Contents

Formaliz. Math. 23 (**4**)

FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 279–288, 2015
DOI: 10.1515/forma-2015-0022

DE GRUYTER OPEN
degruyter.com/view/j/forma

Summable Family in a Commutative Group

Roland Coghetto
Rue de la Brasserie 5
7100 La Louvière, Belgium

Summary. Hölzl et al. showed that it was possible to build "a generic theory of limits based on filters" in Isabelle/HOL [22], [7]. In this paper we present our formalization of this theory in Mizar [6].

First, we compare the notions of the limit of a family indexed by a directed set, or a sequence, in a metric space [30], a real normed linear space [29] and a linear topological space [14] with the concept of the limit of an image filter [16].

Then, following Bourbaki [9], [10] (TG.III, §5.1 *Familles sommables dans un groupe commutatif*), we conclude by defining the summable families in a commutative group ("additive notation" in [17]), using the notion of filters.

MSC: 54A20 54H11 22A05 03B35

Keywords: limits; filters; topological group; summable family; convergence series; linear topological space

MML identifier: CARDFIL3, version: 8.1.04 5.34.1256

The notation and terminology used in this paper have been introduced in the following articles: [26], [16], [1], [27], [4], [18], [34], [32], [30], [11], [12], [35], [17], [23], [29], [20], [37], [2], [13], [8], [28], [39], [14], [36], [19], [31], [38], [24], [3], [25], [5], [21], and [15].

1. Preliminaries

Now we state the propositions:

(1) Let us consider a set I. Then $\emptyset$ is an element of $\operatorname{Fin} I$.

(2) Let us consider sets I, J. Suppose $J \in \operatorname{Fin} I$. Then there exists a finite sequence p of elements of I such that

(i) $J = \operatorname{rng} p$, and

ISSN 1426–2630(Print), 1898-9934(Online)

(ii) p is one-to-one.

(3) Let us consider a set I, a non empty set Y, a Y-valued many sorted set x indexed by I, and a finite sequence p of elements of I. Then $p \cdot x$ is a finite sequence of elements of Y.

(4) Let us consider non empty sets I, X, an X-valued many sorted set x indexed by I, and finite sequences p, q of elements of I. Then $(p \frown q) \cdot x = p \cdot x \frown (q \cdot x)$.

PROOF: For every object t such that $t \in \mathrm{dom}((p \frown q) \cdot x)$ holds $((p \frown q) \cdot x)(t) = (p \cdot x \frown (q \cdot x))(t)$ by [33, (120)], [11, (13)], [4, (25)]. □

Let I be a set, Y be a non empty set, x be a Y-valued many sorted set indexed by I, and p be a finite sequence of elements of I. The functor $\#_x^p$ yielding a finite sequence of elements of Y is defined by the term

(Def. 1) $p \cdot x$.

The functor $\mathcal{F}(I)$ yielding a non empty, transitive, reflexive relational structure is defined by the term

(Def. 2) $\langle \mathrm{Fin}\, I, \subseteq \rangle$.

Now we state the proposition:

(5) Let us consider a set I. Then $\Omega_{\mathcal{F}(I)}$ is directed.

2. Convergence in Metric Spaces

Now we state the propositions:

(6) Let us consider a non empty metric space M, and a point x of M_{top}. Then $\mathrm{Balls}\, x$ is a generalized basis of BooleanFilterToFilter(the neighborhood system of x).

(7) Let us consider a non empty metric space M, a non empty, transitive, reflexive relational structure L, a function f from Ω_L into the carrier of M_{top}, a point x of M_{top}, and a generalized basis B of BooleanFilterToFilter(the neighborhood system of x). Suppose Ω_L is directed. Then $x \in \mathrm{LimF}(f)$ if and only if for every element b of B, there exists an element i of L such that for every element j of L such that $i \leqslant j$ holds $f(j) \in b$.

(8) Let us consider a non empty metric space M, a non empty, transitive, reflexive relational structure L, a function f from Ω_L into the carrier of M_{top}, and a point x of M_{top}. Suppose Ω_L is directed. Then $x \in \mathrm{LimF}(f)$ if and only if for every element b of $\mathrm{Balls}\, x$, there exists an element n of L such that for every element m of L such that $n \leqslant m$ holds $f(m) \in b$. The theorem is a consequence of (6).

(9) Let us consider a non empty metric space M, a sequence s of the carrier of $M_{\rm top}$, and a point x of $M_{\rm top}$. Then $x \in {\rm LimF}(s)$ if and only if for every element b of ${\rm Balls}\, x$, there exists a natural number i such that for every natural number j such that $i \leqslant j$ holds $s(j) \in b$. The theorem is a consequence of (6).

(10) Let us consider a non empty topological structure T, a sequence s of T, and a point x of T. Then $x \in {\rm Lim}\, s$ if and only if for every subset U_1 of T such that U_1 is open and $x \in U_1$ there exists a natural number n such that for every natural number m such that $n \leqslant m$ holds $s(m) \in U_1$.

Let us consider a non empty metric space M, a sequence s of the carrier of $M_{\rm top}$, and a point x of $M_{\rm top}$. Now we state the propositions:

(11) $x \in {\rm Lim}\, s$ if and only if for every element b of ${\rm Balls}\, x$, there exists a natural number n such that for every natural number m such that $n \leqslant m$ holds $s(m) \in b$. The theorem is a consequence of (6) and (10).

(12) $x \in {\rm LimF}(s)$ if and only if $x \in {\rm Lim}\, s$. The theorem is a consequence of (9) and (11).

3. Filter and Limit of a Sequence in Real Normed Space

Now we state the propositions:

(13) Let us consider a real normed space N, a non empty, transitive, reflexive relational structure L, a function f from Ω_L into the carrier of $({\rm MetricSpaceNorm}\, N)_{\rm top}$, a point x of $({\rm MetricSpaceNorm}\, N)_{\rm top}$, and a generalized basis B of BooleanFilterToFilter(the neighborhood system of x). Suppose Ω_L is directed. Then $x \in {\rm LimF}(f)$ if and only if for every element b of B, there exists an element i of L such that for every element j of L such that $i \leqslant j$ holds $f(j) \in b$.

(14) Let us consider a real normed space N,
and a point x of $({\rm MetricSpaceNorm}\, N)_{\rm top}$. Then ${\rm Balls}\, x$ is a generalized basis of BooleanFilterToFilter(the neighborhood system of x).

(15) Let us consider a real normed space N, a sequence s of the carrier of $({\rm MetricSpaceNorm}\, N)_{\rm top}$, and a point x of $({\rm MetricSpaceNorm}\, N)_{\rm top}$. Then $x \in {\rm LimF}(s)$ if and only if for every element b of ${\rm Balls}\, x$, there exists a natural number i such that for every natural number j such that $i \leqslant j$ holds $s(j) \in b$.

(16) Let us consider a real normed space N, and a point x of (MetricSpaceNorm $N)_{\rm top}$. Then there exists a point y of ${\rm MetricSpaceNorm}\, N$ such that

(i) $y = x$, and

(ii) $\mathrm{Balls}\,x = \{\mathrm{Ball}(y, \frac{1}{n})$, where n is a natural number : $n \neq 0\}$.

(17) Let us consider a real normed space N, a point x of $(\mathrm{MetricSpaceNorm}\,N)_{\mathrm{top}}$, a point y of MetricSpaceNorm N, and a positive natural number n. If $x = y$, then $\mathrm{Ball}(y, \frac{1}{n}) \in \mathrm{Balls}\,x$.

(18) Let us consider a real normed space N, a point x of MetricSpaceNorm N, and a natural number n. Suppose $n \neq 0$. Then $\mathrm{Ball}(x, \frac{1}{n}) = \{q$, where q is an element of MetricSpaceNorm N : $\rho(x, q) < \frac{1}{n}\}$.

(19) Let us consider a real normed space N, an element x of MetricSpaceNorm N, and a natural number n. Suppose $n \neq 0$. Then there exists a point y of N such that

(i) $x = y$, and

(ii) $\mathrm{Ball}(x, \frac{1}{n}) = \{q$, where q is a point of N : $\|y - q\| < \frac{1}{n}\}$.

Let us consider a metric structure P_1. Now we state the propositions:

(20) $P_{1\mathrm{top}} = \langle$the carrier of P_1, the open set family of $P_1\rangle$.

(21) The carrier of $\langle$the carrier of P_1, the open set family of $P_1\rangle$ = the carrier of P_1.

(22) The carrier of $P_{1\mathrm{top}}$ = the carrier of $\langle$the carrier of P_1, the open set family of $P_1\rangle$.

(23) The carrier of $P_{1\mathrm{top}}$ = the carrier of P_1.

Now we state the proposition:

(24) Let us consider a real normed space N, a sequence s of the carrier of $(\mathrm{MetricSpaceNorm}\,N)_{\mathrm{top}}$, and a natural number j. Then $s(j)$ is an element of the carrier of $(\mathrm{MetricSpaceNorm}\,N)_{\mathrm{top}}$.

Let N be a real normed space and x be a point of $(\mathrm{MetricSpaceNorm}\,N)_{\mathrm{top}}$. The functor $\#\,x$ yielding a point of N is defined by the term

(Def. 3) x.

Now we state the proposition:

(25) Let us consider a real normed space N, a sequence s of the carrier of $(\mathrm{MetricSpaceNorm}\,N)_{\mathrm{top}}$, and a point x of $(\mathrm{MetricSpaceNorm}\,N)_{\mathrm{top}}$. Then $x \in \mathrm{LimF}(s)$ if and only if for every positive natural number n, there exists a natural number i such that for every natural number j such that $i \leqslant j$ holds $\|\#\,x - \#\,s(j)\| < \frac{1}{n}$.

PROOF: Reconsider $x_1 = x$ as a point of $(\mathrm{MetricSpaceNorm}\,N)_{\mathrm{top}}$. Consider y_0 being a point of MetricSpaceNorm N such that $y_0 = x_1$ and $\mathrm{Balls}\,x_1 = \{\mathrm{Ball}(y_0, \frac{1}{n})$, where n is a natural number : $n \neq 0\}$. If $x \in \mathrm{LimF}(s)$, then for every positive natural number n, there exists a natural number i such that for every natural number j such that $i \leqslant j$ holds

$\|\# x - \# s(j)\| < \frac{1}{n}$ by (9), [20, (2)]. If for every positive natural number n, there exists a natural number i such that for every natural number j such that $i \leqslant j$ holds $\|\# x - \# s(j)\| < \frac{1}{n}$, then $x \in \mathrm{LimF}(s)$ by [20, (2)], (9). □

4. Filter and Limit of a Sequence in Linear Topological Space

Now we state the propositions:

(26) Let us consider a non empty linear topological space X. Then the neighborhood system of 0_X is a local base of X.

(27) Let us consider a linear topological space X, a local base O of X, a point a of X, and a family P of subsets of X. Suppose $P = \{a+U$, where U is a subset of $X : U \in O\}$. Then P is a generalized basis of a.

(28) Let us consider a non empty linear topological space X, a point x of X, and a local base O of X. Then $\{x + U$, where U is a subset of X : $U \in O$ and U is a neighbourhood of $0_X\} = \{x + U$, where U is a subset of $X : U \in O$ and $U \in$ the neighborhood system of $0_X\}$.

(29) Let us consider a non empty linear topological space X, a point x of X, a local base O of X, and a family B of subsets of X. Suppose $B = \{x + U$, where U is a subset of X : $U \in O$ and U is a neighbourhood of $0_X\}$. Then B is a generalized basis of BooleanFilterToFilter(the neighborhood system of x).

Proof: Set $F =$ BooleanFilterToFilter(the neighborhood system of x). $F \subseteq [B]$ by [14, (9)], [27, (3)], [14, (8), (6)]. $[B] \subseteq F$ by [14, (37)]. □

(30) Let us consider a non empty linear topological space X, a sequence s of the carrier of X, a point x of X, a local base V of X, and a family B of subsets of X. Suppose $B = \{x+U$, where U is a subset of $X : U \in V$ and U is a neighbourhood of $0_X\}$. Then $x \in \mathrm{LimF}(s)$ if and only if for every element v of B, there exists a natural number i such that for every natural number j such that $i \leqslant j$ holds $s(j) \in v$. The theorem is a consequence of (29).

(31) Let us consider a non empty linear topological space X, a sequence s of the carrier of X, a point x of X, and a local base V of X. Then $x \in \mathrm{LimF}(s)$ if and only if for every subset v of X such that $v \in V \cap$(the neighborhood system of 0_X) there exists a natural number i such that for every natural number j such that $i \leqslant j$ holds $s(j) \in x + v$.

Proof: Set $B = \{x + U$, where U is a subset of $X : U \in V$ and U is a neighbourhood of $0_X\}$. B is a generalized basis of BooleanFilterToFilter (the neighborhood system of x). For every element b of B, there exists a natural number i such that for every natural number j such that $i \leqslant j$ holds $s(j) \in b$ by [5, (2)]. □

(32) Let us consider a non empty linear topological space T, a non empty, transitive, reflexive relational structure L, a function f from Ω_L into the carrier of T, a point x of T, and a generalized basis B of BooleanFilterToFilter(the neighborhood system of x). Suppose Ω_L is directed. Then $x \in \mathrm{LimF}(f)$ if and only if for every element b of B, there exists an element i of L such that for every element j of L such that $i \leqslant j$ holds $f(j) \in b$.

(33) Let us consider a non empty linear topological space T, a non empty, transitive, reflexive relational structure L, a function f from Ω_L into the carrier of T, a point x of T, and a local base V of T. Suppose Ω_L is directed. Then $x \in \mathrm{LimF}(f)$ if and only if for every subset v of T such that $v \in V \cap$ (the neighborhood system of 0_T) there exists an element i of L such that for every element j of L such that $i \leqslant j$ holds $f(j) \in x + v$.

5. Series in Abelian Group: a Definition

Let I be a non empty set, L be an Abelian group, x be a (the carrier of L)-valued many sorted set indexed by I, and J be an element of $\mathrm{Fin}\, I$. The functor $\sum_{\kappa=0}^{J} x(\kappa)$ yielding an element of L is defined by

(Def. 4) there exists a one-to-one finite sequence p of elements of I such that $\mathrm{rng}\, p = J$ and $it =$ (the addition of L) $\odot \#_x^p$.

Now we state the proposition:

(34) Let us consider a non empty set I, an Abelian group L, a (the carrier of L)-valued many sorted set x indexed by I, an element J of $\mathrm{Fin}\, I$, and an element e of $\mathrm{Fin}\, I$. Suppose $e = \emptyset$. Then

(i) $\sum_{\kappa=0}^{e} x(\kappa) = 0_L$, and

(ii) for every elements e, f of $\mathrm{Fin}\, I$ such that e misses f holds $\sum_{\kappa=0}^{e \cup f} x(\kappa) = \sum_{\kappa=0}^{e} x(\kappa) + \sum_{\kappa=0}^{f} x(\kappa)$.

The theorem is a consequence of (4).

Let I be a non empty set, L be an Abelian group, and x be a (the carrier of L)-valued many sorted set indexed by I. The functor $(\sum_{\alpha=0}^{\kappa} x(\alpha))_{\kappa \in \mathbb{N}}$ yielding a function from $\Omega_{\mathcal{F}(I)}$ into the carrier of L is defined by

(Def. 5) for every element j of $\mathrm{Fin}\, I$, $it(j) = \sum_{\kappa=0}^{j} x(\kappa)$.

6. Product of Family as Limit in Commutative Topological Group

Let I be a non empty set, L be a commutative semi topological group, x be a (the carrier of L)-valued many sorted set indexed by I, and J be an element of Fin I. The functor Product(x, J) yielding an element of L is defined by

(Def. 6) there exists a one-to-one finite sequence p of elements of I such that $\operatorname{rng} p = J$ and $it =$ (the multiplication of L) $\odot \#_x^p$.

(35) Let us consider a set I, a semi topological group G, a function f from $\Omega_{\mathcal{F}(I)}$ into the carrier of G, a point x of G, and a generalized basis B of BooleanFilterToFilter(the neighborhood system of x). Then $x \in \operatorname{LimF}(f)$ if and only if for every element b of B, there exists an element i of $\mathcal{F}(I)$ such that for every element j of $\mathcal{F}(I)$ such that $i \leqslant j$ holds $f(j) \in b$. The theorem is a consequence of (5).

(36) Let us consider a non empty set I, a commutative semi topological group L, a (the carrier of L)-valued many sorted set x indexed by I, an element J of Fin I, and an element e of Fin I. Suppose $e = \emptyset$. Then

(i) Product$(x, e) = \mathbf{1}_L$, and

(ii) for every elements e, f of Fin I such that e misses f holds Product$(x, e \cup f) =$ Product$(x, e) \cdot$ Product(x, f).

The theorem is a consequence of (4).

Let I be a non empty set, L be a commutative semi topological group, and x be a (the carrier of L)-valued many sorted set indexed by I. The functor the partial product of x yielding a function from $\Omega_{\mathcal{F}(I)}$ into the carrier of L is defined by

(Def. 7) for every element j of Fin I, $it(j) =$ Product(x, j).

(37) Let us consider a non empty set I, a commutative semi topological group G, a (the carrier of G)-valued many sorted set s indexed by I, a point x of G, and a generalized basis B of BooleanFilterToFilter(the neighborhood system of x). Then $x \in \operatorname{LimF}$(the partial product of s) if and only if for every element b of B, there exists an element i of $\mathcal{F}(I)$ such that for every element j of $\mathcal{F}(I)$ such that $i \leqslant j$ holds (the partial product of s)$(j) \in b$.

