[13] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[14] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

Received October 22, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Linear Combinations in Left Module over Associative Ring [1]

Michał Muzalewski
Warsaw University
Białystok

Wojciech Skaba
University of Toruń

Summary. Notion of linear combination of vectors in Left Module over Associative Ring, defined as a function from the carrier of Left Module over Associative Ring to the carrier of this Ring. The following operations are included: addition, subtraction of combinations and multiplication of a combination by a scalar of the Ring. Following it, the sum of a finite set of vectors and the sum of linear combinations is defined. Many theorems are proved. This article originated as a generalization of the article [19].

MML Identifier: `LMOD_4`.

The articles [22], [7], [5], [3], [6], [8], [21], [17], [15], [16], [2], [4], [18], [20], [1], [9], [10], [11], [13], [12], and [14] provide the terminology and notation for this paper. For simplicity we follow a convention: R will be an associative ring, V will be a left module over R, a, b will be scalars of R, x will be arbitrary, i will be a natural number, u, v, v_1, v_2, v_3 will be vectors of V, F, G will be finite sequences of elements of the carrier of the carrier of V, A, B will be subsets of V, and f will be a function from the carrier of the carrier of V into the carrier of R. Let D be a non-empty set. Then $\emptyset_D$ is a subset of D.

Let us consider R, V. A subset of V is said to be a finite subset of V if:

(Def.1) it is finite.

In the sequel S, T denote finite subsets of V. Let us consider R, V, S, T. Then $S \cup T$ is a finite subset of V. Then $S \cap T$ is a finite subset of V. Then $S \setminus T$ is a finite subset of V. Then $S \dot{-} T$ is a finite subset of V.

Let us consider R, V. The functor 0_V yields a finite subset of V and is defined as follows:

(Def.2) $0_V = \emptyset$.

[1]Supported by RPBP.III-24.C6

ISSN 0777–4028

One can prove the following proposition

(2)[2] $0_V = \emptyset$.

Let us consider R, V, T. The functor $\sum T$ yields a vector of V and is defined as follows:

(Def.3) there exists F such that $\operatorname{rng} F = T$ and F is one-to-one and $\sum T = \sum F$.

One can prove the following two propositions:

(3) There exists F such that $\operatorname{rng} F = T$ and F is one-to-one and $\sum T = \sum F$.

(4) If $\operatorname{rng} F = T$ and F is one-to-one and $v = \sum F$, then $v = \sum T$.

Let us consider R, V, v. Then $\{v\}$ is a finite subset of V.

Let us consider R, V, v_1, v_2. Then $\{v_1, v_2\}$ is a finite subset of V.

Let us consider R, V, v_1, v_2, v_3. Then $\{v_1, v_2, v_3\}$ is a finite subset of V.

We now state a number of propositions:

(5) $\sum(0_V) = \Theta_V$.

(6) $\sum\{v\} = v$.

(7) If $v_1 \neq v_2$, then $\sum\{v_1, v_2\} = v_1 + v_2$.

(8) If $v_1 \neq v_2$ and $v_2 \neq v_3$ and $v_1 \neq v_3$, then $\sum\{v_1, v_2, v_3\} = v_1 + v_2 + v_3$.

(9) If T misses S, then $\sum(T \cup S) = \sum T + \sum S$.

(10) $\sum(T \cup S) = (\sum T + \sum S) - \sum(T \cap S)$.

(11) $\sum(T \cap S) = (\sum T + \sum S) - \sum(T \cup S)$.

(12) $\sum(T \setminus S) = \sum(T \cup S) - \sum S$.

(13) $\sum(T \setminus S) = \sum T - \sum(T \cap S)$.

(14) $\sum(T \dot{-} S) = \sum(T \cup S) - \sum(T \cap S)$.

(15) $\sum(T \dot{-} S) = \sum(T \setminus S) + \sum(S \setminus T)$.

Let us consider R, V. An element of $(\text{the carrier of } R)^{\text{the carrier of the carrier of } V}$ is called a linear combination of V if:

(Def.4) there exists T such that for every v such that $v \notin T$ holds $\text{it}(v) = 0_R$.

In the sequel K, L, L_1, L_2, L_3 are linear combinations of V. We now state the proposition

(16) There exists T such that for every v such that $v \notin T$ holds $L(v) = 0_R$.

In the sequel E is an element of $(\text{the carrier of } R)^{\text{the carrier of the carrier of } V}$. Next we state the proposition

(17) If there exists T such that for every v such that $v \notin T$ holds $E(v) = 0_R$, then E is a linear combination of V.

Let us consider R, V, L. The functor $\operatorname{support} L$ yields a finite subset of V and is defined as follows:

(Def.5) $\operatorname{support} L = \{v : L(v) \neq 0_R\}$.

The following propositions are true:

[2]The proposition (1) was either repeated or obvious.

(18) support $L = \{v : L(v) \neq 0_R\}$.

(19) $x \in$ support L if and only if there exists v such that $x = v$ and $L(v) \neq 0_R$.

(20) $L(v) = 0_R$ if and only if $v \notin$ support L.

Let us consider R, V. The functor $\mathbf{0}_{\mathrm{LC}_V}$ yielding a linear combination of V is defined by:

(Def.6) support $\mathbf{0}_{\mathrm{LC}_V} = \emptyset$.

We now state two propositions:

(21) $L = \mathbf{0}_{\mathrm{LC}_V}$ if and only if support $L = \emptyset$.