7. Summable Family in Commutative Topological Group

Let I be a non empty set, L be an Abelian semi additive topological group, x be a (the carrier of L)-valued many sorted set indexed by I, and J be an element of Fin I. The functor $\sum_{\kappa=0}^{J} x(\kappa)$ yielding an element of L is defined by

(Def. 8) there exists a one-to-one finite sequence p of elements of I such that $\operatorname{rng} p = J$ and $it = (\text{the addition of } L) \odot \#_x^p$.

Now we state the propositions:

(38) Let us consider a set I, a semi additive topological group G, a function f from $\Omega_{\mathcal{F}(I)}$ into the carrier of G, a point x of G, and a generalized basis B of BooleanFilterToFilter(the neighborhood system of x). Then $x \in \operatorname{LimF}(f)$ if and only if for every element b of B, there exists an element i of $\mathcal{F}(I)$ such that for every element j of $\mathcal{F}(I)$ such that $i \leqslant j$ holds $f(j) \in b$. The theorem is a consequence of (5).

(39) Let us consider a non empty set I, an Abelian semi additive topological group L, a (the carrier of L)-valued many sorted set x indexed by I, an element J of $\operatorname{Fin} I$, and an element e of $\operatorname{Fin} I$. Suppose $e = \emptyset$. Then

(i) $\sum_{\kappa=0}^{e} x(\kappa) = 0_L$, and

(ii) for every elements e, f of $\operatorname{Fin} I$ such that e misses f holds $\sum_{\kappa=0}^{e \cup f} x(\kappa) = \sum_{\kappa=0}^{e} x(\kappa) + \sum_{\kappa=0}^{f} x(\kappa)$.

The theorem is a consequence of (4).

Let I be a non empty set, L be an Abelian semi additive topological group, and x be a (the carrier of L)-valued many sorted set indexed by I. The functor $(\sum_{\alpha=0}^{\kappa} x(\alpha))_{\kappa \in \mathbb{N}}$ yielding a function from $\Omega_{\mathcal{F}(I)}$ into the carrier of L is defined by

(Def. 9) for every element j of $\operatorname{Fin} I$, $it(j) = \sum_{\kappa=0}^{j} x(\kappa)$.

Now we state the proposition:

(40) Let us consider a non empty set I, an Abelian semi additive topological group G, a (the carrier of G)-valued many sorted set s indexed by I, a point x of G, and a generalized basis B of BooleanFilterToFilter(the neighborhood system of x). Then $x \in \operatorname{LimF}((\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa \in \mathbb{N}})$ if and only if for every element b of B, there exists an element i of $\mathcal{F}(I)$ such that for every element j of $\mathcal{F}(I)$ such that $i \leqslant j$ holds $(\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa \in \mathbb{N}}(j) \in b$.

References

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

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

[3] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.

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

[5] Grzegorz Bancerek, Noboru Endou, and Yuji Sakai. On the characterizations of compactness. *Formalized Mathematics*, 9(**4**):733–738, 2001.

[6] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and

beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[7] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Formalization of real analysis: A survey of proof assistants and libraries. *Mathematical Structures in Computer Science*, pages 1–38, 2014.

[8] Leszek Borys. Paracompact and metrizable spaces. *Formalized Mathematics*, 2(**4**):481–485, 1991.

[9] Nicolas Bourbaki. *Topologie générale: Chapitres 1 à 4*. Eléments de mathématique. Springer Science & Business Media, 2007.

[10] Nicolas Bourbaki. *General Topology: Chapters 1–4*. Springer Science and Business Media, 2013.

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

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

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

[14] Czesław Byliński. Introduction to real linear topological spaces. *Formalized Mathematics*, 13(**1**):99–107, 2005.

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

[16] Roland Coghetto. Convergent filter bases. *Formalized Mathematics*, 23(**3**):189–203, 2015. doi:10.1515/forma-2015-0016.

[17] Roland Coghetto. Groups – additive notation. *Formalized Mathematics*, 23(**2**):127–160, 2015. doi:10.1515/forma-2015-0013.

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

[19] Noboru Endou, Takashi Mitsuishi, and Yasunari Shidama. Dimension of real unitary space. *Formalized Mathematics*, 11(**1**):23–28, 2003.

[20] Noboru Endou, Yasunari Shidama, and Katsumasa Okamura. Baire's category theorem and some spaces generated from real normed space. *Formalized Mathematics*, 14(**4**):213–219, 2006. doi:10.2478/v10037-006-0024-x.

[21] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Formalized Mathematics*, 6(**1**):117–121, 1997.

[22] Johannes Hölzl, Fabian Immler, and Brian Huffman. Type classes and filters for mathematical analysis in Isabelle/HOL. In *Interactive Theorem Proving*, pages 279–294. Springer, 2013.

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

[24] Artur Korniłowicz. The definition and basic properties of topological groups. *Formalized Mathematics*, 7(**2**):217–225, 1998.

[25] Artur Korniłowicz. Introduction to meet-continuous topological lattices. *Formalized Mathematics*, 7(**2**):279–283, 1998.

[26] Michał Muzalewski and Wojciech Skaba. From loops to Abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.

[27] Beata Padlewska. Locally connected spaces. *Formalized Mathematics*, 2(**1**):93–96, 1991.

[28] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.

[29] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.

[30] Bartłomiej Skorulski. First-countable, sequential, and Frechet spaces. *Formalized Mathematics*, 7(**1**):81–86, 1998.

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

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

[33] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *For-*

malized Mathematics, 1(**3**):569–573, 1990.
[34] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1 (**5**):979–981, 1990.
[35] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[36] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[37] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski – Zorn lemma. *Formalized Mathematics*, 1(**2**):387–393, 1990.
[38] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[39] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received August 14, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 289–296, 2015
DOI: 10.1515/forma-2015-0023

DE GRUYTER
OPEN
degruyter.com/view/j/forma

Topology from Neighbourhoods

Roland Coghetto
Rue de la Brasserie 5
7100 La Louvière, Belgium

Summary. Using Mizar [9], and the formal topological space structure (`FMT_Space_Str`) [19], we introduce the three `U-FMT` conditions (`U-FMT filter`, `U-FMT with point` and `U-FMT local`) similar to those V_I, V_{II}, V_{III} and V_{IV} of the proposition 2 in [10]:

> If to each element x of a set X there corresponds a set $\mathcal{B}(x)$ of subsets of X such that the properties V_I, V_{II}, V_{III} and V_{IV} are satisfied, then there is a unique topological structure on X such that, for each $x \in X$, $\mathcal{B}(x)$ is the set of neighborhoods of x in this topology.

We present a correspondence between a topological space and a space defined with the formal topological space structure with the three `U-FMT` conditions called the topology from neighbourhoods. For the formalization, we were inspired by the works of Bourbaki [11] and Claude Wagschal [31].

MSC: 54A05 03B35

Keywords: filter; topological space; neighbourhoods system

MML identifier: `FINTOPO7`, version: `8.1.04 5.34.1256`

The notation and terminology used in this paper have been introduced in the following articles: [24], [16], [1], [30], [17], [19], [12], [13], [27], [2], [34], [25], [28], [4], [14], [23], [32], [33], [22], [29], [5], [6], [8], [18], [26], and [15].

1. Preliminaries

From now on X denotes a non empty set.

Now we state the propositions:

(1) Let us consider families B, Y of subsets of X. If $Y \subseteq \mathrm{UniCl}(B)$, then $\bigcup Y \in \mathrm{UniCl}(B)$.

ISSN 1426–2630(Print), 1898-9934(Online)

(2) Let us consider an empty family B of subsets of X. Suppose for every elements B_1, B_2 of B, there exists a subset B_3 of B such that $B_1 \cap B_2 = \bigcup B_3$ and $X = \bigcup B$. Then $\mathrm{FinMeetCl}(B) \subseteq \mathrm{UniCl}(B)$.
PROOF: $\mathrm{FinMeetCl}(B) \subseteq \mathrm{UniCl}(B)$ by [22, (1)]. □

(3) Let us consider a non empty family B of subsets of X. Suppose for every elements B_1, B_2 of B, there exists a subset B_3 of B such that $B_1 \cap B_2 = \bigcup B_3$ and $X = \bigcup B$. Then $\mathrm{FinMeetCl}(B) \subseteq \mathrm{UniCl}(B)$.
PROOF: Reconsider $x_0 = x$ as a subset of X. Consider Y being a family of subsets of X such that $Y \subseteq B$ and Y is finite and $x_0 = \mathrm{Intersect}(Y)$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every family Y of subsets of X for every subset x of X such that $Y \subseteq B$ and $\overline{\overline{Y}} = \$_1$ and $x = \mathrm{Intersect}(Y)$ holds $x \in \mathrm{UniCl}(B)$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [20, (24)], [22, (10), (9)], [15, (2)]. For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 2]. □

(4) Let us consider a family B of subsets of X. Suppose for every elements B_1, B_2 of B, there exists a subset B_3 of B such that $B_1 \cap B_2 = \bigcup B_3$ and $X = \bigcup B$. Then

(i) $\mathrm{UniCl}(B) = \mathrm{UniCl}(\mathrm{FinMeetCl}(B))$, and

(ii) $\langle X, \mathrm{UniCl}(B) \rangle$ is topological space-like.

PROOF: $\mathrm{UniCl}(B) = \mathrm{UniCl}(\mathrm{FinMeetCl}(B))$ by [24, (4)], (2), (3), [7, (15)]. □

(5) Let us consider a non empty formal topological space R. Then there exists a relational structure S such that for every element x of R, $U_F(x)$ is a subset of S.

Let T be a non empty topological space. One can verify that $\mathrm{NeighSp}\,T$ is filled.

2. Open, Neighborhood and Conditions for Topological Space from Neighborhoods

Let E be a non empty, strict formal topological space and O be a subset of E. We say that O is open if and only if

(Def. 1) for every element x of E such that $x \in O$ holds $O \in U_F(x)$.

We say that E is U-FMT filter if and only if

(Def. 2) for every element x of E, $U_F(x)$ is a filter of the carrier of E.

We say that E is U-FMT with point if and only if

(Def. 3) for every element x of E and for every element V of $U_F(x)$, $x \in V$.

We say that E is U-FMT local if and only if

(Def. 4) for every element x of E and for every element V of $U_F(x)$, there exists an element W of $U_F(x)$ such that for every element y of E such that y is an element of W holds V is an element of $U_F(y)$.

Now we state the proposition:

(6) Let us consider a non empty, strict formal topological space E. Suppose E is U-FMT filter. Let us consider an element x of E. Then $U_F(x)$ is not empty.

Let us consider a non empty, strict formal topological space E. Now we state the propositions:

(7) If E is U-FMT with point, then E is filled.

(8) If E is filled and for every element x of E, $U_F(x)$ is not empty, then E is U-FMT with point.

(9) If E is filled and U-FMT filter, then E is U-FMT with point. The theorem is a consequence of (8).

Observe that there exists a non empty, strict formal topological space which is U-FMT local, U-FMT with point, and U-FMT filter.

Now we state the proposition:

(10) Let us consider a U-FMT filter, non empty, strict formal topological space E, and an element x of E. Then the carrier of $E \in U_F(x)$.

Let E be a U-FMT filter, non empty, strict formal topological space and x be an element of E.

A neighbourhood of x is a subset of E and is defined by

(Def. 5) $it \in U_F(x)$.

Let us observe that there exists a neighbourhood of x which is open.

Let A be a subset of E.

A neighbourhood of A is a subset of E and is defined by

(Def. 6) for every element x of E such that $x \in A$ holds $it \in U_F(x)$.

Note that there exists a neighbourhood of A which is open.

Now we state the proposition:

(11) Let us consider a U-FMT filter, non empty, strict formal topological space E, a subset A of E, a neighbourhood C of A, and a subset B of E. If $C \subseteq B$, then B is a neighbourhood of A.

Let E be a U-FMT filter, non empty, strict formal topological space and A be a subset of E. The functor Neighborhood A yielding a family of subsets of E is defined by the term

(Def. 7) the set of all N where N is a neighbourhood of A.

Now we state the proposition:

(12) Let us consider a U-FMT filter, non empty, strict formal topological space E, and a non empty subset A of E. Then Neighborhood A is a filter of the carrier of E. The theorem is a consequence of (10).

Let E be a non empty, strict formal topological space. We say that E is U-FMT filter base if and only if

(Def. 8) for every element x of the carrier of E, $U_F(x)$ is a filter base of the carrier of E.

Let E be a non empty formal topological space. The functor $[E]$ yielding a function from the carrier of E into $2^{2^{(\text{the carrier of } E)}}$ is defined by

(Def. 9) for every element x of the carrier of E, $it(x) = [U_F(x)]$.

Let E be a non empty, strict formal topological space. The functor gen-filter E yielding a non empty, strict formal topological space is defined by the term

(Def. 10) $\langle$the carrier of $E, [E]\rangle$.

Now we state the proposition:

(13) Let us consider a non empty, strict formal topological space E. Suppose E is U-FMT filter base. Then gen-filter E is U-FMT filter.

PROOF: For every element x of gen-filter E, $U_F(x)$ is a filter of the carrier of gen-filter E by [16, (25)]. $\square$

3. Topology from Neighborhoods: a Definition

A topology from neighbourhoods is a U-FMT local, U-FMT with point, U-FMT filter, non empty, strict formal topological space. Let E be a topology from neighbourhoods and x be an element of E. We introduce the notation the neighborhood system of x as a synonym of $U_F(x)$.

Let us note that there exists a subset of E which is open.

The functor the open set family of E yielding a non empty family of subsets of the carrier of E is defined by the term

(Def. 11) the set of all O where O is an open subset of E.

Now we state the propositions:

(14) Let us consider a topology from neighbourhoods E. Then

(i) $\emptyset$, the carrier of $E \in$ the open set family of E, and

(ii) for every family a of subsets of E such that $a \subseteq$ the open set family of E holds $\bigcup a \in$ the open set family of E, and

(iii) for every subsets a, b of E such that $a, b \in$ the open set family of E holds $a \cap b \in$ the open set family of E.

Proof: $\emptyset \in$ the open set family of E. The carrier of $E \in$ the open set family of E by [30, (5)]. For every family a of subsets of E such that $a \subseteq$ the open set family of E holds $\bigcup a \in$ the open set family of E by [15, (74)]. For every subsets a, b of E such that a, $b \in$ the open set family of E holds $a \cap b \in$ the open set family of E. □

(15) Let us consider a topology from neighbourhoods E, an element a of E, and a neighbourhood V of a. Then there exists an open subset O of E such that

(i) $a \in O$, and

(ii) $O \subseteq V$.

The theorem is a consequence of (6).

(16) Let us consider a topology from neighbourhoods E, a non empty subset A of E, and a subset V of E. Then V is a neighbourhood of A if and only if there exists an open subset O of E such that $A \subseteq O \subseteq V$.

Proof: If V is a neighbourhood of A, then there exists an open subset O of E such that $A \subseteq O \subseteq V$ by (15), (14), [13, (4)]. If there exists an open subset O of E such that $A \subseteq O \subseteq V$, then V is a neighbourhood of A. □

(17) Let us consider a topology from neighbourhoods E, and a non empty subset A of E. Then Neighborhood A is a filter of the carrier of E.

Let E be a topology from neighbourhoods and A be a non empty subset of E. The open neighbourhoods of A yielding a family of subsets of the carrier of E is defined by the term

(Def. 12) the set of all N where N is an open neighbourhood of A.

Now we state the propositions:

(18) Let us consider a topology from neighbourhoods E, a filter $\mathcal{F}$ of the carrier of E, a non empty subset $\mathcal{S}$ of $\mathcal{F}$, and a non empty subset A of E. Suppose $\mathcal{F}$ = Neighborhood A and $\mathcal{S}$ = the open neighbourhoods of A. Then $\mathcal{S}$ is filter basis. The theorem is a consequence of (16).

(19) Let us consider a non empty topological space T. Then there exists a topology from neighbourhoods E such that

(i) the carrier of T = the carrier of E, and

(ii) the open set family of E = the topology of T.

Proof: There exists a non empty, strict formal topological space E such that E is U-FMT filter, U-FMT with point, and U-FMT local and the carrier of T = the carrier of E and there exists a topology from neighbourhoods T_1 such that $T_1 = E$ and the open set family of T_1 = the topology of T by (13), [23, (1)], [21, (3), (7)]. Consider E being a non empty, strict formal topological space such that the carrier of T = the carrier of E and E is U-FMT filter, U-FMT with point, and U-FMT local and there exists a topology from neighbourhoods T_1 such that $T_1 = E$ and the open set family of T_1 = the topology of T. Consider T_1 being a topology from neighbourhoods such that $T_1 = E$ and the open set family of T_1 = the topology of T. □

(20) Let us consider a non empty topological space T, and a topology from neighbourhoods E. Suppose the carrier of T = the carrier of E and the open set family of E = the topology of T. Let us consider an element x of E. Then $U_F(x) = \{V$, where V is a subset of E : there exists a subset O of T such that $O \in$ the topology of T and $x \in O$ and $O \subseteq V\}$. The theorem is a consequence of (15).

4. Basis

Let E be a topology from neighbourhoods and F be a family of subsets of E. We say that F is quasi basis if and only if

(Def. 13) the open set family of $E \subseteq \mathrm{UniCl}(F)$.

Note that the open set family of E is quasi basis and there exists a family of subsets of E which is quasi basis.

Let S be a family of subsets of E. We say that S is open if and only if

(Def. 14) $S \subseteq$ the open set family of E.

One can check that there exists a family of subsets of E which is open and there exists a family of subsets of E which is open and quasi basis.

A basis of E is an open, quasi basis family of subsets of E. Now we state the propositions:

(21) Let us consider a topology from neighbourhoods E, and a basis B of E. Then the open set family of $E = \mathrm{UniCl}(B)$. The theorem is a consequence of (14).

(22) Let us consider a non empty family B of subsets of X. Suppose for every elements B_1, B_2 of B, there exists a subset B_3 of B such that $B_1 \cap B_2 = \bigcup B_3$ and $X = \bigcup B$. Then there exists a topology from neighbourhoods E such that

  (i) the carrier of $E = X$, and

  (ii) B is a basis of E.

The theorem is a consequence of (4) and (19).

(23) Let us consider a topology from neighbourhoods E, and a basis B of E. Then

(i) for every elements B_1, B_2 of B, there exists a subset B_3 of B such that $B_1 \cap B_2 = \bigcup B_3$, and

(ii) the carrier of $E = \bigcup B$.

PROOF: For every elements B_1, B_2 of B, there exists a subset B_3 of B such that $B_1 \cap B_2 = \bigcup B_3$ by [7, (16)], (14). The carrier of $X \in$ the open set family of X. Consider Y being a family of subsets of X such that $Y \subseteq B$ and the carrier of $X = \bigcup Y$. □

5. CORRESPONDENCE BETWEEN TOPOLOGICAL SPACE AND TOPOLOGY FROM NEIGHBORHOODS

Let T be a non empty topological space. The functor TopSpace2FMT T yielding a topology from neighbourhoods is defined by

(Def. 15) the carrier of *it* = the carrier of T and the open set family of *it* = the topology of T.

Let E be a topology from neighbourhoods. The functor FMT2TopSpace E yielding a strict topological space is defined by

(Def. 16) the carrier of *it* = the carrier of E and the open set family of E = the topology of *it*.

Let us observe that FMT2TopSpace E is non empty.

Now we state the propositions:

(24) Let us consider a non empty, strict topological space T. Then T = FMT2TopSpace TopSpace2FMT T.

(25) Let us consider a topology from neighbourhoods E. Then E = TopSpace2FMT FMT2TopSpace E.

REFERENCES

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

[2] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.

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

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

[5] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.

[6] Grzegorz Bancerek. Prime ideals and filters. *Formalized Mathematics*, 6(**2**):241–247, 1997.

[7] Grzegorz Bancerek. Bases and refinements of topologies. *Formalized Mathematics*, 7(**1**): 35–43, 1998.

[8] Grzegorz Bancerek, Noboru Endou, and Yuji Sakai. On the characterizations of compactness. *Formalized Mathematics*, 9(**4**):733–738, 2001.

[9] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[10] Nicolas Bourbaki. *General Topology: Chapters 1–4*. Springer Science and Business Media, 2013.

[11] Nicolas Bourbaki. *Topologie générale: Chapitres 1 à 4*. Eléments de mathématique. Springer Science & Business Media, 2007.

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

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

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

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

[16] Roland Coghetto. Convergent filter bases. *Formalized Mathematics*, 23(**3**):189–203, 2015. doi:10.1515/forma-2015-0016.

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

[18] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Formalized Mathematics*, 6(**1**):117–121, 1997.

[19] Gang Liu, Yasushi Fuwa, and Masayoshi Eguchi. Formal topological spaces. *Formalized Mathematics*, 9(**3**):537–543, 2001.

[20] Yatsuka Nakamura, Piotr Rudnicki, Andrzej Trybulec, and Pauline N. Kawamoto. Preliminaries to circuits, I. *Formalized Mathematics*, 5(**2**):167–172, 1996.

[21] Beata Padlewska. Locally connected spaces. *Formalized Mathematics*, 2(**1**):93–96, 1991.

[22] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[23] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.

[24] Alexander Yu. Shibakov and Andrzej Trybulec. The Cantor set. *Formalized Mathematics*, 5(**2**):233–236, 1996.

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

[26] Andrzej Trybulec. Moore-Smith convergence. *Formalized Mathematics*, 6(**2**):213–225, 1997.

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

[28] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski – Zorn lemma. *Formalized Mathematics*, 1(**2**):387–393, 1990.

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

[30] Josef Urban. Basic facts about inaccessible and measurable cardinals. *Formalized Mathematics*, 9(**2**):323–329, 2001.

[31] Claude Wagschal. *Topologie et analyse fonctionnelle*. Hermann, 1995.

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

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

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

Received August 14, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 297–307, 2015
DOI: 10.1515/forma-2015-0024

DE GRUYTER OPEN
degruyter.com/view/j/forma

Torsion Part of $\mathbb{Z}$-module

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

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize in Mizar [7] the definition of "torsion part" of $\mathbb{Z}$-module and its properties. We show $\mathbb{Z}$-module generated by the field of rational numbers as an example of torsion-free non free $\mathbb{Z}$-modules. We also formalize the rank-nullity theorem over finite-rank free $\mathbb{Z}$-modules (previously formalized in [1]). $\mathbb{Z}$-module is necessary for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm [23] and cryptographic systems with lattices [24].

MSC: 15A03 13C12 03B35

Keywords: torsion part of $\mathbb{Z}$-module; torsion-free non free $\mathbb{Z}$-module

MML identifier: ZMODUL07, version: 8.1.04 5.33.1254

The notation and terminology used in this paper have been introduced in the following articles: [27], [8], [2], [29], [6], [13], [9], [10], [17], [30], [22], [28], [25], [4], [5], [11], [20], [38], [39], [32], [37], [21], [33], [34], [35], [36], [12], [14], [15], [16], [26], and [19].

1. Torsion Part of $\mathbb{Z}$-module

From now on x, y, y_1, y_2 denote objects, V denotes a $\mathbb{Z}$-module, W, W_1, W_2 denote submodules of V, u, v denote vectors of V, and i, j, k, n denote elements of $\mathbb{N}$.

Now we state the proposition:

ISSN 1426–2630(Print), 1898-9934(Online)

(1) Let us consider an integer n. Suppose $n \neq 0$ and $n \neq -1$ and $n \neq -2$. Then $\frac{n}{n+1} \notin \mathbb{Z}$.

One can check that there exists an element of $\mathbb{Z}^{\mathrm{R}}$ which is prime and non zero and every element of $\mathbb{Z}^{\mathrm{R}}$ which is prime is also non zero.

Now we state the propositions:

(2) Let us consider a $\mathbb{Z}$-module V, and a subset A of V. Suppose A is linearly independent. Then there exists a subset B of V such that

(i) $A \subseteq B$, and

(ii) B is linearly independent, and

(iii) for every vector v of V, there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0$ and $a \cdot v \in \mathrm{Lin}(B)$.

PROOF: Define $\mathcal{P}[\text{set}] \equiv$ there exists a subset B of V such that $B = \$_1$ and $A \subseteq B$ and B is linearly independent. Consider Q being a set such that For every set Z, $Z \in Q$ iff $Z \in 2^{\alpha}$ and $\mathcal{P}[Z]$, where α is the carrier of V. Consider X being a set such that $X \in Q$ and for every set Z such that $Z \in Q$ and $Z \neq X$ holds $X \not\subseteq Z$. Consider B being a subset of V such that $B = X$ and $A \subseteq B$ and B is linearly independent. Consider v being a vector of V such that for every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0$ holds $a \cdot v \notin \mathrm{Lin}(B)$. $B \cup \{v\}$ is linearly independent by [10, (8)], [15, (39), (55)], [31, (61)]. □

(3) Let us consider a $\mathbb{Z}$-module V, a finite subset I of V, and a submodule W of V. Suppose for every vector v of V such that $v \in I$ there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $a \cdot v \in W$. Then there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that

(i) $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$, and

(ii) for every vector v of V such that $v \in I$ holds $a \cdot v \in W$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite subset I of V such that $\overline{\overline{I}} = \$_1$ and for every vector v of V such that $v \in I$ there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $a \cdot v \in W$ there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and for every vector v of V such that $v \in I$ holds $a \cdot v \in W$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [37, (41)], [3, (44)], [2, (30)], [14, (37)]. For every natural number n, $\mathcal{P}[n]$ from [4, Sch. 2]. □

(4) Let us consider a finite rank, free $\mathbb{Z}$-module V. Then every linearly independent subset of V is finite.

Let V be a finite rank, free $\mathbb{Z}$-module. Let us observe that every subset of V which is linearly independent is also finite.

Let us consider a finite rank, free $\mathbb{Z}$-module V and a linearly independent subset A of V. Now we state the propositions:

(5) There exists a finite, linearly independent subset I of V and there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $A \subseteq I$ and $a \circ V$ is a submodule of $\mathrm{Lin}(I)$.

(6) There exists a finite, linearly independent subset I of V such that

(i) $A \subseteq I$, and

(ii) $\operatorname{rank} V = \overline{\overline{I}}$.

The theorem is a consequence of (5).

Now we state the proposition:

(7) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a basis I_1 of W_1. Then there exists a finite, linearly independent subset I of V such that

(i) I is a subset of $W_1 + W_2$, and

(ii) $I_1 \subseteq I$, and

(iii) $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} \mathrm{Lin}(I)$.

The theorem is a consequence of (6).

Let us consider a torsion-free $\mathbb{Z}$-module V and finite rank, free submodules W_1, W_2 of V. Now we state the propositions:

(8) Suppose W_2 is a submodule of W_1. Then there exists a finite rank, free submodule W_3 of V such that

(i) $\operatorname{rank} W_1 = \operatorname{rank} W_2 + \operatorname{rank} W_3$, and

(ii) $W_2 \cap W_3 = \mathbf{0}_V$, and

(iii) W_3 is a submodule of W_1.

Proof: Set $I_2 =$ the basis of W_2. Reconsider $J_2 = I_2$ as a subset of W_1. Consider J_1 being a finite, linearly independent subset of W_1 such that $J_2 \subseteq J_1$ and $\operatorname{rank} W_1 = \overline{\overline{J_1}}$. Set $J_3 = J_1 \setminus J_2$. Reconsider $I_3 = J_3$ as a subset of V. $W_2 \cap \mathrm{Lin}(I_3) = \mathbf{0}_V$ by [16, (20)], [14, (42)], [18, (23)], [19, (4)]. □

(9) There exists a finite rank, free submodule W_3 of V such that

(i) $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_1 + \operatorname{rank} W_3$, and

(ii) $W_1 \cap W_3 = \mathbf{0}_V$, and

(iii) W_3 is a submodule of $W_1 + W_2$.

PROOF: Set I_1 = the basis of W_1. Consider I being a finite, linearly independent subset of V such that I is a subset of $W_1 + W_2$ and $I_1 \subseteq I$ and $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} \operatorname{Lin}(I)$. Set $I_2 = I \setminus I_1$. Reconsider $J_2 = I_2$ as a finite, linearly independent subset of V. $W_1 \cap \operatorname{Lin}(J_2) = \mathbf{0}_V$ by [16, (20)], [14, (42)], [18, (23)], [19, (4)]. □

Now we state the proposition:

(10) Let us consider a finite rank, free $\mathbb{Z}$-module V, and submodules W_1, W_2 of V. Then $\operatorname{rank}(W_1 \cap W_2) \geqslant \operatorname{rank} W_1 + \operatorname{rank} W_2 - \operatorname{rank} V$.

Let V be a $\mathbb{Z}$-module. The functor torsion-part(V) yielding a strict submodule of V is defined by

(Def. 1) the carrier of *it* = $\{v$, where v is a vector of $V : v$ is torsion$\}$.

Now we state the propositions:

(11) Let us consider a $\mathbb{Z}$-module V, and a vector v of V. Then v is torsion if and only if $v \in$ torsion-part(V).

(12) Let us consider a $\mathbb{Z}$-module V. Then V is torsion-free if and only if torsion-part$(V) = \mathbf{0}_V$. The theorem is a consequence of (11).

Let V be a $\mathbb{Z}$-module. Observe that $\mathbb{Z}$-ModuleQuot$(V,$ torsion-part$(V))$ is torsion-free.

Let W be a submodule of V. The functor $\mathbb{Z}$-QMorph(V, W) yielding a linear transformation from V to $\mathbb{Z}$-ModuleQuot(V, W) is defined by

(Def. 2) for every element v of V, $it(v) = v + W$.

One can check that $\mathbb{Z}$-QMorph(V, W) is onto.

Now we state the proposition:

(13) Let us consider $\mathbb{Z}$-modules V, W, a linear transformation T from V to W, a finite sequence s of elements of V, and a finite sequence t of elements of W. Suppose $\operatorname{len} s = \operatorname{len} t$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} s$ there exists a vector s_1 of V such that $s_1 = s(i)$ and $t(i) = T(s_1)$. Then $\sum t = T(\sum s)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence s of elements of V for every finite sequence t of elements of W such that $\operatorname{len} s = \$_1$ and $\operatorname{len} s = \operatorname{len} t$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} s$ there exists a vector s_1 of V such that $s_1 = s(i)$ and $t(i) = T(s_1)$ holds $\sum t = T(\sum s)$. $\mathcal{P}[0]$ by [32, (43)], [26, (19)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (59)], [4, (11)], [6, (4)], [9, (3)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

Let V be a finitely generated $\mathbb{Z}$-module and W be a submodule of V. Observe that $\mathbb{Z}$-ModuleQuot(V, W) is finitely generated and

$\mathbb{Z}$-ModuleQuot$(V,$ torsion-part$(V))$ is free.

2. $\mathbb{Z}$-module Generated by the Field of Rational Numbers

The functor $\mathbb{Z}$-module$\mathbb{Q}$ yielding a vector space structure over $\mathbb{Z}^{\mathrm{R}}$ is defined by the term

(Def. 3) $\langle$the carrier of $\mathbb{F}_{\mathbb{Q}}$, the addition of $\mathbb{F}_{\mathbb{Q}}$, the zero of $\mathbb{F}_{\mathbb{Q}}$, the left integer multiplication of $\mathbb{F}_{\mathbb{Q}}\rangle$.

One can verify that $\mathbb{Z}$-module$\mathbb{Q}$ is non empty and $\mathbb{Z}$-module$\mathbb{Q}$ is Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, and scalar unital.

Now we state the propositions:

(14) Let us consider an element v of $\mathbb{F}_{\mathbb{Q}}$, and a rational number v_1. Suppose $v = v_1$. Let us consider a natural number n. Then (Nat-mult-left $\mathbb{F}_{\mathbb{Q}})(n, v) = n \cdot v_1$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ (Nat-mult-left $\mathbb{F}_{\mathbb{Q}})(\$_1, v) = \$_1 \cdot v_1$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$. For every natural number n, $\mathcal{P}[n]$ from [4, Sch. 2]. □

(15) Let us consider an integer x, an element v of $\mathbb{F}_{\mathbb{Q}}$, and a rational number v_1. Suppose $v = v_1$. Then (the left integer multiplication of $\mathbb{F}_{\mathbb{Q}})(x, v) = x \cdot v_1$. The theorem is a consequence of (14).

Let us observe that $\mathbb{Z}$-module$\mathbb{Q}$ is torsion-free and $\mathbb{Z}$-module$\mathbb{Q}$ is non trivial.

Now we state the propositions:

(16) Let us consider an element s of $\mathbb{Z}$-module$\mathbb{Q}$. Then $\mathrm{Lin}(\{s\}) \neq \mathbb{Z}$-module$\mathbb{Q}$. The theorem is a consequence of (15) and (1).

(17) Let us consider elements s, t of $\mathbb{Z}$-module$\mathbb{Q}$. If $s \neq t$, then $\{s, t\}$ is not linearly independent. The theorem is a consequence of (15).

Let us observe that $\mathbb{Z}$-module$\mathbb{Q}$ is non free.

Now we state the proposition:

(18) Let us consider a finite subset A of $\mathbb{Z}$-module$\mathbb{Q}$. Then there exists an integer n such that

(i) $n \neq 0$, and

(ii) for every element s of $\mathbb{Z}$-module$\mathbb{Q}$ such that $s \in \mathrm{Lin}(A)$ there exists an integer m such that $s = \frac{m}{n}$.

PROOF: Set $S = \mathbb{Z}$-module$\mathbb{Q}$. Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset A of S such that $\overline{\overline{A}} = \$_1$ there exists an integer n such that $n \neq 0$ and for every element s of S such that $s \in \mathrm{Lin}(A)$ there exists an integer m such that $s = \frac{m}{n}$. $\mathcal{P}[0]$ by [15, (67)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [37, (41)], [3, (44)], [2, (30)], [20, (1)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

One can verify that $\mathbb{Z}$-module$\mathbb{Q}$ is non finitely generated.

Now we state the proposition:

(19) Let us consider a finite subset A of $\mathbb{Z}$-module$\mathbb{Q}$. Then $\operatorname{rank} \operatorname{Lin}(A) \leqslant 1$.

PROOF: Set $S = \mathbb{Z}$-module$\mathbb{Q}$. Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset A of S such that $\overline{\overline{A}} = \$_1$ holds $\operatorname{rank} \operatorname{Lin}(A) \leqslant 1$. $\mathcal{P}[0]$ by [15, (67)], [14, (51)], [26, (1)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [12, (31)], [3, (44)], [2, (30)], [15, (72)]. For every natural number n, $\mathcal{P}[n]$ from [4, Sch. 2]. $\square$

3. The Rank-Nullity Theorem

In the sequel V, W denote finite rank, free $\mathbb{Z}$-modules and T denotes a linear transformation from V to W.