(22) $\mathbf{0}_{\mathrm{LC}_V}(v) = 0_R$.

Let us consider R, V, A. A linear combination of V is called a linear combination of A if:

(Def.7) support it $\subseteq A$.

We now state the proposition

(23) If support $L \subseteq A$, then L is a linear combination of A.

In the sequel l will denote a linear combination of A. We now state several propositions:

(24) support $l \subseteq A$.

(25) If $A \subseteq B$, then l is a linear combination of B.

(26) $\mathbf{0}_{\mathrm{LC}_V}$ is a linear combination of A.

(27) For every linear combination l of $\emptyset_{\text{the carrier of the carrier of } V}$ holds $l = \mathbf{0}_{\mathrm{LC}_V}$.

(28) L is a linear combination of support L.

Let us consider R, V, F, f. The functor fF yields a finite sequence of elements of the carrier of the carrier of V and is defined by:

(Def.8) $\mathrm{len}(fF) = \mathrm{len}\, F$ and for every i such that $i \in \mathrm{dom}(fF)$ holds $(fF)(i) = f(\pi_i F) \cdot \pi_i F$.

We now state several propositions:

(29) $\mathrm{len}(fF) = \mathrm{len}\, F$.

(30) For every i such that $i \in \mathrm{dom}(fF)$ holds $(fF)(i) = f(\pi_i F) \cdot \pi_i F$.

(31) If $\mathrm{len}\, G = \mathrm{len}\, F$ and for every i such that $i \in \mathrm{dom}\, G$ holds $G(i) = f(\pi_i F) \cdot \pi_i F$, then $G = fF$.

(32) If $i \in \mathrm{dom}\, F$ and $v = F(i)$, then $(fF)(i) = f(v) \cdot v$.

(33) $f\varepsilon_{\text{the carrier of the carrier of } V} = \varepsilon_{\text{the carrier of the carrier of } V}$.

(34) $f\langle v\rangle = \langle f(v) \cdot v\rangle$.

(35) $f\langle v_1, v_2\rangle = \langle f(v_1) \cdot v_1, f(v_2) \cdot v_2\rangle$.

(36) $f\langle v_1, v_2, v_3\rangle = \langle f(v_1) \cdot v_1, f(v_2) \cdot v_2, f(v_3) \cdot v_3\rangle$.

(37) $f(F \frown G) = (fF) \frown (fG)$.

Let us consider R, V, L. The functor $\sum L$ yields a vector of V and is defined as follows:

(Def.9) there exists F such that F is one-to-one and $\operatorname{rng} F = \operatorname{support} L$ and $\sum L = \sum(LF)$.

The following propositions are true:

(38) There exists F such that F is one-to-one and $\operatorname{rng} F = \operatorname{support} L$ and $\sum L = \sum(LF)$.

(39) If F is one-to-one and $\operatorname{rng} F = \operatorname{support} L$ and $u = \sum(LF)$, then $u = \sum L$.

(40) If $0_R \neq 1_R$, then $A \neq \emptyset$ and A is linearly closed if and only if for every l holds $\sum l \in A$.

(41) $\sum \mathbf{0}_{\mathrm{LC}_V} = \Theta_V$.

(42) For every linear combination l of $\emptyset_{\text{the carrier of the carrier of } V}$ holds $\sum l = \Theta_V$.

(43) For every linear combination l of $\{v\}$ holds $\sum l = l(v) \cdot v$.

(44) If $v_1 \neq v_2$, then for every linear combination l of $\{v_1, v_2\}$ holds $\sum l = l(v_1) \cdot v_1 + l(v_2) \cdot v_2$.

(45) If $\operatorname{support} L = \emptyset$, then $\sum L = \Theta_V$.

(46) If $\operatorname{support} L = \{v\}$, then $\sum L = L(v) \cdot v$.

(47) If $\operatorname{support} L = \{v_1, v_2\}$ and $v_1 \neq v_2$, then $\sum L = L(v_1) \cdot v_1 + L(v_2) \cdot v_2$.

Let us consider R, V, L_1, L_2. Let us note that one can characterize the predicate $L_1 = L_2$ by the following (equivalent) condition:

(Def.10) for every v holds $L_1(v) = L_2(v)$.

Next we state the proposition

(48) If for every v holds $L_1(v) = L_2(v)$, then $L_1 = L_2$.

Let us consider R, V, L_1, L_2. The functor $L_1 + L_2$ yielding a linear combination of V is defined by:

(Def.11) for every v holds $(L_1 + L_2)(v) = L_1(v) + L_2(v)$.

The following propositions are true:

(49) If for every v holds $L(v) = L_1(v) + L_2(v)$, then $L = L_1 + L_2$.

(50) $(L_1 + L_2)(v) = L_1(v) + L_2(v)$.

(51) $\operatorname{support}(L_1 + L_2) \subseteq \operatorname{support} L_1 \cup \operatorname{support} L_2$.

(52) If L_1 is a linear combination of A and L_2 is a linear combination of A, then $L_1 + L_2$ is a linear combination of A.

(53) For every commutative ring R and for every left module V over R and for all linear combinations L_1, L_2 of V holds $L_1 + L_2 = L_2 + L_1$.

(54) $L_1 + (L_2 + L_3) = L_1 + L_2 + L_3$.

(55) For every commutative ring R and for every left module V over R and for every linear combination L of V holds $L + \mathbf{0}_{\mathrm{LC}_V} = L$ and $\mathbf{0}_{\mathrm{LC}_V} + L = L$.