Let W be a finite rank, free $\mathbb{Z}$-module, V be a $\mathbb{Z}$-module, and T be a linear transformation from V to W. Observe that $\operatorname{im} T$ is finite rank and free.

The functor $\operatorname{rank} T$ yielding a natural number is defined by the term

(Def. 4) $\operatorname{rank} \operatorname{im} T$.

Let V be a finite rank, free $\mathbb{Z}$-module and W be a $\mathbb{Z}$-module. The functor $\operatorname{nullity} T$ yielding a natural number is defined by the term

(Def. 5) $\operatorname{rank} \ker T$.

Now we state the propositions:

(20) Let us consider a finite rank, free $\mathbb{Z}$-module V, a subset A of V, a linearly independent subset B of V, and a linear transformation T from V to W. Suppose $\operatorname{rank} V = \overline{\overline{B}}$ and A is a basis of $\ker T$ and $A \subseteq B$. Then $T \restriction (B \setminus A)$ is one-to-one.

(21) Let us consider a finite rank, free $\mathbb{Z}$-module V, a subset A of V, a linearly independent subset B of V, a linear transformation T from V to W, and a linear combination l of $B \setminus A$. Suppose $\operatorname{rank} V = \overline{\overline{B}}$ and A is a basis of $\ker T$ and $A \subseteq B$. Then $T(\sum l) = \sum(T \,@\!*\, l)$. The theorem is a consequence of (20).

(22) Let us consider $\mathbb{Z}$-modules V, W, a linear transformation T from V to W, and a subset A of V. Suppose $A \subseteq$ the carrier of $\ker T$. Then $\operatorname{Lin}(T^{\circ} A) = \mathbf{0}_W$.

(23) Let us consider $\mathbb{Z}$-modules V, W, a linear transformation T from V to W, and subsets A, B, X of V. Suppose $A \subseteq$ the carrier of $\ker T$ and $X = B \cup A$. Then $\operatorname{Lin}(T^{\circ} X) = \operatorname{Lin}(T^{\circ} B)$. The theorem is a consequence of (22).

Let us consider finite rank, free $\mathbb{Z}$-modules V, W and a linear transformation T from V to W. Now we state the propositions:

(24) $\operatorname{rank} V = \operatorname{rank} T + \operatorname{nullity} T$.

PROOF: Set $A =$ the finite basis of $\ker T$. Reconsider $A' = A$ as a subset of V. Consider B' being a finite, linearly independent subset of V, a being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $A' \subseteq B'$ and $a \circ V$ is a submodule of $\mathrm{Lin}(B')$. Reconsider $X = B' \setminus A'$ as a finite subset of B'. Reconsider $C = T^{\circ}X$ as a finite subset of W. $T{\restriction}X$ is one-to-one. C is linearly independent by [26, (60)], (21), [26, (20)], [16, (20)]. Reconsider $a_1 = a \circ \operatorname{im} T$ as a submodule of W. $\mathrm{Lin}(T^{\circ}B') = \mathrm{Lin}(T^{\circ}X)$. For every vector v of W such that $v \in a_1$ holds $v \in \mathrm{Lin}(C)$ by [14, (25)], [26, (23)], [14, (29), (24)]. $\square$

(25) If T is one-to-one, then $\operatorname{rank} V = \operatorname{rank} T$. The theorem is a consequence of (24).

Let V, W be $\mathbb{Z}$-modules and T be a linear transformation from V to W. The functor $\mathbb{Z}$-decom(T) yielding a linear transformation from $\mathbb{Z}$-ModuleQuot$(V, \ker T)$ to $\operatorname{im} T$ is defined by

(Def. 6) *it* is bijective and for every element v of V, $it((\mathbb{Z}\text{-QMorph}(V, \ker T))(v)) = T(v)$.

Now we state the propositions:

(26) Let us consider $\mathbb{Z}$-modules V, W, and a linear transformation T from V to W. Then $T = \mathbb{Z}\text{-decom}(T) \cdot \mathbb{Z}\text{-QMorph}(V, \ker T)$.

PROOF: Set $g = \mathbb{Z}\text{-decom}(T) \cdot \mathbb{Z}\text{-QMorph}(V, \ker T)$. For every element z of V, $T(z) = g(z)$ by [10, (15)]. $\square$

(27) Let us consider $\mathbb{Z}$-modules V, U, W, a linear transformation f from V to U, and a linear transformation g from U to W. Then $g \cdot f$ is a linear transformation from V to W.

PROOF: Set $\mathfrak{f} = g \cdot f$. For every elements x, y of V, $\mathfrak{f}(x + y) = \mathfrak{f}(x) + \mathfrak{f}(y)$ by [10, (15)]. For every element a of $\mathbb{Z}^{\mathrm{R}}$ and for every element x of V, $\mathfrak{f}(a \cdot x) = a \cdot \mathfrak{f}(x)$ by [10, (15)]. $\square$

Let V, U, W be $\mathbb{Z}$-modules, f be a linear transformation from V to U, and g be a linear transformation from U to W. One can check that the functor $g \cdot f$ yields a linear transformation from V to W. Now we state the propositions:

(28) Let us consider $\mathbb{Z}$-modules V, W, and a linear transformation f from V to W. Then the carrier of $\ker f = f^{-1}(\{0_W\})$.

PROOF: For every object x, $x \in$ the carrier of $\ker f$ iff $x \in f^{-1}(\{0_W\})$ by [10, (38)]. $\square$

(29) Let us consider $\mathbb{Z}$-modules V, U, W, a linear transformation f from V to U, and a linear transformation g from U to W. Then the carrier of

$\ker g \cdot f = f^{-1}$(the carrier of $\ker g$). The theorem is a consequence of (28).

(30) Let us consider $\mathbb{Z}$-modules V, W, and a linear transformation f from V to W. If f is onto, then $\operatorname{im} f = \Omega_W$.

(31) Let us consider a $\mathbb{Z}$-module V, and a submodule W of V. Then $\ker \mathbb{Z}\text{-QMorph}(V, W) = \Omega_W$.
PROOF: Set $f = \mathbb{Z}\text{-QMorph}(V, W)$. Reconsider $W_1 = \Omega_W$ as a strict submodule of V. For every object x, $x \in f^{-1}(\{0_{\mathbb{Z}\text{-ModuleQuot}(V,W)}\})$ iff $x \in$ the carrier of W by [10, (38)], [14, (63)]. $\ker f = W_1$. □

(32) Let us consider a $\mathbb{Z}$-module V, a submodule W of V, a strict submodule W_1 of V, and a vector v of V. If $W_1 = \Omega_W$, then $v + W = v + W_1$.
PROOF: For every object x, $x \in v + W$ iff $x \in v + W_1$ by [14, (72)]. □

(33) Let us consider a $\mathbb{Z}$-module V, a submodule W of V, a strict submodule W_1 of V, and an object A. If $W_1 = \Omega_W$, then A is a coset of W iff A is a coset of W_1. The theorem is a consequence of (32).

Let us consider a $\mathbb{Z}$-module V, a submodule W of V, and a strict submodule W_1 of V.

Let us assume that $W_1 = \Omega_W$. Now we state the propositions:

(34) $\text{CosetSet}(V, W) = \text{CosetSet}(V, W_1)$. The theorem is a consequence of (33).

(35) $\text{addCoset}(V, W) = \text{addCoset}(V, W_1)$. The theorem is a consequence of (34) and (32).

(36) $\text{lmultCoset}(V, W) = \text{lmultCoset}(V, W_1)$. The theorem is a consequence of (34) and (32).

(37) $\mathbb{Z}\text{-ModuleQuot}(V, W) = \mathbb{Z}\text{-ModuleQuot}(V, W_1)$. The theorem is a consequence of (34), (35), and (36).

Now we state the propositions:

(38) Let us consider $\mathbb{Z}$-modules V, U, a submodule V_1 of V, a submodule U_1 of U, and a linear transformation f from V to U. Suppose f is onto and the carrier of $V_1 = f^{-1}$(the carrier of U_1). Then there exists a linear transformation F from $\mathbb{Z}\text{-ModuleQuot}(V, V_1)$ to $\mathbb{Z}\text{-ModuleQuot}(U, U_1)$ such that F is bijective. The theorem is a consequence of (37), (29), (31), and (30).

(39) Let us consider a $\mathbb{Z}$-module V, submodules W_1, W_2 of V, a submodule U_1 of $W_1 + W_2$, and a strict submodule U_2 of W_1. Suppose $U_1 = W_2$ and $U_2 = W_1 \cap W_2$. Then there exists a linear transformation F from $\mathbb{Z}\text{-ModuleQuot}(W_1 + W_2, U_1)$ to $\mathbb{Z}\text{-ModuleQuot}(W_1, U_2)$ such that F is bijective.
PROOF: Set $Z_1 = \mathbb{Z}\text{-ModuleQuot}(W_1 + W_2, U_1)$. Set $Z_2 = \mathbb{Z}\text{-ModuleQuot}$

(W_1, U_2). Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists an element v of $W_1 + W_2$ such that $\$_1 = v$ and $\$_2 = v + U_1$. For every element z of W_1, there exists an element y of Z_1 such that $\mathcal{P}[z, y]$ by [14, (25), (93)]. Consider f being a function from the carrier of W_1 into the carrier of Z_1 such that for every element z of W_1, $\mathcal{P}[z, f(z)]$ from [10, Sch. 3]. f is a linear transformation from W_1 to Z_1 by [14, (25), (28), (29)]. $\ker f = U_2$ by [26, (20)], [14, (63), (94), (46)]. $\operatorname{im} f = \mathbb{Z}$-ModuleQuot$(W_1 + W_2, U_1)$ by [14, (92), (93), (28)]. Reconsider $F = \mathbb{Z}$-decom(f) as a linear transformation from Z_2 to Z_1. Consider F_1 being a linear transformation from Z_1 to Z_2 such that $F_1 = F^{-1}$ and F_1 is bijective. □

(40) Let us consider a $\mathbb{Z}$-module V, a submodule W_1 of V, a submodule W_2 of W_1, a submodule U_1 of V, and a submodule U_2 of $\mathbb{Z}$-ModuleQuot(V, U_1). Suppose $U_1 = W_2$ and $U_2 = \mathbb{Z}$-ModuleQuot(W_1, W_2). Then there exists a linear transformation F from $\mathbb{Z}$-ModuleQuot($\mathbb{Z}$-ModuleQuot$(V, U_1), U_2)$ to $\mathbb{Z}$-ModuleQuot(V, W_1) such that F is bijective.

Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists an element v of V such that $\$_1 = v + U_1$ and $\$_2 = v + W_1$. For every element z of $\mathbb{Z}$-ModuleQuot(V, U_1), there exists an element y of $\mathbb{Z}$-ModuleQuot(V, W_1) such that $\mathcal{P}[z, y]$ by [10, (113)]. Consider f being a function from $\mathbb{Z}$-ModuleQuot(V, U_1) into $\mathbb{Z}$-ModuleQuot(V, W_1) such that for every element z of $\mathbb{Z}$-ModuleQuot(V, U_1), $\mathcal{P}[z, f(z)]$ from [10, Sch. 3]. f is a linear transformation from $\mathbb{Z}$-ModuleQuot(V, U_1) to $\mathbb{Z}$-ModuleQuot(V, W_1) by [14, (58), (24), (68)]. $\ker f = U_2$ by [26, (20)], [14, (63), (24), (28)]. $\operatorname{im} f = \mathbb{Z}$-ModuleQuot$(V, W_1)$ by [14, (58), (24), (68)], [10, (38), (41)]. □

Let V be a $\mathbb{Z}$-module and a be a non zero element of $\mathbb{Z}^{\mathrm{R}}$. Let us observe that $\mathbb{Z}$-ModuleQuot$(V, a \circ V)$ is torsion.

Now we state the propositions:

(41) Let us consider a trivial $\mathbb{Z}$-module V. Then $\Omega_V = \mathbf{0}_V$.

(42) Let us consider a $\mathbb{Z}$-module V, and a vector v of V. If $v \neq 0_V$, then $\operatorname{Lin}(\{v\})$ is not trivial. The theorem is a consequence of (41).

(43) There exists a $\mathbb{Z}$-module V and there exists an element p of $\mathbb{Z}^{\mathrm{R}}$ such that $p \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$ is not trivial.

Proof: Reconsider $V = \langle$the carrier of $\mathbb{Z}^{\mathrm{R}}$, the addition of $\mathbb{Z}^{\mathrm{R}}$, the zero of $\mathbb{Z}^{\mathrm{R}}$, the left integer multiplication of $(\mathbb{Z}^{\mathrm{R}})\rangle$ as a $\mathbb{Z}$-module. Reconsider $p = 2$ as an element of $\mathbb{Z}^{\mathrm{R}}$. $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$ is not trivial by [14, (63)], [19, (14)]. □

Note that there exists a torsion $\mathbb{Z}$-module which is non trivial and there exists a $\mathbb{Z}$-module which is non torsion-free.

Let V be a non torsion-free $\mathbb{Z}$-module. Let us note that there exists a vector of V which is non zero and torsion and there exists a finitely generated $\mathbb{Z}$-module which is non trivial.

Now we state the proposition:

(44) Let us consider a $\mathbb{Z}$-module V. Then V is torsion-free if and only if Ω_V is torsion-free.

Observe that every non torsion-free $\mathbb{Z}$-module is non trivial and there exists a finitely generated, torsion-free $\mathbb{Z}$-module which is non trivial.

Let V be a non trivial, finitely generated, torsion-free $\mathbb{Z}$-module and p be a prime element of $\mathbb{Z}^{\mathrm{R}}$. Let us note that $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$ is non trivial and there exists a torsion $\mathbb{Z}$-module which is finitely generated and there exists a finitely generated, torsion $\mathbb{Z}$-module which is non trivial.

Let V be a non trivial, finitely generated, torsion-free $\mathbb{Z}$-module and p be a prime element of $\mathbb{Z}^{\mathrm{R}}$. Note that $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$ is finitely generated and torsion.

Let V be a non torsion $\mathbb{Z}$-module.

One can verify that $\mathbb{Z}$-ModuleQuot$(V, \text{torsion-part}(V))$ is non trivial.

References

[1] Jesse Alama. The rank+nullity theorem. *Formalized Mathematics*, 15(**3**):137–142, 2007. doi:10.2478/v10037-007-0015-6.

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

[3] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.

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

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

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

[7] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

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

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

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

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

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

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

[14] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.

[15] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Quotient module of $\mathbb{Z}$-module. *Formalized Mathematics*, 20(**3**):205–214, 2012. doi:10.2478/v10037-012-0024-y.

[16] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Free ℤ-module. *Formalized Mathematics*, 20(**4**):275–280, 2012. doi:10.2478/v10037-012-0033-x.

[17] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Gaussian integers. *Formalized Mathematics*, 21(**2**):115–125, 2013. doi:10.2478/forma-2013-0013.

[18] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Submodule of free ℤ-module. *Formalized Mathematics*, 21(**4**):273–282, 2013. doi:10.2478/forma-2013-0029.

[19] Yuichi Futa, Hiroyuki Okazaki, Kazuhisa Nakasho, and Yasunari Shidama. Torsion ℤ-module and torsion-free ℤ-module. *Formalized Mathematics*, 22(**4**):277–289, 2014. doi:10.2478/forma-2014-0028.

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

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

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

[23] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4), 1982.

[24] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: a cryptographic perspective. *The International Series in Engineering and Computer Science*, 2002.

[25] Michał Muzalewski. Rings and modules – part II. *Formalized Mathematics*, 2(**4**):579–585, 1991.

[26] Kazuhisa Nakasho, Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Rank of submodule, linear transformations and linearly independent subsets of ℤ-module. *Formalized Mathematics*, 22(**3**):189–198, 2014. doi:10.2478/forma-2014-0021.

[27] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

[28] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.

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

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

[31] Wojciech A. Trybulec. Operations on subspaces in real linear space. *Formalized Mathematics*, 1(**2**):395–399, 1990.

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

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

[34] Wojciech A. Trybulec. Operations on subspaces in vector space. *Formalized Mathematics*, 1(**5**):871–876, 1990.

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

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

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

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

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

Received August 14, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 309–323, 2015
DOI: 10.1515/forma-2015-0025

DE GRUYTER OPEN
degruyter.com/view/j/forma

Construction of Measure from Semialgebra of Sets[1]

Noboru Endou
Gifu National College of Technology
Gifu, Japan

Summary. In our previous article [22], we showed complete additivity as a condition for extension of a measure. However, this condition premised the existence of a σ-field and the measure on it. In general, the existence of the measure on σ-field is not obvious. On the other hand, the proof of existence of a measure on a semialgebra is easier than in the case of a σ-field. Therefore, in this article we define a measure (`pre-measure`) on a semialgebra and extend it to a measure on a σ-field. Furthermore, we give a σ-measure as an extension of the measure on a σ-field. We follow [24], [10], and [31].

MSC: 28A12 03B35

Keywords: measure theory; pre-measure

MML identifier: `MEASURE9`, version: `8.1.04 5.34.1256`

The notation and terminology used in this paper have been introduced in the following articles: [1], [2], [19], [11], [5], [12], [17], [32], [13], [14], [26], [6], [7], [22], [20], [18], [21], [3], [4], [15], [27], [28], [35], [36], [30], [29], [23], [34], [8], [9], [25], and [16].

1. Joining Finite Sequences

Now we state the propositions:

(1) Let us consider a binary relation K. If $\operatorname{rng} K$ is empty-membered, then $\bigcup \operatorname{rng} K = \emptyset$.

(2) Let us consider a function K. Then $\operatorname{rng} K$ is empty-membered if and only if for every object x, $K(x) = \emptyset$.

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

Let D be a set, F be a set of finite sequences of D, f be a finite sequence of elements of F, and n be a natural number. Note that the functor $f(n)$ yields a finite sequence of elements of D. Let Y be a set of finite sequences of D and F be a finite sequence of elements of Y. The functor $\mathrm{Length}\, F$ yielding a finite sequence of elements of $\mathbb{N}$ is defined by

(Def. 1) $\mathrm{dom}\, it = \mathrm{dom}\, F$ and for every natural number n such that $n \in \mathrm{dom}\, it$ holds $it(n) = \mathrm{len}(F(n))$.

Now we state the propositions:

(3) Let us consider a set D, a set Y of finite sequences of D, and a finite sequence F of elements of Y. Suppose for every natural number n such that $n \in \mathrm{dom}\, F$ holds $F(n) = \varepsilon_D$. Then $\sum \mathrm{Length}\, F = 0$.

(4) Let us consider a set D, a set Y of finite sequences of D, a finite sequence F of elements of Y, and a natural number k. Suppose $k < \mathrm{len}\, F$. Then $\mathrm{Length}(F{\restriction}(k+1)) = \mathrm{Length}(F{\restriction}k) \frown \langle \mathrm{len}(F(k+1)) \rangle$.

(5) Let us consider a set D, a set Y of finite sequences of D, a finite sequence F of elements of Y, and a natural number n. Suppose $1 \leqslant n \leqslant \sum \mathrm{Length}\, F$. Then there exist natural numbers k, m such that

(i) $1 \leqslant m \leqslant \mathrm{len}(F(k+1))$, and

(ii) $k < \mathrm{len}\, F$, and

(iii) $m + \sum \mathrm{Length}(F{\restriction}k) = n$, and

(iv) $n \leqslant \sum \mathrm{Length}(F{\restriction}(k+1))$.

The theorem is a consequence of (4).

(6) Let us consider a set D, a set Y of finite sequences of D, and finite sequences F_1, F_2 of elements of Y. Then $\mathrm{Length}(F_1 \frown F_2) = \mathrm{Length}\, F_1 \frown \mathrm{Length}\, F_2$.

(7) Let us consider a set D, a set Y of finite sequences of D, a finite sequence F of elements of Y, and natural numbers k_1, k_2. Suppose $k_1 \leqslant k_2$. Then $\sum \mathrm{Length}(F{\restriction}k_1) \leqslant \sum \mathrm{Length}(F{\restriction}k_2)$. The theorem is a consequence of (6).

(8) Let us consider a set D, a set Y of finite sequences of D, a finite sequence F of elements of Y, and natural numbers m_1, m_2, k_1, k_2. Suppose $1 \leqslant m_1$ and $1 \leqslant m_2$ and $m_1 + \sum \mathrm{Length}(F{\restriction}k_1) = m_2 + \sum \mathrm{Length}(F{\restriction}k_2)$ and $m_1 + \sum \mathrm{Length}(F{\restriction}k_1) \leqslant \sum \mathrm{Length}(F{\restriction}(k_1+1))$ and $m_2 + \sum \mathrm{Length}(F{\restriction}k_2) \leqslant \sum \mathrm{Length}(F{\restriction}(k_2+1))$. Then

(i) $m_1 = m_2$, and

(ii) $k_1 = k_2$.

The theorem is a consequence of (7).

Let D be a non empty set, Y be a set of finite sequences of D, and F be a finite sequence of elements of Y. The functor joinedFinSeq F yielding a finite sequence of elements of D is defined by

(Def. 2) $\operatorname{len} it = \sum \operatorname{Length} F$ and for every natural number n such that $n \in \operatorname{dom} it$ there exist natural numbers k, m such that $1 \leqslant m \leqslant \operatorname{len}(F(k+1))$ and $k < \operatorname{len} F$ and $m + \sum \operatorname{Length}(F \restriction k) = n$ and $n \leqslant \sum \operatorname{Length}(F \restriction (k+1))$ and $it(n) = F(k+1)(m)$.

Let D be a set, Y be a set of finite sequences of D and s be a sequence of Y. The functor Length s yielding a sequence of $\mathbb{N}$ is defined by

(Def. 3) for every natural number n, $it(n) = \operatorname{len}(s(n))$.

Let s be a sequence of $\mathbb{N}$. One can check that the functor $(\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa \in \mathbb{N}}$ yields a sequence of $\mathbb{N}$. Let D be a non empty set. Let us note that there exists a set of finite sequences of D which is non empty and has a non-empty element.

Let us consider a non empty set D, a non empty set Y of finite sequences of D with a non-empty element, a non-empty sequence s of Y, and a natural number n. Now we state the propositions:

(9) (i) $\operatorname{len}(s(n)) \geqslant 1$, and

(ii) $n < (\sum_{\alpha=0}^{\kappa} (\operatorname{Length} s)(\alpha))_{\kappa \in \mathbb{N}}(n) < (\sum_{\alpha=0}^{\kappa} (\operatorname{Length} s)(\alpha))_{\kappa \in \mathbb{N}}(n+1)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \$_1 < (\sum_{\alpha=0}^{\kappa} (\operatorname{Length} s)(\alpha))_{\kappa \in \mathbb{N}}(\$_1)$. For every natural number k, $\operatorname{len}(s(k)) \geqslant 1$ by [5, (20)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 2]. □

(10) There exist natural numbers k, m such that

(i) $m \in \operatorname{dom}(s(k))$, and

(ii) $(\sum_{\alpha=0}^{\kappa} (\operatorname{Length} s)(\alpha))_{\kappa \in \mathbb{N}}(k) - \operatorname{len}(s(k)) + m - 1 = n$.

The theorem is a consequence of (9).

(11) Let us consider a non empty set D, a non empty set Y of finite sequences of D with a non-empty element, and a non-empty sequence s of Y. Then $(\sum_{\alpha=0}^{\kappa} (\operatorname{Length} s)(\alpha))_{\kappa \in \mathbb{N}}$ is increasing.

(12) Let us consider a non empty set D, a non empty set Y of finite sequences of D with a non-empty element, a non-empty sequence s of Y, and natural numbers m_1, m_2, k_1, k_2. Suppose $m_1 \in \operatorname{dom}(s(k_1))$ and $m_2 \in \operatorname{dom}(s(k_2))$ and $(\sum_{\alpha=0}^{\kappa} (\operatorname{Length} s)(\alpha))_{\kappa \in \mathbb{N}}(k_1) - \operatorname{len}(s(k_1)) + m_1 = (\sum_{\alpha=0}^{\kappa} (\operatorname{Length} s)(\alpha))_{\kappa \in \mathbb{N}}(k_2) - \operatorname{len}(s(k_2)) + m_2$. Then

(i) $m_1 = m_2$, and

(ii) $k_1 = k_2$.

The theorem is a consequence of (11).

(13) Let us consider a non empty set D, a set Y of finite sequences of D with a non-empty element, and a non-empty sequence s of Y. Then there exists an increasing sequence N of $\mathbb{N}$ such that for every natural number k, $N(k) = (\sum_{\alpha=0}^{\kappa}(\text{Length}\, s)(\alpha))_{\kappa\in\mathbb{N}}(k) - 1$.

Proof: Define $\mathcal{P}[\text{natural number}, \text{natural number}] \equiv \$_2 = (\sum_{\alpha=0}^{\kappa}(\text{Length}\, s)(\alpha))_{\kappa\in\mathbb{N}}(\$_1) - 1$. For every element k of $\mathbb{N}$, there exists an element n of $\mathbb{N}$ such that $\mathcal{P}[k, n]$ by (9), [3, (20)]. Consider N being a function from $\mathbb{N}$ into $\mathbb{N}$ such that for every element k of $\mathbb{N}$, $\mathcal{P}[k, N(k)]$ from [14, Sch. 3]. For every natural number k, $N(k) = (\sum_{\alpha=0}^{\kappa}(\text{Length}\, s)(\alpha))_{\kappa\in\mathbb{N}}(k) - 1$. For every natural number n, $N(n) < N(n+1)$. □

Let D be a non empty set, Y be a set of finite sequences of D with a non-empty element, and s be a non-empty sequence of Y. The functor joinedSeq s yielding a sequence of D is defined by

(Def. 4) for every natural number n, there exist natural numbers k, m such that $m \in \text{dom}(s(k))$ and $(\sum_{\alpha=0}^{\kappa}(\text{Length}\, s)(\alpha))_{\kappa\in\mathbb{N}}(k) - \text{len}(s(k)) + m - 1 = n$ and $it(n) = s(k)(m)$.

Now we state the propositions:

(14) Let us consider a non empty set D, a set Y of finite sequences of D with a non-empty element, a non-empty sequence s of Y, and a sequence s_1 of D. Suppose for every natural number n, $s_1(n) = (\text{joinedSeq}\, s)((\sum_{\alpha=0}^{\kappa}(\text{Length}\, s)(\alpha))_{\kappa\in\mathbb{N}}(n) - 1)$. Then s_1 is a subsequence of joinedSeq s.

Proof: Consider N being an increasing sequence of $\mathbb{N}$ such that for every natural number n, $N(n) = (\sum_{\alpha=0}^{\kappa}(\text{Length}\, s)(\alpha))_{\kappa\in\mathbb{N}}(n) - 1$. For every element n of $\mathbb{N}$, $s_1(n) = (\text{joinedSeq}\, s \cdot N)(n)$ by [14, (15)]. □

(15) Let us consider a non empty set D, a set Y of finite sequences of D with a non-empty element, a non-empty sequence s of Y, and natural numbers k, m. Suppose $m \in \text{dom}(s(k))$. Then there exists a natural number n such that

(i) $n = (\sum_{\alpha=0}^{\kappa}(\text{Length}\, s)(\alpha))_{\kappa\in\mathbb{N}}(k) - \text{len}(s(k)) + m - 1$, and

(ii) $(\text{joinedSeq}\, s)(n) = s(k)(m)$.

The theorem is a consequence of (12).

Let us consider a non empty set D, a set Y of finite sequences of D, and a finite sequence F of elements of Y. Now we state the propositions:

(16) Suppose for every natural numbers n, m such that $n \neq m$ holds $\bigcup \text{rng}(F(n))$ misses $\bigcup \text{rng}(F(m))$ and for every natural number n, $F(n)$ is disjoint valued. Then joinedFinSeq F is disjoint valued.

(17) rng joinedFinSeq $F = \bigcup\{\text{rng}(F(n))$, where n is a natural number : $n \in \text{dom}\, F\}$. The theorem is a consequence of (4), (7), and (8).

2. Extended Real-Valued Matrix

Let x be an extended real number. One can check that the functor $\langle x \rangle$ yields a finite sequence of elements of $\overline{\mathbb{R}}$. Let e be a finite sequence of elements of $\overline{\mathbb{R}}^*$. The functor $\sum e$ yielding a finite sequence of elements of $\overline{\mathbb{R}}$ is defined by

(Def. 5) len it = len e and for every natural number k such that $k \in \text{dom}\, it$ holds $it(k) = \sum(e(k))$.

Let M be a matrix over $\overline{\mathbb{R}}$. The functor SumAll M yielding an element of $\overline{\mathbb{R}}$ is defined by the term

(Def. 6) $\sum \sum M$.

Now we state the propositions:

(18) Let us consider a matrix M over $\overline{\mathbb{R}}$. Then

(i) len $\sum M$ = len M, and

(ii) for every natural number i such that $i \in \text{Seg len}\, M$ holds $(\sum M)(i) = \sum \text{Line}(M, i)$.

(19) Let us consider a finite sequence F of elements of $\overline{\mathbb{R}}$. Suppose for every natural number i such that $i \in \text{dom}\, F$ holds $F(i) \neq -\infty$. Then $\sum F \neq -\infty$.

Proof: Consider f being a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$ such that $\sum F = f(\text{len}\, F)$ and $f(0) = 0$ and for every natural number i such that $i < \text{len}\, F$ holds $f(i+1) = f(i) + F(i+1)$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant \text{len}\, F$, then $f(\$_1) \neq -\infty$. For every natural number j such that $\mathcal{P}[j]$ holds $\mathcal{P}[j+1]$ by [3, (13), (11)], [33, (25)]. For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

(20) Let us consider finite sequences F, G, H of elements of $\overline{\mathbb{R}}$. Suppose $-\infty \notin \text{rng}\, F$ and $-\infty \notin \text{rng}\, G$ and $\text{dom}\, F = \text{dom}\, G$ and $H = F + G$. Then $\sum H = \sum F + \sum G$.

Proof: Consider h being a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$ such that $\sum H = h(\text{len}\, H)$ and $h(0) = 0_{\overline{\mathbb{R}}}$ and for every natural number i such that $i < \text{len}\, H$ holds $h(i+1) = h(i) + H(i+1)$. Consider f being a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$ such that $\sum F = f(\text{len}\, F)$ and $f(0) = 0_{\overline{\mathbb{R}}}$ and for every natural number i such that $i < \text{len}\, F$ holds $f(i+1) = f(i) + F(i+1)$. Consider g being a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$ such that $\sum G = g(\text{len}\, G)$ and $g(0) = 0_{\overline{\mathbb{R}}}$ and for every natural number i such that $i < \text{len}\, G$ holds $g(i+1) = g(i) + G(i+1)$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant \text{len}\, H$, then $h(\$_1) = f(\$_1) + g(\$_1)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [3, (13), (11)], [33, (25)], [13, (3)]. For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

(21) Let us consider an extended real number r, and a finite sequence F of elements of $\overline{\mathbb{R}}$. Then $\sum(F \frown \langle r \rangle) = \sum F + r$.

PROOF: Consider f being a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$ such that $\sum(F \frown \langle r \rangle) = f(\mathrm{len}(F \frown \langle r \rangle))$ and $f(0) = 0$ and for every natural number i such that $i < \mathrm{len}(F \frown \langle r \rangle)$ holds $f(i+1) = f(i) + (F \frown \langle r \rangle)(i+1)$. Consider g being a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$ such that $\sum F = g(\mathrm{len}\, F)$ and $g(0) = 0$ and for every natural number i such that $i < \mathrm{len}\, F$ holds $g(i+1) = g(i) + F(i+1)$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant \mathrm{len}\, F$, then $f(\$_1) = g(\$_1)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [3, (13)], [5, (64)], [3, (11)]. For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

(22) Let us consider an extended real number r, and a natural number i. If r is real, then $\sum(i \mapsto r) = i \cdot r$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \sum(\$_1 \mapsto r) = \$_1 \cdot r$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [12, (60)], (21). For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

(23) Let us consider a matrix M over $\overline{\mathbb{R}}$. If $\mathrm{len}\, M = 0$, then $\mathrm{SumAll}\, M = 0$.

(24) Let us consider a natural number m, and a matrix M over $\overline{\mathbb{R}}$ of dimension $m \times 0$. Then $\mathrm{SumAll}\, M = 0$. The theorem is a consequence of (23) and (22).

(25) Let us consider natural numbers n, m, k, a matrix M_1 over $\overline{\mathbb{R}}$ of dimension $n \times k$, and a matrix M_2 over $\overline{\mathbb{R}}$ of dimension $m \times k$. Then $\sum(M_1 \frown M_2) = \sum M_1 \frown \sum M_2$.

Let us consider matrices M_1, M_2 over $\overline{\mathbb{R}}$. Now we state the propositions:

(26) Suppose for every natural number i such that $i \in \mathrm{dom}\, M_1$ holds $-\infty \notin \mathrm{rng}(M_1(i))$ and for every natural number i such that $i \in \mathrm{dom}\, M_2$ holds $-\infty \notin \mathrm{rng}(M_2(i))$. Then $\sum M_1 + \sum M_2 = \sum(M_1 \frown M_2)$. The theorem is a consequence of (19).

(27) Suppose $\mathrm{len}\, M_1 = \mathrm{len}\, M_2$ and for every natural number i such that $i \in \mathrm{dom}\, M_1$ holds $-\infty \notin \mathrm{rng}(M_1(i))$ and for every natural number i such that $i \in \mathrm{dom}\, M_2$ holds $-\infty \notin \mathrm{rng}(M_2(i))$. Then $\mathrm{SumAll}\, M_1 + \mathrm{SumAll}\, M_2 = \mathrm{SumAll}(M_1 \frown M_2)$. The theorem is a consequence of (19), (26), and (20).

Now we state the propositions:

(28) Let us consider a finite sequence p of elements of $\overline{\mathbb{R}}$. Suppose $-\infty \notin \mathrm{rng}\, p$. Then $\mathrm{SumAll}\langle p \rangle = \mathrm{SumAll}\langle p \rangle^{\mathrm{T}}$.

PROOF: Define $x[\text{finite sequence of elements of } \overline{\mathbb{R}}] \equiv$ if $-\infty \notin \mathrm{rng}\, \$_1$, then $\mathrm{SumAll}\langle \$_1 \rangle = \mathrm{SumAll}\langle \$_1 \rangle^{\mathrm{T}}$. For every finite sequence p of elements of $\overline{\mathbb{R}}$ and for every element x of $\overline{\mathbb{R}}$ such that $x[p]$ holds $x[p \frown \langle x \rangle]$ by [5, (31), (38), (6)]. $x[\varepsilon_{\overline{\mathbb{R}}}]$. For every finite sequence p of elements of $\overline{\mathbb{R}}$, $x[p]$ from [12, Sch. 2]. □

(29) Let us consider an extended real number p, and a matrix M over $\overline{\mathbb{R}}$. Suppose for every natural number i such that $i \in \operatorname{dom} M$ holds $p \notin \operatorname{rng}(M(i))$. Let us consider a natural number j. If $j \in \operatorname{dom} M^{\mathrm{T}}$, then $p \notin \operatorname{rng}(M^{\mathrm{T}}(j))$.