Let us consider R, V, a, L. The functor $a \cdot L$ yielding a linear combination of V is defined as follows:

(Def.12) for every v holds $(a \cdot L)(v) = a \cdot L(v)$.

One can prove the following propositions:

(56) If for every v holds $K(v) = a \cdot L(v)$, then $K = a \cdot L$.

(57) $(a \cdot L)(v) = a \cdot L(v)$.

(58) $\mathrm{support}(a \cdot L) \subseteq \mathrm{support}\, L$.

In the sequel R_1 denotes an integral domain, V_1 denotes a left module over R_1, L_4 denotes a linear combination of V_1, and a_1 denotes a scalar of R_1. Next we state several propositions:

(59) If $a_1 \neq 0_{R_1}$, then $\mathrm{support}(a_1 \cdot L_4) = \mathrm{support}\, L_4$.

(60) $0_R \cdot L = \mathbf{0}_{\mathrm{LC}_V}$.

(61) If L is a linear combination of A, then $a \cdot L$ is a linear combination of A.

(62) $(a + b) \cdot L = a \cdot L + b \cdot L$.

(63) $a \cdot (L_1 + L_2) = a \cdot L_1 + a \cdot L_2$.

(64) $a \cdot (b \cdot L) = a \cdot b \cdot L$.

(65) $(1_R) \cdot L = L$.

Let us consider R, V, L. The functor $-L$ yields a linear combination of V and is defined as follows:

(Def.13) $-L = (-1_R) \cdot L$.

One can prove the following propositions:

(66) $-L = (-1_R) \cdot L$.

(67) $(-L)(v) = -L(v)$.

(68) If $L_1 + L_2 = \mathbf{0}_{\mathrm{LC}_V}$, then $L_2 = -L_1$.

(69) $\mathrm{support} -L = \mathrm{support}\, L$.

(70) If L is a linear combination of A, then $-L$ is a linear combination of A.

(71) $- - L = L$.

Let us consider R, V, L_1, L_2. The functor $L_1 - L_2$ yields a linear combination of V and is defined by:

(Def.14) $L_1 - L_2 = L_1 + -L_2$.

One can prove the following propositions:

(72) $L_1 - L_2 = L_1 + -L_2$.

(73) $(L_1 - L_2)(v) = L_1(v) - L_2(v)$.

(74) $\mathrm{support}(L_1 - L_2) \subseteq \mathrm{support}\, L_1 \cup \mathrm{support}\, L_2$.

(75) If L_1 is a linear combination of A and L_2 is a linear combination of A, then $L_1 - L_2$ is a linear combination of A.

(76) $L - L = \mathbf{0}_{\mathrm{LC}_V}$.

(77) $\sum(L_1 + L_2) = \sum L_1 + \sum L_2$.

For simplicity we adopt the following convention: R will be an integral domain, V will be a left module over R, L, L_1, L_2 will be linear combinations of V, and a will be a scalar of R. We now state three propositions:

(78) $\sum(a \cdot L) = a \cdot \sum L$.

(79) $\sum -L = -\sum L$.

(80) $\sum(L_1 - L_2) = \sum L_1 - \sum L_2$.

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 and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[8] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[9] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[10] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[11] Michał Muzalewski and Wojciech Skaba. Finite sums of vectors in left module over associative ring. *Formalized Mathematics*, 2(**2**):279–282, 1991.
[12] Michał Muzalewski and Wojciech Skaba. Operations on submodules in left module over associative ring. *Formalized Mathematics*, 2(**2**):289–293, 1991.
[13] Michał Muzalewski and Wojciech Skaba. Submodules and cosets of submodules in left module over associative ring. *Formalized Mathematics*, 2(**2**):283–287, 1991.
[14] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.
[15] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[16] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.
[17] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[18] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[19] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1(**5**):877–882, 1990.
[20] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[22] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

Received October 22, 1990

FORMALIZED MATHEMATICS
Vol.2, No.2, March–April 1991
Université Catholique de Louvain

Linear Independence in Left Module over Domain [1]

Michał Muzalewski
Warsaw University
Białystok

Wojciech Skaba
University of Toruń

Summary. Notion of submodule generated by a set of vectors and linear independence of a set of vectors. A few theorems originated as a generalization of the theorems from the article [18].

MML Identifier: `LMOD_5`.

The articles [22], [5], [3], [2], [4], [6], [21], [16], [14], [15], [1], [17], [19], [20], [7], [8], [9], [12], [11], [10], and [13] provide the terminology and notation for this paper. For simplicity we adopt the following rules: x is arbitrary, R is an associative ring, V is a left module over R, v, v_1, v_2 are vectors of V, A, B are subsets of V, and l is a linear combination of A. We now define two new predicates. Let us consider R, V, A. We say that A is linearly independent if and only if:

(Def.1) for every l such that $\sum l = \Theta_V$ holds $\mathrm{support}\, l = \emptyset$.

A is linearly dependent stands for A is not linearly independent.

One can prove the following propositions:

(2)[2] If $A \subseteq B$ and B is linearly independent, then A is linearly independent.

(3) If $0_R \neq 1_R$ and A is linearly independent, then $\Theta_V \notin A$.

(4) $\emptyset_{\text{the carrier of the carrier of } V}$ is linearly independent.

(5) If $0_R \neq 1_R$ and $\{v_1, v_2\}$ is linearly independent, then $v_1 \neq \Theta_V$ and $v_2 \neq \Theta_V$.

(6) If $0_R \neq 1_R$, then $\{v, \Theta_V\}$ is linearly dependent and $\{\Theta_V, v\}$ is linearly dependent.

[1]Supported by RPBP.III-24.C6
[2]The proposition (1) was either repeated or obvious.

ISSN 0777–4028

For simplicity we follow the rules: R will be an integral domain, V will be a left module over R, W will be a submodule of V, A, B will be subsets of V, and l will be a linear combination of A. Let us consider R, V, A. The functor $\mathrm{Lin}(A)$ yields a submodule of V and is defined as follows:

(Def.2) the carrier of the carrier of $\mathrm{Lin}(A) = \{\sum l\}$.

One can prove the following propositions:

(7) If the carrier of the carrier of $W = \{\sum l\}$, then $W = \mathrm{Lin}(A)$.

(8) The carrier of the carrier of $\mathrm{Lin}(A) = \{\sum l\}$.

(9) $x \in \mathrm{Lin}(A)$ if and only if there exists l such that $x = \sum l$.

(10) If $x \in A$, then $x \in \mathrm{Lin}(A)$.

We now state several propositions:

(11) $\mathrm{Lin}(\emptyset_{\text{the carrier of the carrier of } V}) = \mathbf{0}_V$.

(12) If $\mathrm{Lin}(A) = \mathbf{0}_V$, then $A = \emptyset$ or $A = \{\Theta_V\}$.

(13) If $0_R \neq 1_R$ and $A =$ the carrier of the carrier of W, then $\mathrm{Lin}(A) = W$.

(14) If $0_R \neq 1_R$ and $A =$ the carrier of the carrier of V, then $\mathrm{Lin}(A) = V$.

(15) If $A \subseteq B$, then $\mathrm{Lin}(A)$ is a submodule of $\mathrm{Lin}(B)$.

(16) If $\mathrm{Lin}(A) = V$ and $A \subseteq B$, then $\mathrm{Lin}(B) = V$.

(17) $\mathrm{Lin}(A \cup B) = \mathrm{Lin}(A) + \mathrm{Lin}(B)$.

(18) $\mathrm{Lin}(A \cap B)$ is a submodule of $\mathrm{Lin}(A) \cap \mathrm{Lin}(B)$.

References

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

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 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] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[6] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

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

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

[9] Michał Muzalewski and Wojciech Skaba. Finite sums of vectors in left module over associative ring. *Formalized Mathematics*, 2(**2**):279–282, 1991.

[10] Michał Muzalewski and Wojciech Skaba. Linear combinations in left module over associative ring. *Formalized Mathematics*, 2(**2**):295–300, 1991.

[11] Michał Muzalewski and Wojciech Skaba. Operations on submodules in left module over associative ring. *Formalized Mathematics*, 2(**2**):289–293, 1991.

[12] Michał Muzalewski and Wojciech Skaba. Submodules and cosets of submodules in left module over associative ring. *Formalized Mathematics*, 2(**2**):283–287, 1991.

[13] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.

[14] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[15] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.
[16] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[17] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[18] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.
[19] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[20] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[22] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

Received October 22, 1990

FORMALIZED MATHEMATICS
Vol.2, No.**2**, March–April 1991
Université Catholique de Louvain

Calculus of Propositions [1]

Jan Popiołek
Warsaw University
Białystok

Andrzej Trybulec
Warsaw University
Białystok

Summary. Continues the analysis of the classical language of first order (see [6], [1], [3], [4], [2]). Three connectives : truth, negation and conjuction are primary (see [6]). The others (alternative, implication and equivalence) are defined with respect to them (see [1]). We prove some important tautologies of the calculus of propositions. Most of them are given as axioms of the classical logical calculus (see [5]). In the last part of our article we give some basic rules of inference.

MML Identifier: `PROCAL_1`.

The notation and terminology used here have been introduced in the papers [3] and [4]. In the sequel p, q, r, s are elements of CQC−WFF. One can prove the following propositions:

(1) $\neg(p \wedge \neg p) \in \mathrm{Taut}$.

(2) $p \vee \neg p \in \mathrm{Taut}$.

(3) $p \Rightarrow p \vee q \in \mathrm{Taut}$.

(4) $q \Rightarrow p \vee q \in \mathrm{Taut}$.

(5) $p \vee q \Rightarrow (\neg p \Rightarrow q) \in \mathrm{Taut}$.

(6) $\neg(p \vee q) \Rightarrow \neg p \wedge \neg q \in \mathrm{Taut}$.

(7) $\neg p \wedge \neg q \Rightarrow \neg(p \vee q) \in \mathrm{Taut}$.

(8) $p \vee q \Rightarrow q \vee p \in \mathrm{Taut}$.

(9) $\neg p \vee p \in \mathrm{Taut}$.

(10) $\neg(p \vee q) \Rightarrow \neg p \in \mathrm{Taut}$.

(11) $p \vee p \Rightarrow p \in \mathrm{Taut}$.

(12) $p \Rightarrow p \vee p \in \mathrm{Taut}$.

(13) $p \wedge \neg p \Rightarrow q \in \mathrm{Taut}$.

(14) $(p \Rightarrow q) \Rightarrow \neg p \vee q \in \mathrm{Taut}$.