(30) Let us consider a matrix M over $\overline{\mathbb{R}}$. Suppose for every natural number i such that $i \in \operatorname{dom} M$ holds $-\infty \notin \operatorname{rng}(M(i))$. Then $\operatorname{SumAll} M = \operatorname{SumAll} M^{\mathrm{T}}$.

Proof: Define x[natural number] $\equiv$ for every matrix M over $\overline{\mathbb{R}}$ such that $\operatorname{len} M = \$_1$ and for every natural number i such that $i \in \operatorname{dom} M$ holds $-\infty \notin \operatorname{rng}(M(i))$ holds $\operatorname{SumAll} M = \operatorname{SumAll} M^{\mathrm{T}}$. For every natural number n such that $x[n]$ holds $x[n+1]$ by [3, (11)], [33, (25)], [5, (40)], (28). $x[0]$. For every natural number n, $x[n]$ from [3, Sch. 2]. □

3. Definition of Pre-Measure

Let x be an object. Let us observe that $\langle x \rangle$ is disjoint valued.

Now we state the proposition:

(31) Let us consider a set X, a semi-diff-closed, $\cap$-closed family S of subsets of X with the empty element, a finite sequence F of elements of S, and an element G of S. Then there exists a disjoint valued finite sequence H of elements of S such that $G \setminus \bigcup F = \bigcup H$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence f of elements of S such that $\operatorname{len} f = \$_1$ there exists a disjoint valued finite sequence H of elements of S such that $G \setminus \bigcup f = \bigcup H$. For every finite sequence f of elements of S such that $\operatorname{len} f = 0$ there exists a disjoint valued finite sequence H of elements of S such that $G \setminus \bigcup f = \bigcup H$ by [16, (2)], [5, (38)], [16, (25)]. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [3, (11)], [5, (59)], [33, (55)], [5, (36), (38)]. For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

Let X be a set and P be a semi-diff-closed, $\cap$-closed family of subsets of X with the empty element. Let us note that there exists a sequence of P which is disjoint valued.

Let P be a non empty family of subsets of X. Note that there exists a function from P into $\overline{\mathbb{R}}$ which is non-negative, additive, and zeroed.

Let P be a family of subsets of X with the empty element. One can check that there exists a function from $\mathbb{N}$ into P which is disjoint valued.

A pre-measure of P is a non-negative, zeroed function from P into $\overline{\mathbb{R}}$ and is defined by

(Def. 7) for every disjoint valued finite sequence F of elements of P such that $\bigcup F \in P$ holds $it(\bigcup F) = \sum(it \cdot F)$ and for every disjoint valued function K from $\mathbb{N}$ into P such that $\bigcup K \in P$ holds $it(\bigcup K) \leqslant \overline{\sum}(it \cdot K)$.

Now we state the propositions:

(32) Let us consider a set X with the empty element, and a finite sequence F of elements of X. Then there exists a function G from $\mathbb{N}$ into X such that

(i) for every natural number i, $F(i) = G(i)$, and

(ii) $\bigcup F = \bigcup G$.

Proof: Define $\mathcal{P}[\text{element of } \mathbb{N}, \text{set}] \equiv$ if $\$_1 \in \operatorname{dom} F$, then $F(\$_1) = \$_2$ and if $\$_1 \notin \operatorname{dom} F$, then $\$_2 = \emptyset$. For every element i of $\mathbb{N}$, there exists an element y of X such that $\mathcal{P}[i, y]$ by [13, (3)]. Consider G being a function from $\mathbb{N}$ into X such that for every element i of $\mathbb{N}$, $\mathcal{P}[i, G(i)]$ from [14, Sch. 3]. $\square$

(33) Let us consider a non empty set X, a finite sequence F of elements of X, and a function G from $\mathbb{N}$ into X. Suppose for every natural number i, $F(i) = G(i)$. Then F is disjoint valued if and only if G is disjoint valued.

(34) Let us consider a finite sequence F of elements of $\overline{\mathbb{R}}$, and a sequence G of extended reals. Suppose for every natural number i, $F(i) = G(i)$. Then F is non-negative if and only if G is non-negative.

Let us observe that there exists a finite sequence of elements of $\overline{\mathbb{R}}$ which is non-negative and there exists a finite sequence of elements of $\overline{\mathbb{R}}$ which is without $-\infty$ and there exists a finite sequence of elements of $\overline{\mathbb{R}}$ which is non-positive and there exists a finite sequence of elements of $\overline{\mathbb{R}}$ which is without $+\infty$ and every finite sequence of elements of $\overline{\mathbb{R}}$ which is non-negative is also without $-\infty$ and every finite sequence of elements of $\overline{\mathbb{R}}$ which is non-positive is also without $+\infty$.

Let X, Y be non empty sets, F be a without $-\infty$ function from Y into $\overline{\mathbb{R}}$, and G be a function from X into Y. One can check that $F \cdot G$ is without $-\infty$ as a function from X into $\overline{\mathbb{R}}$.

Let F be a non-negative function from Y into $\overline{\mathbb{R}}$. One can check that $F \cdot G$ is non-negative as a function from X into $\overline{\mathbb{R}}$.

Now we state the propositions:

(35) Let us consider an extended real number a. Then $\sum\langle a \rangle = a$.

(36) Let us consider a finite sequence F of elements of $\overline{\mathbb{R}}$, and a natural number k. Then

(i) if F is without $-\infty$, then $F \restriction k$ is without $-\infty$, and

(ii) if F is without $+\infty$, then $F \restriction k$ is without $+\infty$.

(37) Let us consider a without $-\infty$ finite sequence F of elements of $\overline{\mathbb{R}}$, and a sequence G of extended reals. Suppose for every natural number i, $F(i) = G(i)$. Let us consider a natural number i. Then $\sum(F{\restriction}i) = (\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}(i)$. The theorem is a consequence of (36) and (35).

(38) Let us consider a without $-\infty$ finite sequence F of elements of $\overline{\mathbb{R}}$, and a sequence G of extended reals. Suppose for every natural number i, $F(i) = G(i)$. Then

(i) G is summable, and

(ii) $\sum F = \sum G$.

Proof: $\sum(F{\restriction}\operatorname{len} F) = (\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}(\operatorname{len} F)$. Define $\mathcal{P}[\text{natural number}] \equiv \sum F = (\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}(\operatorname{len} F + \$_1)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [3, (11), (19)], [33, (25)]. For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 2]. □

(39) Let us consider a set X, a semi-diff-closed, $\cap$-closed family S of subsets of X with the empty element, a disjoint valued finite sequence F of elements of S, and a non empty, preboolean family R of subsets of X. Suppose $S \subseteq R$ and $\bigcup F \in R$. Let us consider a natural number i. Then $\bigcup(F{\restriction}i) \in R$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv \bigcup(F{\restriction}\$_1) \in R$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [3, (12)], [5, (58)], [3, (13)], [5, (82), (17)]. For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

(40) Let us consider a set X, a semi-diff-closed, $\cap$-closed family S of subsets of X with the empty element, a pre-measure P of S, and disjoint valued finite sequences F_1, F_2 of elements of S. Suppose $\bigcup F_1 \in S$ and $\bigcup F_1 = \bigcup F_2$. Then $P(\bigcup F_1) = P(\bigcup F_2)$.

(41) Let us consider a non empty, $\cap$-closed set S, and finite sequences F_1, F_2 of elements of S. Then there exists a matrix M over S of dimension $\operatorname{len} F_1 \times \operatorname{len} F_2$ such that for every natural numbers i, j such that $\langle i, j\rangle \in$ the indices of M holds $M_{i,j} = F_1(i) \cap F_2(j)$.
Proof: Define $\mathcal{P}[\text{natural number}, \text{natural number}, \text{set}] \equiv \$_3 = F_1(\$_1) \cap F_2(\$_2)$. For every natural numbers i, j such that $\langle i, j\rangle \in \operatorname{Seg} \operatorname{len} F_1 \times \operatorname{Seg} \operatorname{len} F_2$ there exists an element K of S such that $\mathcal{P}[i, j, K]$ by [16, (87)], [13, (3)]. Consider M being a matrix over S of dimension $\operatorname{len} F_1 \times \operatorname{len} F_2$ such that for every natural numbers i, j such that $\langle i, j\rangle \in$ the indices of M holds $\mathcal{P}[i, j, M_{i,j}]$. □

Let us consider a set X, a $\cap$-closed family S of subsets of X with the empty element, non empty, disjoint valued finite sequences F_1, F_2 of elements of S, a non-negative, zeroed function P from S into $\overline{\mathbb{R}}$, and a matrix M over $\overline{\mathbb{R}}$ of dimension $\operatorname{len} F_1 \times \operatorname{len} F_2$.

Let us assume that $\bigcup F_1 = \bigcup F_2$ and for every natural numbers i, j such that $\langle i, j\rangle \in$ the indices of M holds $M_{i,j} = P(F_1(i) \cap F_2(j))$ and for every disjoint valued finite sequence F of elements of S such that $\bigcup F \in S$ holds $P(\bigcup F) = \sum(P \cdot F)$. Now we state the propositions:

(42) (i) for every natural number i such that $i \leqslant \mathrm{len}(P \cdot F_1)$ holds $(P \cdot F_1)(i) = (\sum M)(i)$, and

(ii) $\sum(P \cdot F_1) = \mathrm{SumAll}\, M$.

PROOF: Consider K being a matrix over S of dimension $\mathrm{len}\, F_1 \times \mathrm{len}\, F_2$ such that for every natural numbers i, j such that $\langle i, j\rangle \in$ the indices of K holds $K_{i,j} = F_1(i) \cap F_2(j)$. For every natural number i such that $i \leqslant \mathrm{len}(P \cdot F_1)$ holds $(P \cdot F_1)(i) = (\sum M)(i)$ by [33, (24)], [3, (14)], [33, (25)], [13, (11), (3)]. Consider Q being a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$ such that $\sum(P \cdot F_1) = Q(\mathrm{len}(P \cdot F_1))$ and $Q(0) = 0$ and for every natural number i such that $i < \mathrm{len}(P \cdot F_1)$ holds $Q(i+1) = Q(i) + (P \cdot F_1)(i+1)$. Consider L being a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$ such that $\mathrm{SumAll}\, M = L(\mathrm{len} \sum M)$ and $L(0) = 0_{\overline{\mathbb{R}}}$ and for every natural number i such that $i < \mathrm{len} \sum M$ holds $L(i + 1) = L(i) + (\sum M)(i + 1)$. Define $\mathcal{R}$[natural number] $\equiv$ if $\$_1 \leqslant \mathrm{len}(P \cdot F_1)$, then $Q(\$_1) = L(\$_1)$. For every natural number i such that $\mathcal{R}[i]$ holds $\mathcal{R}[i+1]$ by [3, (13)]. For every natural number i, $\mathcal{R}[i]$ from [3, Sch. 2]. □

(43) (i) for every natural number i such that $i \leqslant \mathrm{len}(P \cdot F_2)$ holds $(P \cdot F_2)(i) = (\sum M^{\mathrm{T}})(i)$, and

(ii) $\sum(P \cdot F_2) = \mathrm{SumAll}\, M^{\mathrm{T}}$.

PROOF: Consider K being a matrix over S of dimension $\mathrm{len}\, F_1 \times \mathrm{len}\, F_2$ such that for every natural numbers i, j such that $\langle i, j\rangle \in$ the indices of K holds $K_{i,j} = F_1(i) \cap F_2(j)$. For every natural number i such that $i \leqslant \mathrm{len}(P \cdot F_2)$ holds $(P \cdot F_2)(i) = (\sum M^{\mathrm{T}})(i)$ by [33, (24)], [3, (14)], [33, (25)], [13, (11), (3)]. Consider Q being a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$ such that $\sum(P \cdot F_2) = Q(\mathrm{len}(P \cdot F_2))$ and $Q(0) = 0$ and for every natural number i such that $i < \mathrm{len}(P \cdot F_2)$ holds $Q(i+1) = Q(i) + (P \cdot F_2)(i+1)$. Consider L being a function from $\mathbb{N}$ into $\overline{\mathbb{R}}$ such that $\mathrm{SumAll}\, M^{\mathrm{T}} = L(\mathrm{len} \sum M^{\mathrm{T}})$ and $L(0) = 0_{\overline{\mathbb{R}}}$ and for every natural number i such that $i < \mathrm{len} \sum M^{\mathrm{T}}$ holds $L(i + 1) = L(i) + (\sum M^{\mathrm{T}})(i + 1)$. Define $\mathcal{R}$[natural number] $\equiv$ if $\$_1 \leqslant \mathrm{len}(P \cdot F_2)$, then $Q(\$_1) = L(\$_1)$. For every natural number i such that $\mathcal{R}[i]$ holds $\mathcal{R}[i+1]$ by [3, (13)]. For every natural number i, $\mathcal{R}[i]$ from [3, Sch. 2]. □

(44) Let us consider a set X, a semi-diff-closed, $\cap$-closed family S of subsets of X with the empty element, a pre-measure P of S, and a set A. Suppose $A \in$ the ring generated by S. Let us consider disjoint valued finite sequences F_1,

F_2 of elements of S. If $A = \bigcup F_1$ and $A = \bigcup F_2$, then $\sum(P \cdot F_1) = \sum(P \cdot F_2)$. The theorem is a consequence of (42), (43), and (30).

(45) Let us consider finite sequences f_1, f_2. Suppose f_1 is disjoint valued and f_2 is disjoint valued and $\bigcup \operatorname{rng} f_1$ misses $\bigcup \operatorname{rng} f_2$. Then $f_1 \frown f_2$ is disjoint valued.

(46) Let us consider a set X, a semi-diff-closed family P of subsets of X with the empty element, a pre-measure M of P, and sets A, B. If A, B, $A \setminus B \in P$ and $B \subseteq A$, then $M(A) \geqslant M(B)$. The theorem is a consequence of (45).

(47) Let us consider non empty sets Y, S, a partial function F from Y to S, and a function M from S into $\overline{\mathbb{R}}$. If M is non-negative, then $M \cdot F$ is non-negative.

(48) Let us consider a set X, a semi-diff-closed, $\cap$-closed family S of subsets of X with the empty element, and a pre-measure P of S. Then there exists a non-negative, additive, zeroed function M from the ring generated by S into $\overline{\mathbb{R}}$ such that for every set A such that $A \in$ the ring generated by S for every disjoint valued finite sequence F of elements of S such that $A = \bigcup F$ holds $M(A) = \sum(P \cdot F)$.

Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ for every disjoint valued finite sequence F of elements of S such that $\$_1 = \bigcup F$ holds $\$_2 = \sum(P \cdot F)$. For every object A such that $A \in$ the ring generated by S there exists an object p such that $p \in \overline{\mathbb{R}}$ and $\mathcal{P}[A, p]$ by [23, (18)], (44). Consider M being a function from the ring generated by S into $\overline{\mathbb{R}}$ such that for every object A such that $A \in$ the ring generated by S holds $\mathcal{P}[A, M(A)]$ from [14, Sch. 1]. For every element A of the ring generated by S, $0 \leqslant M(A)$ by [23, (18)], [3, (11)], [33, (25)], [13, (12)]. For every elements A, B of the ring generated by S such that A misses B and $A \cup B \in$ the ring generated by S holds $M(A \cup B) = M(A) + M(B)$ by [23, (18)], (45), [5, (31)], [16, (78)]. □

(49) Let us consider sets X, Y, and functions F, G from $\mathbb{N}$ into 2^X. Suppose for every natural number i, $G(i) = F(i) \cap Y$ and $\bigcup F = Y$. Then $\bigcup G = \bigcup F$.

(50) Let us consider a set X, a semi-diff-closed, $\cap$-closed family S of subsets of X with the empty element, and a pre-measure P of S. Then there exists a function M from the ring generated by S into $\overline{\mathbb{R}}$ such that

(i) $M(\emptyset) = 0$, and

(ii) for every disjoint valued finite sequence K of elements of S such that $\bigcup K \in$ the ring generated by S holds $M(\bigcup K) = \sum(P \cdot K)$.

The theorem is a consequence of (48).

(51) Let us consider sets X, Z, a semi-diff-closed, $\cap$-closed family P of subsets of X with the empty element, and a disjoint valued function K from $\mathbb{N}$ into the ring generated by P. Suppose $Z = \{\langle n, F\rangle$, where n is a natural number, F is a disjoint valued finite sequence of elements of $P : \bigcup F = K(n)$ and if $K(n) = \emptyset$, then $F = \langle\emptyset\rangle\}$. Then

(i) $\pi_2(Z)$ is a set of finite sequences of P, and

(ii) for every object x, $x \in \operatorname{rng} K$ iff there exists a finite sequence F of elements of P such that $F \in \pi_2(Z)$ and $\bigcup F = x$, and

(iii) $\pi_2(Z)$ has non empty elements.

(52) Let us consider a set X, a semi-diff-closed, $\cap$-closed family P of subsets of X with the empty element, and a disjoint valued function K from $\mathbb{N}$ into the ring generated by P. Suppose $\operatorname{rng} K$ has a non-empty element. Then there exists a non empty set Y of finite sequences of P such that

(i) $Y = \{F$, where F is a disjoint valued finite sequence of elements of $P : \bigcup F \in \operatorname{rng} K$ and $F \neq \emptyset\}$, and

(ii) Y has non empty elements.