[1]Supported by RPBP.III-24

ISSN 0777–4028

(15) $p \wedge q \Rightarrow \neg(p \Rightarrow \neg q) \in$ Taut.
(16) $\neg(p \Rightarrow \neg q) \Rightarrow p \wedge q \in$ Taut.
(17) $\neg(p \wedge q) \Rightarrow \neg p \vee \neg q \in$ Taut.
(18) $\neg p \vee \neg q \Rightarrow \neg(p \wedge q) \in$ Taut.
(19) $p \wedge q \Rightarrow p \in$ Taut.
(20) $p \wedge q \Rightarrow p \vee q \in$ Taut.
(21) $p \wedge q \Rightarrow q \in$ Taut.
(22) $p \Rightarrow p \wedge p \in$ Taut.
(23) $(p \Leftrightarrow q) \Rightarrow (p \Rightarrow q) \in$ Taut.
(24) $(p \Leftrightarrow q) \Rightarrow (q \Rightarrow p) \in$ Taut.
(25) $p \vee q \vee r \Rightarrow p \vee (q \vee r) \in$ Taut.
(26) $p \wedge q \wedge r \Rightarrow p \wedge (q \wedge r) \in$ Taut.
(27) $p \vee (q \vee r) \Rightarrow p \vee q \vee r \in$ Taut.
(28) $p \Rightarrow (q \Rightarrow p \wedge q) \in$ Taut.
(29) $(p \Rightarrow q) \Rightarrow ((q \Rightarrow p) \Rightarrow (p \Leftrightarrow q)) \in$ Taut.
(30) $p \vee q \Leftrightarrow q \vee p \in$ Taut.
(31) $(p \wedge q \Rightarrow r) \Rightarrow (p \Rightarrow (q \Rightarrow r)) \in$ Taut.

The following propositions are true:

(32) $(p \Rightarrow (q \Rightarrow r)) \Rightarrow (p \wedge q \Rightarrow r) \in$ Taut.
(33) $(r \Rightarrow p) \Rightarrow ((r \Rightarrow q) \Rightarrow (r \Rightarrow p \wedge q)) \in$ Taut.
(34) $(p \vee q \Rightarrow r) \Rightarrow (p \Rightarrow r) \vee (q \Rightarrow r) \in$ Taut.
(35) $(p \Rightarrow r) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \vee q \Rightarrow r)) \in$ Taut.
(36) $(p \Rightarrow r) \wedge (q \Rightarrow r) \Rightarrow (p \vee q \Rightarrow r) \in$ Taut.
(37) $(p \Rightarrow q \wedge \neg q) \Rightarrow \neg p \in$ Taut.
(38) $(p \vee q) \wedge (p \vee r) \Rightarrow p \vee q \wedge r \in$ Taut.
(39) $p \wedge (q \vee r) \Rightarrow p \wedge q \vee p \wedge r \in$ Taut.
(40) $(p \vee r) \wedge (q \vee r) \Rightarrow p \wedge q \vee r \in$ Taut.
(41) $(p \vee q) \wedge r \Rightarrow p \wedge r \vee q \wedge r \in$ Taut.
(42) If $p \in$ Taut, then $p \vee q \in$ Taut.
(43) If $q \in$ Taut, then $p \vee q \in$ Taut.
(44) If $p \wedge q \in$ Taut, then $p \in$ Taut.
(45) If $p \wedge q \in$ Taut, then $q \in$ Taut.
(46) If $p \wedge q \in$ Taut, then $p \vee q \in$ Taut.
(47) If $p \in$ Taut and $q \in$ Taut, then $p \wedge q \in$ Taut.
(48) If $p \Rightarrow q \in$ Taut, then $p \vee r \Rightarrow q \vee r \in$ Taut.
(49) If $p \Rightarrow q \in$ Taut, then $r \vee p \Rightarrow r \vee q \in$ Taut.
(50) If $p \Rightarrow q \in$ Taut, then $r \wedge p \Rightarrow r \wedge q \in$ Taut.
(51) If $p \Rightarrow q \in$ Taut, then $p \wedge r \Rightarrow q \wedge r \in$ Taut.
(52) If $r \Rightarrow p \in$ Taut and $r \Rightarrow q \in$ Taut, then $r \Rightarrow p \wedge q \in$ Taut.

(53) If $p \Rightarrow r \in$ Taut and $q \Rightarrow r \in$ Taut, then $p \vee q \Rightarrow r \in$ Taut.

(54) If $p \vee q \in$ Taut and $\neg p \in$ Taut, then $q \in$ Taut.

(55) If $p \vee q \in$ Taut and $\neg q \in$ Taut, then $p \in$ Taut.

(56) If $p \Rightarrow q \in$ Taut and $r \Rightarrow s \in$ Taut, then $p \wedge r \Rightarrow q \wedge s \in$ Taut.

(57) If $p \Rightarrow q \in$ Taut and $r \Rightarrow s \in$ Taut, then $p \vee r \Rightarrow q \vee s \in$ Taut.

(58) If $p \wedge \neg q \Rightarrow \neg p \in$ Taut, then $p \Rightarrow q \in$ Taut.

References

[1] Grzegorz Bancerek. Connectives and subformulae of the first order language. *Formalized Mathematics*, 1(**3**):451–458, 1990.

[2] Grzegorz Bancerek, Agata Darmochwał, and Andrzej Trybulec. Propositional calculus. *Formalized Mathematics*, 2(**1**):147–150, 1991.

[3] Czesław Byliński. A classical first order language. *Formalized Mathematics*, 1(**4**):669–676, 1990.

[4] Agata Darmochwał. A first–order predicate calculus. *Formalized Mathematics*, 1(**4**):689–695, 1990.

[5] Andrzej Grzegorczyk. *Zarys logiki matematycznej.* PWN, Warsaw, 1973.

[6] Piotr Rudnicki and Andrzej Trybulec. A first order language. *Formalized Mathematics*, 1(**2**):303–311, 1990.

Received October 23, 1990

FORMALIZED MATHEMATICS
Vol.2, No.2, March–April 1991
Université Catholique de Louvain

Calculus of Quantifiers. Deduction Theorem

Agata Darmochwał
Warsaw Uniwersity
Białystok

Summary. Some tautologies of the Classical Quantifier Calculus. The deduction theorem is also proved.

MML Identifier: CQC_THE2.

The papers [11], [13], [8], [2], [5], [3], [12], [10], [9], [1], [6], [4], and [7] provide the terminology and notation for this paper. For simplicity we adopt the following convention: X will denote a subset of CQC−WFF, F, G, p, q, r will denote elements of CQC−WFF, s, h will denote formulae, and x, y will denote bound variables. Next we state a number of propositions:

(1) If $\vdash p \Rightarrow (q \Rightarrow r)$, then $\vdash p \wedge q \Rightarrow r$.

(2) If $\vdash p \Rightarrow (q \Rightarrow r)$, then $\vdash q \wedge p \Rightarrow r$.

(3) If $\vdash p \wedge q \Rightarrow r$, then $\vdash p \Rightarrow (q \Rightarrow r)$.

(4) If $\vdash p \wedge q \Rightarrow r$, then $\vdash q \Rightarrow (p \Rightarrow r)$.

(5) $y \in \mathrm{snb}(\forall_x s)$ if and only if $y \in \mathrm{snb}(s)$ and $y \neq x$.

(6) $y \in \mathrm{snb}(\exists_x s)$ if and only if $y \in \mathrm{snb}(s)$ and $y \neq x$.

(7) $y \in \mathrm{snb}(s \Rightarrow h)$ if and only if $y \in \mathrm{snb}(s)$ or $y \in \mathrm{snb}(h)$.

(8) $y \in \mathrm{snb}(\neg s)$ if and only if $y \in \mathrm{snb}(s)$.

(9) $y \in \mathrm{snb}(s \wedge h)$ if and only if $y \in \mathrm{snb}(s)$ or $y \in \mathrm{snb}(h)$.

(10) $y \in \mathrm{snb}(s \vee h)$ if and only if $y \in \mathrm{snb}(s)$ or $y \in \mathrm{snb}(h)$.

(11) $x \notin \mathrm{snb}(\forall_{x,y} s)$ and $y \notin \mathrm{snb}(\forall_{x,y} s)$.

(12) $x \notin \mathrm{snb}(\exists_{x,y} s)$ and $y \notin \mathrm{snb}(\exists_{x,y} s)$.

(13) If F is closed, then $x \notin \mathrm{snb}(F)$.

(14) $s \Rightarrow h(x) = (s(x)) \Rightarrow (h(x))$.

(15) $s \vee h(x) = (s(x)) \vee (h(x))$.

ISSN 0777–4028

(16) $\exists_x p(x) = \exists_x p$.
(17) If $x \neq y$, then $\exists_x p(y) = \exists_x (p(y))$.
(18) $\vdash p \Rightarrow \exists_x p$.
(19) If $\vdash p$, then $\vdash \exists_x p$.
(20) $\vdash \forall_x p \Rightarrow \exists_x p$.
(21) $\vdash \forall_x p \Rightarrow \exists_y p$.
(22) If $\vdash p \Rightarrow q$ and $x \notin \mathrm{snb}(q)$, then $\vdash (\exists_x p) \Rightarrow q$.
(23) If $x \notin \mathrm{snb}(p)$, then $\vdash (\exists_x p) \Rightarrow p$.
(24) If $x \notin \mathrm{snb}(p)$ and $\vdash \exists_x p$, then $\vdash p$.
(25) If $p = h(x)$ and $q = h(y)$ and $y \notin \mathrm{snb}(h)$, then $\vdash p \Rightarrow \exists_y q$.
(26) If $\vdash p$, then $\vdash \forall_x p$.
(27) If $x \notin \mathrm{snb}(p)$, then $\vdash p \Rightarrow \forall_x p$.
(28) If $p = h(x)$ and $q = h(y)$ and $x \notin \mathrm{snb}(h)$, then $\vdash \forall_x p \Rightarrow q$.
(29) If $y \notin \mathrm{snb}(p)$, then $\vdash \forall_x p \Rightarrow \forall_y p$.
(30) If $p = h(x)$ and $q = h(y)$ and $x \notin \mathrm{snb}(h)$ and $y \notin \mathrm{snb}(p)$, then $\vdash \forall_x p \Rightarrow \forall_y q$.
(31) If $x \notin \mathrm{snb}(p)$, then $\vdash (\exists_x p) \Rightarrow \exists_y p$.