4. Pre-Measure on Semialgebra and Construction of Measure

Now we state the propositions:

(53) Let us consider sets X, Z, a semialgebra P of sets of X, and a disjoint valued function K from $\mathbb{N}$ into the field generated by P. Suppose $Z = \{\langle n, F\rangle$, where n is a natural number, F is a disjoint valued finite sequence of elements of $P : \bigcup F = K(n)$ and if $K(n) = \emptyset$, then $F = \langle\emptyset\rangle\}$. Then

(i) $\pi_2(Z)$ is a set of finite sequences of P, and

(ii) for every object x, $x \in \operatorname{rng} K$ iff there exists a finite sequence F of elements of P such that $F \in \pi_2(Z)$ and $\bigcup F = x$, and

(iii) $\pi_2(Z)$ has non empty elements.

(54) Let us consider a set X, a semialgebra S of sets of X, a pre-measure P of S, a set A, and disjoint valued finite sequences F_1, F_2 of elements of S. If $A = \bigcup F_1$ and $A = \bigcup F_2$, then $\sum(P \cdot F_1) = \sum(P \cdot F_2)$. The theorem is a consequence of (42), (43), and (30).

(55) Let us consider a set X, a semialgebra S of sets of X, and a pre-measure P of S. Then there exists a measure M on the field generated by S such that for every set A such that $A \in$ the field generated by S for every disjoint valued finite sequence F of elements of S such that $A = \bigcup F$ holds $M(A) = \sum(P \cdot F)$.

PROOF: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ for every disjoint valued finite sequence F of elements of S such that $\$_1 = \bigcup F$ holds $\$_2 = \sum(P \cdot F)$. For every object A such that $A \in$ the field generated by S there exists an object p such that $p \in \overline{\mathbb{R}}$ and $\mathcal{P}[A, p]$ by [23, (22)], (54). Consider M being a function from the field generated by S into $\overline{\mathbb{R}}$ such that for every object A such that $A \in$ the field generated by S holds $\mathcal{P}[A, M(A)]$ from [14, Sch. 1]. For every element A of the field generated by S, $0 \leqslant M(A)$ by [23, (22)], [3, (11)], [33, (25)], [13, (12)]. For every elements A, B of the field generated by S such that A misses B holds $M(A \cup B) = M(A) + M(B)$ by [23, (22)], (45), [5, (31)], [16, (78)]. □

(56) Let us consider a sequence F of extended reals, a natural number n, and an extended real number a. Suppose for every natural number k, $F(k) = a$. Then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(n) = a \cdot (n+1)$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(\$_1) = a \cdot (\$_1 + 1)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. □

(57) Let us consider a non empty set X, a sequence F of X, and a natural number n. Then $\text{rng}(F \restriction \mathbb{Z}_{n+1}) = \text{rng}(F \restriction \mathbb{Z}_n) \cup \{F(n)\}$.

(58) Let us consider a set X, a field S of subsets of X, a measure M on S, a sequence F of separated subsets of S, and a natural number n. Then

(i) $\bigcup \text{rng}(F \restriction \mathbb{Z}_{n+1}) \in S$, and

(ii) $(\sum_{\alpha=0}^{\kappa} (M \cdot F)(\alpha))_{\kappa \in \mathbb{N}}(n) = M(\bigcup \text{rng}(F \restriction \mathbb{Z}_{n+1}))$.

PROOF: $\text{rng}(F \restriction \mathbb{Z}_{0+1}) = \text{rng}(F \restriction \mathbb{Z}_0) \cup \{F(0)\}$. Define $\mathcal{R}[\text{natural number}] \equiv \bigcup \text{rng}(F \restriction \mathbb{Z}_{\$_1+1}) \in S$. For every natural number k such that $\mathcal{R}[k]$ holds $\mathcal{R}[k+1]$ by (57), [16, (78), (25)], [27, (3)]. For every natural number k, $\mathcal{R}[k]$ from [3, Sch. 2]. Define $\mathcal{P}[\text{natural number}] \equiv (\sum_{\alpha=0}^{\kappa} (M \cdot F)(\alpha))_{\kappa \in \mathbb{N}}(\$_1) = M(\bigcup \text{rng}(F \restriction \mathbb{Z}_{\$_1+1}))$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [14, (15)], [35, (57)], [3, (44)], [13, (47)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(59) Let us consider a set X, a semialgebra S of sets of X, a pre-measure P of S, and a measure M on the field generated by S. Suppose for every set A such that $A \in$ the field generated by S for every disjoint valued finite sequence F of elements of S such that $A = \bigcup F$ holds $M(A) = \sum(P \cdot F)$. Then M is completely-additive. The theorem is a consequence of (53), (15), (13), (58), and (1).

Let X be a set, S be a semialgebra of sets of X, and P be a pre-measure of S.

An induced measure of S and P is a measure on the field generated by S and is defined by

(Def. 8) for every set A such that $A \in$ the field generated by S for every disjoint valued finite sequence F of elements of S such that $A = \bigcup F$ holds $it(A) = \sum(P \cdot F)$.

Now we state the propositions:

(60) Let us consider a set X, a semialgebra S of sets of X, and a pre-measure P of S. Then every induced measure of S and P is completely-additive. The theorem is a consequence of (59).

(61) Let us consider a non empty set X, a semialgebra S of sets of X, a pre-measure P of S, and an induced measure M of S and P. Then σ-Meas(the Caratheodory measure determined by M)$\restriction\sigma$(the field generated by S) is a σ-measure on σ(the field generated by S). The theorem is a consequence of (60).

Let X be a non empty set, S be a semialgebra of sets of X, P be a pre-measure of S, and M be an induced measure of S and P.

An induced σ-measure of S and M is a σ-measure on σ(the field generated by S) and is defined by

(Def. 9) $it = \sigma$-Meas(the Caratheodory measure determined by M)$\restriction\sigma$(the field generated by S).

Now we state the proposition:

(62) Let us consider a non empty set X, a semialgebra S of sets of X, a pre-measure P of S, and an induced measure m of S and P. Then every induced σ-measure of S and m is an extension of m. The theorem is a consequence of (60).

References

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

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

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

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

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

[6] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

[7] Józef Białas. Properties of Caratheodor's measure. *Formalized Mathematics*, 3(**1**):67–70, 1992.

[8] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):163–171, 1991.

[9] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.

[10] V.I. Bogachev. *Measure Theory*, volume 1. Springer, 2006.

[11] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

[12] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[13] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[14] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[15] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[16] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[17] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[18] Noboru Endou and Yasunari Shidama. Integral of measurable function. *Formalized Mathematics*, 14(**2**):53–70, 2006. doi:10.2478/v10037-006-0008-x.
[19] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Basic properties of extended real numbers. *Formalized Mathematics*, 9(**3**):491–494, 2001.
[20] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.
[21] Noboru Endou, Keiko Narita, and Yasunari Shidama. The Lebesgue monotone convergence theorem. *Formalized Mathematics*, 16(**2**):167–175, 2008. doi:10.2478/v10037-008-0023-1.
[22] Noboru Endou, Hiroyuki Okazaki, and Yasunari Shidama. Hopf extension theorem of measure. *Formalized Mathematics*, 17(**2**):157–162, 2009. doi:10.2478/v10037-009-0018-6.
[23] Noboru Endou, Kazuhisa Nakasho, and Yasunari Shidama. σ-ring and σ-algebra of sets. *Formalized Mathematics*, 23(**1**):51–57, 2015. doi:10.2478/forma-2015-0004.
[24] P. R. Halmos. *Measure Theory*. Springer-Verlag, 1974.
[25] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**): 573–577, 1997.
[26] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(**3**):339–345, 1996.
[27] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.
[28] Andrzej Nędzusiak. Probability. *Formalized Mathematics*, 1(**4**):745–749, 1990.
[29] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[30] Konrad Raczkowski and Andrzej Nędzusiak. Series. *Formalized Mathematics*, 2(**4**):449–452, 1991.
[31] M.M. Rao. *Measure Theory and Integration*. CRC Press, 2nd edition, 2004.
[32] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1 (**1**):187–190, 1990.
[33] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
[34] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[35] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[36] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received August 14, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 325–331, 2015
DOI: 10.1515/forma-2015-0026

DE GRUYTER
OPEN
degruyter.com/view/j/forma

Event-Based Proof of the Mutual Exclusion Property of Peterson's Algorithm

Ievgen Ivanov
Taras Shevchenko National University
Kyiv, Ukraine

Mykola Nikitchenko
Taras Shevchenko National University
Kyiv, Ukraine

Uri Abraham
Ben-Gurion University
Beer-Sheva, Israel

Summary. Proving properties of distributed algorithms is still a highly challenging problem and various approaches that have been proposed to tackle it [1] can be roughly divided into state-based and event-based proofs. Informally speaking, state-based approaches define the behavior of a distributed algorithm as a set of sequences of memory states during its executions, while event-based approaches treat the behaviors by means of events which are produced by the executions of an algorithm. Of course, combined approaches are also possible.

Analysis of the literature [1], [7], [12], [9], [13], [14], [15] shows that state-based approaches are more widely used than event-based approaches for proving properties of algorithms, and the difficulties in the event-based approach are often emphasized. We believe, however, that there is a certain naturalness and intuitive content in event-based proofs of correctness of distributed algorithms that makes this approach worthwhile. Besides, state-based proofs of correctness of distributed algorithms are usually applicable only to discrete-time models of distributed systems and cannot be easily adapted to the continuous time case which is important in the domain of cyber-physical systems. On the other hand, event-based proofs can be readily applied to continuous-time / hybrid models of distributed systems.

In the paper [2] we presented a compositional approach to reasoning about behavior of distributed systems in terms of events. Compositionality here means (informally) that semantics and properties of a program is determined by semantics of processes and process communication mechanisms. We demonstrated the proposed approach on a proof of the mutual exclusion property of the Peterson's algorithm [11]. We have also demonstrated an application of this approach for

ISSN 1426–2630(Print), 1898-9934(Online)

proving the mutual exclusion property in the setting of continuous-time models of cyber-physical systems in [8].

Using Mizar [3], in this paper we give a formal proof of the mutual exclusion property of the Peterson's algorithm in Mizar on the basis of the event-based approach proposed in [2]. Firstly, we define an event-based model of a shared-memory distributed system as a multi-sorted algebraic structure in which sorts are events, processes, locations (i.e. addresses in the shared memory), traces (of the system). The operations of this structure include a binary precedence relation $\leqslant$ on the set of events which turns it into a linear preorder (events are considered simultaneous, if $e_1 \leqslant e_2$ and $e_2 \leqslant e_1$), special predicates which check if an event occurs in a given process or trace, predicates which check if an event causes the system to read from or write to a given memory location, and a special partial function "`val of`" on events which gives the value associated with a memory read or write event (i.e. a value which is written or is read in this event) [2]. Then we define several natural consistency requirements (axioms) for this structure which must hold in every distributed system, e.g. each event occurs in some process, etc. (details are given in [2]).

After this we formulate and prove the main theorem about the mutual exclusion property of the Peterson's algorithm in an arbitrary consistent algebraic structure of events. Informally, the main theorem states that if a system consists of two processes, and in some trace there occur two events e_1 and e_2 in different processes and each of these events is preceded by a series of three special events (in the same process) guaranteed by execution of the Peterson's algorithm (setting the flag of the current process, writing the identifier of the opposite process to the "turn" shared variable, and reading zero from the flag of the opposite process or reading the identifier of the current process from the "turn" variable), and moreover, if neither process writes to the flag of the opposite process or writes its own identifier to the "turn" variable, then either the events e_1 and e_2 coincide, or they are not simultaneous (mutual exclusion property).

MSC: 68M14 68W15 68N30 03B35

Keywords: distributed system; parallel computing; algorithm; verification; mathematical model

MML identifier: `PETERSON`, version: `8.1.04 5.33.1254`

The notation and terminology used in this paper have been introduced in the following articles: [4], [5], [16], [18], [19], [10], [17], and [6].

1. Preliminaries

We consider values⟨true, false⟩ which extend 1-sorted structures and are systems

$$\langle \text{a carrier}, \text{a true}, \text{a false} \rangle$$

where the carrier is a set, the true is an element of the carrier, the false is an element of the carrier.

Let A be a value⟨true, false⟩. We say that A is consistent if and only if

(Def. 1) the true of $A \neq$ the false of A.

Let us observe that there exists a value⟨true, false⟩ which is consistent.

A value with bool is a consistent value⟨true, false⟩. Let A be a relational structure. We say that A is strongly connected if and only if

(Def. 2) the internal relation of A is strongly connected in the carrier of A.

Let us observe that there exists a relational structure which is non empty, reflexive, transitive, and strongly connected.

A linear preorder is a reflexive, transitive, strongly connected relational structure. Let V be a value with bool. We consider events structures over V and are systems

$$\langle \text{events}, \text{processes}, \text{locations}, \text{traces},$$
$$\text{a proc-E}, \text{a trace-E}, \text{a read-E}, \text{a write-E}, \text{a val} \rangle$$

where the events constitute a non empty linear preorder, the processes constitute a non empty set, the locations constitute a non empty set, the traces constitute a non empty set, the proc-E is a function from the processes into $2^{(\text{the carrier of the events})}$, the trace-E is a function from the traces into $2^{(\text{the carrier of the events})}$, the read-E is a function from the locations into $2^{(\text{the carrier of the events})}$, the write-E is a function from the locations into $2^{(\text{the carrier of the events})}$, the val is a partial function from the carrier of the events to the carrier of V.

Let S be an events structure over V.

A process of S is an element of the processes of S.

An event of S is an element of the carrier of the events of S.

An event set of S is a subset of the carrier of the events of S.

A location of S is an element of the locations of S.

A trace of S is an element of the traces of S. From now on V denotes a value with bool, a, a_1, a_2 denote elements of the carrier of V, S denotes an events structure over V, p, p_1, p_2 denote processes of S, x, x_1, x_2 denote locations of S, t denotes traces of S, e, e_0, e_1, e_2, e_3 denote events of S, and E denotes an event set of S.

Let us consider V, S, e, and x. We say that e reads x if and only if

(Def. 3) $e \in$ (the read-E of S)(x).

We say that e writes to x if and only if

(Def. 4) $e \in$ (the write-E of S)(x).

Let us consider E. We say that E reads x if and only if

(Def. 5) there exists e such that $e \in E$ and e reads x.

We say that E writes to x if and only if

(Def. 6) there exists e such that $e \in E$ and e writes to x.

Let us consider e and t. We say that $e \in t$ if and only if

(Def. 7) $e \in$ (the trace-E of S)(t).

Let us consider p. We say that $e \in p$ if and only if

(Def. 8) $e \in$ (the proc-E of S)(p).

The value associated with event e is defined by the term

(Def. 9) (the val of S)(e).

Let us consider p and t. We say that $e \in p, t$ if and only if

(Def. 10) $e \in p$ and $e \in t$.

Let us consider x and a. We say that e writes to x the value a if and only if

(Def. 11) e writes to x and the value associated with event $e = a$.

We say that e reads from x the value a if and only if

(Def. 12) e reads x and the value associated with event $e = a$.

We say that S is process-complete if and only if

(Def. 13) for every t and e such that $e \in t$ there exists p such that $e \in p$.

We say that S is process-ordered if and only if

(Def. 14) for every p, e_1, and e_2 such that e_1, $e_2 \in p$ holds if $e_1 \leqslant e_2 \leqslant e_1$, then $e_1 = e_2$.

We say that S is rw-ordered if and only if

(Def. 15) for every x, e_1, and e_2 such that (e_1 reads x or e_1 writes to x) and (e_2 reads x or e_2 writes to x) holds if $e_1 \leqslant e_2 \leqslant e_1$, then $e_1 = e_2$.

We say that S is rw-consistent if and only if

(Def. 16) for every t, x, e, and a such that $e \in t$ and e reads x and the value associated with event $e = a$ there exists e_0 such that $e_0 \in t$ and $e_0 < e$ and e_0 writes to x and the value associated with event $e_0 = a$ and for every e_1 such that $e_1 \in t$ and $e_1 \leqslant e$ and e_1 writes to x holds $e_1 \leqslant e_0$.

We say that S is rw-exclusive if and only if

(Def. 17) for every e, x_1, and x_2, it is not true that e reads x_1 and e writes to x_2.

We say that S is consistent if and only if

(Def. 18) S is process-complete, process-ordered, rw-ordered, rw-consistent, and rw-exclusive.

One can check that there exists an events structure over V which is consistent.

A distributed system with shared memory over a set of values V is a consistent events structure over V.

2. Peterson's Algorithm

From now on D denotes a distributed system with shared memory over a set of values V, p, p_1, p_2 denote processes of D, x, x_1, x_2, f_1, f_2, t_1 denote locations of D, t denotes traces of D, e, e_0, e_1, e_2, e_3 denote events of D, and E denotes an event set of D.

Let us consider V, D, e_1, and e_2. We say that $e_1 \ll e_2$ if and only if

(Def. 19) $e_1 \leqslant e_2$ and $e_2 \nleqslant e_1$.

The interval (e_1, e_2) yielding an event set of D is defined by the term

(Def. 20) $\{e : e_1 < e < e_2\}$.

Let us consider p and t. The (e_1, e_2) interval in (p, t) yielding an event set of D is defined by the term

(Def. 21) $\{e : e_1 < e < e_2$ and $e \in p, t\}$.

Now we state the propositions:

(1) The (e_1, e_2) interval in $(p, t) \subseteq$ the interval (e_1, e_2).