One can prove the following propositions:

(32) If $p = h(x)$ and $q = h(y)$ and $x \notin \mathrm{snb}(q)$ and $y \notin \mathrm{snb}(h)$, then $\vdash (\exists_x p) \Rightarrow \exists_y q$.
(34)[1] $\vdash \forall_x (p \Rightarrow q) \Rightarrow (\forall_x p \Rightarrow \forall_x q)$.
(35) If $\vdash \forall_x (p \Rightarrow q)$, then $\vdash \forall_x p \Rightarrow \forall_x q$.
(36) $\vdash \forall_x (p \Leftrightarrow q) \Rightarrow (\forall_x p \Leftrightarrow \forall_x q)$.
(37) If $\vdash \forall_x (p \Leftrightarrow q)$, then $\vdash \forall_x p \Leftrightarrow \forall_x q$.
(38) $\vdash \forall_x (p \Rightarrow q) \Rightarrow ((\exists_x p) \Rightarrow \exists_x q)$.
(39) If $\vdash \forall_x (p \Rightarrow q)$, then $\vdash (\exists_x p) \Rightarrow \exists_x q$.
(40) $\vdash \forall_x (p \wedge q) \Rightarrow \forall_x p \wedge \forall_x q$ and $\vdash \forall_x p \wedge \forall_x q \Rightarrow \forall_x (p \wedge q)$.
(41) $\vdash \forall_x (p \wedge q) \Leftrightarrow \forall_x p \wedge \forall_x q$.
(42) $\vdash \forall_x (p \wedge q)$ if and only if $\vdash \forall_x p \wedge \forall_x q$.
(43) $\vdash \forall_x p \vee \forall_x q \Rightarrow \forall_x (p \vee q)$.
(44) $\vdash (\exists_x p \vee q) \Rightarrow (\exists_x p) \vee \exists_x q$ and $\vdash (\exists_x p) \vee \exists_x q \Rightarrow \exists_x p \vee q$.
(45) $\vdash (\exists_x p \vee q) \Leftrightarrow (\exists_x p) \vee \exists_x q$.
(46) $\vdash \exists_x p \vee q$ if and only if $\vdash (\exists_x p) \vee \exists_x q$.
(47) $\vdash (\exists_x p \wedge q) \Rightarrow (\exists_x p) \wedge \exists_x q$.
(48) If $\vdash \exists_x p \wedge q$, then $\vdash (\exists_x p) \wedge \exists_x q$.
(49) $\vdash \forall_x \neg\neg p \Rightarrow \forall_x p$ and $\vdash \forall_x p \Rightarrow \forall_x \neg\neg p$.
(50) $\vdash \forall_x \neg\neg p \Leftrightarrow \forall_x p$.
(51) $\vdash (\exists_x \neg\neg p) \Rightarrow \exists_x p$ and $\vdash (\exists_x p) \Rightarrow \exists_x \neg\neg p$.

[1]The proposition (33) was either repeated or obvious.

(52) $\vdash (\exists_x\neg\neg p) \Leftrightarrow \exists_x p$.
(53) $\vdash \neg\exists_x\neg p \Rightarrow \forall_x p$ and $\vdash \forall_x p \Rightarrow \neg\exists_x\neg p$.
(54) $\vdash \neg\exists_x\neg p \Leftrightarrow \forall_x p$.
(55) $\vdash \neg\forall_x p \Rightarrow \exists_x\neg p$ and $\vdash (\exists_x\neg p) \Rightarrow \neg\forall_x p$.
(56) $\vdash \neg\forall_x p \Leftrightarrow \exists_x\neg p$.
(57) $\vdash \neg\exists_x p \Rightarrow \forall_x\neg p$ and $\vdash \forall_x\neg p \Rightarrow \neg\exists_x p$.
(58) $\vdash \forall_x\neg p \Leftrightarrow \neg\exists_x p$.
(59) $\vdash \forall_x\forall_y p \Rightarrow \forall_y\forall_x p$ and $\vdash \forall_{x,y} p \Rightarrow \forall_{y,x} p$.
(60) If $p = h(x)$ and $q = h(y)$ and $y \notin \mathrm{snb}(h)$, then $\vdash \forall_x\forall_y q \Rightarrow \forall_x p$.
(61) $\vdash (\exists_x\exists_y p) \Rightarrow \exists_y\exists_x p$ and $\vdash (\exists_{x,y} p) \Rightarrow (\exists_{y,x} p)$.
(62) If $p = h(x)$ and $q = h(y)$ and $y \notin \mathrm{snb}(h)$, then $\vdash (\exists_x p) \Rightarrow (\exists_{x,y} q)$.

We now state a number of propositions:

(63) $\vdash (\exists_x\forall_y p) \Rightarrow \forall_y\exists_x p$.
(64) $\vdash \exists_x p \Leftrightarrow p$.
(65) $\vdash (\exists_x p \Rightarrow q) \Rightarrow (\forall_x p \Rightarrow \exists_x q)$ and $\vdash (\forall_x p \Rightarrow \exists_x q) \Rightarrow \exists_x p \Rightarrow q$.
(66) $\vdash (\exists_x p \Rightarrow q) \Leftrightarrow (\forall_x p \Rightarrow \exists_x q)$.
(67) $\vdash \exists_x p \Rightarrow q$ if and only if $\vdash \forall_x p \Rightarrow \exists_x q$.
(68) $\vdash \forall_x(p \wedge q) \Rightarrow p \wedge \forall_x q$.
(69) $\vdash \forall_x(p \wedge q) \Rightarrow \forall_x p \wedge q$.
(70) If $x \notin \mathrm{snb}(p)$, then $\vdash p \wedge \forall_x q \Rightarrow \forall_x(p \wedge q)$.
(71) If $x \notin \mathrm{snb}(p)$ and $\vdash p \wedge \forall_x q$, then $\vdash \forall_x(p \wedge q)$.
(72) If $x \notin \mathrm{snb}(p)$, then $\vdash p \vee \forall_x q \Rightarrow \forall_x(p \vee q)$ and $\vdash \forall_x(p \vee q) \Rightarrow p \vee \forall_x q$.
(73) If $x \notin \mathrm{snb}(p)$, then $\vdash p \vee \forall_x q \Leftrightarrow \forall_x(p \vee q)$.
(74) If $x \notin \mathrm{snb}(p)$, then $\vdash p \vee \forall_x q$ if and only if $\vdash \forall_x(p \vee q)$.
(75) If $x \notin \mathrm{snb}(p)$, then $\vdash p \wedge \exists_x q \Rightarrow \exists_x p \wedge q$ and $\vdash (\exists_x p \wedge q) \Rightarrow p \wedge \exists_x q$.
(76) If $x \notin \mathrm{snb}(p)$, then $\vdash p \wedge \exists_x q \Leftrightarrow \exists_x p \wedge q$.
(77) If $x \notin \mathrm{snb}(p)$, then $\vdash p \wedge \exists_x q$ if and only if $\vdash \exists_x p \wedge q$.
(78) If $x \notin \mathrm{snb}(p)$, then $\vdash \forall_x(p \Rightarrow q) \Rightarrow (p \Rightarrow \forall_x q)$ and $\vdash (p \Rightarrow \forall_x q) \Rightarrow \forall_x(p \Rightarrow q)$.
(79) If $x \notin \mathrm{snb}(p)$, then $\vdash (p \Rightarrow \forall_x q) \Leftrightarrow \forall_x(p \Rightarrow q)$.
(80) If $x \notin \mathrm{snb}(p)$, then $\vdash \forall_x(p \Rightarrow q)$ if and only if $\vdash p \Rightarrow \forall_x q$.
(81) If $x \notin \mathrm{snb}(q)$, then $\vdash (\exists_x p \Rightarrow q) \Rightarrow (\forall_x p \Rightarrow q)$.
(82) $\vdash (\forall_x p \Rightarrow q) \Rightarrow \exists_x p \Rightarrow q$.
(83) If $x \notin \mathrm{snb}(q)$, then $\vdash \forall_x p \Rightarrow q$ if and only if $\vdash \exists_x p \Rightarrow q$.
(84) If $x \notin \mathrm{snb}(q)$, then $\vdash ((\exists_x p) \Rightarrow q) \Rightarrow \forall_x(p \Rightarrow q)$ and $\vdash \forall_x(p \Rightarrow q) \Rightarrow ((\exists_x p) \Rightarrow q)$.
(85) If $x \notin \mathrm{snb}(q)$, then $\vdash ((\exists_x p) \Rightarrow q) \Leftrightarrow \forall_x(p \Rightarrow q)$.
(86) If $x \notin \mathrm{snb}(q)$, then $\vdash (\exists_x p) \Rightarrow q$ if and only if $\vdash \forall_x(p \Rightarrow q)$.
(87) If $x \notin \mathrm{snb}(p)$, then $\vdash (\exists_x p \Rightarrow q) \Rightarrow (p \Rightarrow \exists_x q)$.

(88) $\vdash (p \Rightarrow \exists_x q) \Rightarrow \exists_x p \Rightarrow q$.

(89) If $x \notin \mathrm{snb}(p)$, then $\vdash (p \Rightarrow \exists_x q) \Leftrightarrow \exists_x p \Rightarrow q$.

(90) If $x \notin \mathrm{snb}(p)$, then $\vdash p \Rightarrow \exists_x q$ if and only if $\vdash \exists_x p \Rightarrow q$.

(91) $\{p\} \vdash p$.

(92) $\mathrm{Cn}(\{p\} \cup \{q\}) = \mathrm{Cn}\{p \wedge q\}$.

(93) $\{p, q\} \vdash r$ if and only if $\{p \wedge q\} \vdash r$.

The following propositions are true:

(94) If $X \vdash p$, then $X \vdash \forall_x p$.

(95) If $x \notin \mathrm{snb}(p)$, then $X \vdash \forall_x (p \Rightarrow q) \Rightarrow (p \Rightarrow \forall_x q)$.

(96) If F is closed and $X \cup \{F\} \vdash G$, then $X \vdash F \Rightarrow G$.

References

[1] Grzegorz Bancerek. Connectives and subformulae of the first order language. *Formalized Mathematics*, 1(**3**):451–458, 1990.

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

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

[4] Czesław Byliński. A classical first order language. *Formalized Mathematics*, 1(**4**):669–676, 1990.

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

[6] Czesław Byliński and Grzegorz Bancerek. Variables in formulae of the first order language. *Formalized Mathematics*, 1(**3**):459–469, 1990.

[7] Agata Darmochwał. A first–order predicate calculus. *Formalized Mathematics*, 1(**4**):689–695, 1990.

[8] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[9] Piotr Rudnicki and Andrzej Trybulec. A first order language. *Formalized Mathematics*, 1(**2**):303–311, 1990.

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

[11] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[12] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

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

Received October 24, 1990

alalalalalal
alalalalalalal

Index of MML Identifiers

Contents

Form. Math. 2 (**2**)

Continued on inside back cover