(2) (i) $e_1 \leqslant e_2$, or

(ii) $e_2 \leqslant e_1$.

(3) Suppose $e \in p, t$ and $e_1 < e < e_2$. Then $e \in$ the (e_1, e_2) interval in (p, t).

(4) If $e_1 < e_2$, then $e_1 \leqslant e_2$.

(5) If e_1, $e_2 \in p$ and $e_1 < e_2$, then $e_1 \ll e_2$.

(6) If $e_1 \in p, t$ and $e_2 \in p, t$ and $e_1 < e_2$, then $e_1 \ll e_2$.

(7) If $e_1 \ll e_2$, then $e_1 < e_2$.

(8) If e_1, $e_2 \in p$, then $e_1 = e_2$ or $e_1 \ll e_2$ or $e_2 \ll e_1$.

(9) If $e_1 \leqslant e_2 \leqslant e_3$, then $e_1 \leqslant e_3$.

(10) If $e_1 \leqslant e_2 \ll e_3$, then $e_1 \ll e_3$.

(11) If $e_1 \ll e_2 \leqslant e_3$, then $e_1 \ll e_3$.

(12) If $e_1 \ll e_2 \ll e_3$, then $e_1 \ll e_3$.

Let us consider V, D, e_1, and e_2. We say that e_1 and e_2 are simultaneous events if and only if

(Def. 22) $e_1 \leqslant e_2 \leqslant e_1$.

Now we state the proposition:

(13) If e_1 and e_2 are not simultaneous events, then $e_1 \ll e_2$ or $e_2 \ll e_1$.

Let us consider V, D, p, t, e, x_1, x_2, t_1, a_1, and a_2. We say that e is a Peterson critical section with respect to p, x_1, x_2, t_1, a_1, a_2 and t if and only if

(Def. 23) there exists e_1 and there exists e_2 and there exists e_3 such that $e_1 \in p, t$ and $e_2 \in p, t$ and $e_3 \in p, t$ and $e_1 < e_2 < e_3 < e$ and e_1 writes to x_1 the value the true of V and the (e_1, e) interval in (p, t) does not write to x_1 and e_2 writes to t_1 the value a_2 and the (e_2, e) interval in (p, t) does not write to t_1 and (e_3 reads from x_2 the value the false of V or e_3 reads from t_1 the value a_1).

Let E_1 be a set. We say that E_1 are Peterson critical sections in t if and only if

(Def. 24) there exists p_1 and there exists p_2 such that for every process p of D, $p = p_1$ or $p = p_2$ and there exists f_1 and there exists f_2 and there exists t_1 such that for every e such that $e \in p_1, t$ holds e does not write to f_2 and e does not write to t_1 the value the false of V and for every e such that $e \in p_2, t$ holds e does not write to f_1 and e does not write to t_1 the value the true of V and for every e such that $e \in E_1$ holds e is a Peterson critical section with respect to p_1, f_1, f_2, t_1, the false of V, the true of V and t and e is a Peterson critical section with respect to p_2, f_2, f_1, t_1, the true of V, the false of V and t.

Now we state the propositions:

(14) Suppose $e_1, e_2 \in t$ and e_1 reads from x the value a_1 and e_2 reads from x the value a_2 and $e_1 \leqslant e_2$ and $a_1 \neq a_2$. Then there exists e such that

(i) $e \in t$, and

(ii) $e_1 \ll e \ll e_2$, and

(iii) e writes to x the value a_2.

The theorem is a consequence of (9) and (2).

(15) Main result: Mutual exclusion property of Peterson's algorithm:

If e_1, $e_2 \in t$ and $\{e_1, e_2\}$ are Peterson critical sections in t, then $e_1 = e_2$ or $e_1 \ll e_2$ or $e_2 \ll e_1$. The theorem is a consequence of (2), (5), (9), (11), (10), and (14).

References

[1] Uri Abraham. *Models for Concurrency.* Gordon and Breach, 1999.

[2] Uri Abraham, Ievgen Ivanov, and Mykola Nikitchenko. Proving behavioral properties of distributed algorithms using their compositional semantics. In *Proceedings of the First International Seminar Specification and Verification of Hybrid Systems, October 10-12, 2011, Taras Shevchenko National University of Kyiv*, pages 9–19, 2011.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

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

[7] K. Chandy and J. Misra. *Parallel Program Design: A Foundation.* Addison Wesley, 1988.

[8] Ievgen Ivanov, Mykola Nikitchenko, and Uri Abraham. On a decidable formal theory for abstract continuous-time dynamical systems. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications*, volume 469 of *Communications in Computer and Information Science*, pages 78–99. Springer International Publishing, 2014. ISBN 978-3-319-13205-1. doi:10.1007/978-3-319-13206-8_4.

[9] L. Lamport. On interprocess communication. Part I: Basic formalism; Part II: Algorithms. *Distributed Computing*, 1:77–101, 1986.

[10] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[11] G. Peterson. Myths about the mutual exclusion problem. *Information Processing Letters*, 12:1133–1145, 1981.

[12] V. Pratt. Modeling concurrency with partial orders. *International Journal of Parallel Programming*, 15:33–71, 1986.

[13] M. Raynal. A simple taxonomy for distributed mutual exclusion algorithms. *ACM SIGOPS Operating Systems Review*, 25:47–50, 1991.

[14] Tom Ridge. Peterson's algorithm in Isabelle/HOL. `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.99.3484`, 2006.

[15] Tom Ridge. Operational reasoning for concurrent Caml programs and weak memory models. In Klaus Schneider and Jens Brandt, editors, *Theorem Proving in Higher Order Logics*, volume 4732 of *Lecture Notes in Computer Science*, pages 278–293. Springer Berlin Heidelberg, 2007. ISBN 978-3-540-74590-7. doi:10.1007/978-3-540-74591-4_21.

[16] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski – Zorn lemma. *Formalized Mathematics*, 1(**2**):387–393, 1990.

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

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

[19] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received August 14, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 333–349, 2015
DOI: 10.1515/forma-2015-0027

DE GRUYTER OPEN
degruyter.com/view/j/forma

Characteristic of Rings. Prime Fields

Christoph Schwarzweller
Institute of Computer Science
University of Gdańsk
Poland

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Summary. The notion of the characteristic of rings and its basic properties are formalized [14], [39], [20]. Classification of prime fields in terms of isomorphisms with appropriate fields ($\mathbb{Q}$ or $\mathbb{Z}/p$) are presented. To facilitate reasonings within the field of rational numbers, values of numerators and denominators of basic operations over rationals are computed.

MSC: 13A35 12E05 03B35

Keywords: commutative algebra; characteristic of rings; prime field

MML identifier: RING_3, version: 8.1.04 5.34.1256

The notation and terminology used in this paper have been introduced in the following articles: [25], [27], [6], [31], [2], [21], [32], [12], [11], [7], [8], [13], [28], [35], [37], [1], [34], [19], [29], [26], [33], [22], [3], [4], [9], [30], [15], [5], [40], [23], [16], [36], [38], [17], [18], [24], and [10].

1. Preliminaries

Now we state the propositions:

(1) Let us consider a function f, a set A, and objects a, b. If $a, b \in A$, then $(f \restriction A)(a, b) = f(a, b)$.

(2) $+_{\mathbb{C}} \restriction \mathbb{R} = +_{\mathbb{R}}$.

PROOF: Set $c = +_{\mathbb{C}} \restriction \mathbb{R}$. For every object z such that $z \in \operatorname{dom} c$ holds $c(z) = +_{\mathbb{R}}(z)$ by [7, (49)]. □

(3) $\cdot_{\mathbb{C}} \restriction \mathbb{R} = \cdot_{\mathbb{R}}$.

PROOF: Set $d = \cdot_{\mathbb{C}} \restriction \mathbb{R}$. For every object z such that $z \in \operatorname{dom} d$ holds $d(z) = \cdot_{\mathbb{R}}(z)$ by [7, (49)]. □

ISSN 1426–2630(Print), 1898-9934(Online)

(4) $+_{\mathbb{Q}} \restriction \mathbb{Z} = +_{\mathbb{Z}}$.
PROOF: Set $c = +_{\mathbb{Q}} \restriction \mathbb{Z}$. For every object z such that $z \in \operatorname{dom} c$ holds $c(z) = (+_{\mathbb{Z}})(z)$ by [7, (49)]. □

(5) $\cdot_{\mathbb{Q}} \restriction \mathbb{Z} = \cdot_{\mathbb{Z}}$.
PROOF: Set $d = \cdot_{\mathbb{Q}} \restriction \mathbb{Z}$. For every object z such that $z \in \operatorname{dom} d$ holds $d(z) = \cdot_{\mathbb{Z}}(z)$ by [7, (49)]. □

2. Properties of Fractions

From now on p, q denote rational numbers, g, m, m_1, m_2, n, n_1, n_2 denote natural numbers, and i, j denote integers.

Now we state the propositions:

(6) If $n \mid i$, then $i \operatorname{div} n = \frac{i}{n}$.

(7) $i \operatorname{div}(\gcd(i,n)) = \frac{i}{\gcd(i,n)}$. The theorem is a consequence of (6).

(8) $n \operatorname{div}(\gcd(n,i)) = \frac{n}{\gcd(n,i)}$. The theorem is a consequence of (6).

(9) If $g \mid i$ and $g \mid m$, then $\frac{i}{m} = \frac{i \operatorname{div} g}{m \operatorname{div} g}$.

(10) $\frac{i}{m} = \frac{i \operatorname{div}(\gcd(i,m))}{m \operatorname{div}(\gcd(i,m))}$. The theorem is a consequence of (9).

(11) If $0 < m$ and $m \cdot i \mid m$, then $i = 1$ or $i = -1$.

(12) If $0 < m$ and $m \cdot n \mid m$, then $n = 1$.

(13) If $m \mid i$, then $i \operatorname{div} m \mid i$. The theorem is a consequence of (6).

Let us assume that $m \neq 0$. Now we state the propositions:

(14) $\gcd(i \operatorname{div}(\gcd(i,m)), m \operatorname{div}(\gcd(i,m))) = 1$. The theorem is a consequence of (6) and (11).

(15) (i) $\operatorname{den}(\frac{i}{m}) = m \operatorname{div}(\gcd(i,m))$, and
(ii) $\operatorname{num}(\frac{i}{m}) = i \operatorname{div}(\gcd(i,m))$.
The theorem is a consequence of (10) and (14).

(16) (i) $\operatorname{den}(\frac{i}{m}) = \frac{m}{\gcd(i,m)}$, and
(ii) $\operatorname{num}(\frac{i}{m}) = \frac{i}{\gcd(i,m)}$.
The theorem is a consequence of (15), (8), and (7).

(17) (i) $\operatorname{den}(-(\frac{i}{m})) = m \operatorname{div}(\gcd(-i,m))$, and
(ii) $\operatorname{num}(-(\frac{i}{m})) = -i \operatorname{div}(\gcd(-i,m))$.
The theorem is a consequence of (15).

(18) (i) $\operatorname{den}(-(\frac{i}{m})) = \frac{m}{\gcd(-i,m)}$, and
(ii) $\operatorname{num}(-(\frac{i}{m})) = \frac{-i}{\gcd(-i,m)}$.
The theorem is a consequence of (17), (8), and (7).

(19) (i) $\mathrm{den}(\frac{m}{i})^{-1} = m\,\mathrm{div}(\mathrm{gcd}(m,i))$, and

(ii) $\mathrm{num}(\frac{m}{i})^{-1} = i\,\mathrm{div}(\mathrm{gcd}(m,i))$.

The theorem is a consequence of (15).

(20) (i) $\mathrm{den}(\frac{m}{i})^{-1} = \frac{m}{\mathrm{gcd}(m,i)}$, and

(ii) $\mathrm{num}(\frac{m}{i})^{-1} = \frac{i}{\mathrm{gcd}(m,i)}$.

The theorem is a consequence of (19), (8), and (7).

Let us assume that $m \neq 0$ and $n \neq 0$. Now we state the propositions:

(21) (i) $\mathrm{den}((\frac{i}{m}) + (\frac{j}{n})) = m \cdot n\,\mathrm{div}(\mathrm{gcd}(i \cdot n + j \cdot m, m \cdot n))$, and

(ii) $\mathrm{num}((\frac{i}{m}) + (\frac{j}{n})) = i \cdot n + j \cdot m\,\mathrm{div}(\mathrm{gcd}(i \cdot n + j \cdot m, m \cdot n))$.

The theorem is a consequence of (15).

(22) (i) $\mathrm{den}((\frac{i}{m}) + (\frac{j}{n})) = \frac{m \cdot n}{\mathrm{gcd}(i \cdot n + j \cdot m, m \cdot n)}$, and

(ii) $\mathrm{num}((\frac{i}{m}) + (\frac{j}{n})) = \frac{i \cdot n + j \cdot m}{\mathrm{gcd}(i \cdot n + j \cdot m, m \cdot n)}$.

The theorem is a consequence of (21), (8), and (7).

(23) (i) $\mathrm{den}((\frac{i}{m}) - (\frac{j}{n})) = m \cdot n\,\mathrm{div}(\mathrm{gcd}(i \cdot n - j \cdot m, m \cdot n))$, and

(ii) $\mathrm{num}((\frac{i}{m}) - (\frac{j}{n})) = i \cdot n - j \cdot m\,\mathrm{div}(\mathrm{gcd}(i \cdot n - j \cdot m, m \cdot n))$.

The theorem is a consequence of (15).

(24) (i) $\mathrm{den}((\frac{i}{m}) - (\frac{j}{n})) = \frac{m \cdot n}{\mathrm{gcd}(i \cdot n - j \cdot m, m \cdot n)}$, and

(ii) $\mathrm{num}((\frac{i}{m}) - (\frac{j}{n})) = \frac{i \cdot n - j \cdot m}{\mathrm{gcd}(i \cdot n - j \cdot m, m \cdot n)}$.

The theorem is a consequence of (23), (8), and (7).

(25) (i) $\mathrm{den}((\frac{i}{m}) \cdot (\frac{j}{n})) = m \cdot n\,\mathrm{div}(\mathrm{gcd}(i \cdot j, m \cdot n))$, and

(ii) $\mathrm{num}((\frac{i}{m}) \cdot (\frac{j}{n})) = i \cdot j\,\mathrm{div}(\mathrm{gcd}(i \cdot j, m \cdot n))$.

The theorem is a consequence of (15).

(26) (i) $\mathrm{den}((\frac{i}{m}) \cdot (\frac{j}{n})) = \frac{m \cdot n}{\mathrm{gcd}(i \cdot j, m \cdot n)}$, and

(ii) $\mathrm{num}((\frac{i}{m}) \cdot (\frac{j}{n})) = \frac{i \cdot j}{\mathrm{gcd}(i \cdot j, m \cdot n)}$.

The theorem is a consequence of (25), (8), and (7).

(27) (i) $\mathrm{den}(\frac{(\frac{i}{m})}{(\frac{n}{j})}) = m \cdot n\,\mathrm{div}(\mathrm{gcd}(i \cdot j, m \cdot n))$, and

(ii) $\mathrm{num}(\frac{(\frac{i}{m})}{(\frac{n}{j})}) = i \cdot j\,\mathrm{div}(\mathrm{gcd}(i \cdot j, m \cdot n))$.

The theorem is a consequence of (15).

(28) (i) $\mathrm{den}(\frac{(\frac{i}{m})}{(\frac{n}{j})}) = \frac{m \cdot n}{\mathrm{gcd}(i \cdot j, m \cdot n)}$, and

(ii) $\mathrm{num}(\frac{(\frac{i}{m})}{(\frac{n}{j})}) = \frac{i \cdot j}{\mathrm{gcd}(i \cdot j, m \cdot n)}$.

The theorem is a consequence of (27), (8), and (7).

Now we state the propositions:

(29) $\operatorname{den} p = \operatorname{den} p \operatorname{div}(\gcd(\operatorname{num} p, \operatorname{den} p))$. The theorem is a consequence of (15).

(30) $\operatorname{num} p = \operatorname{num} p \operatorname{div}(\gcd(\operatorname{num} p, \operatorname{den} p))$. The theorem is a consequence of (15).

Let us assume that $m = \operatorname{den} p$ and $i = \operatorname{num} p$. Now we state the propositions:

(31) (i) $\operatorname{den}(-p) = m \operatorname{div}(\gcd(-i, m))$, and

(ii) $\operatorname{num}(-p) = -i \operatorname{div}(\gcd(-i, m))$.

The theorem is a consequence of (17).

(32) (i) $\operatorname{den}(-p) = \frac{m}{\gcd(-i,m)}$, and

(ii) $\operatorname{num}(-p) = \frac{-i}{\gcd(-i,m)}$.

The theorem is a consequence of (31), (8), and (7).

Let us assume that $m = \operatorname{den} p$ and $n = \operatorname{num} p$ and $n \neq 0$. Now we state the propositions:

(33) (i) $\operatorname{den} p^{-1} = n \operatorname{div}(\gcd(n, m))$, and

(ii) $\operatorname{num} p^{-1} = m \operatorname{div}(\gcd(n, m))$.

The theorem is a consequence of (19).

(34) (i) $\operatorname{den} p^{-1} = \frac{n}{\gcd(n,m)}$, and

(ii) $\operatorname{num} p^{-1} = \frac{m}{\gcd(n,m)}$.

The theorem is a consequence of (33), (8), and (7).

Let us assume that $m = \operatorname{den} p$ and $n = \operatorname{den} q$ and $i = \operatorname{num} p$ and $j = \operatorname{num} q$. Now we state the propositions:

(35) (i) $\operatorname{den}(p + q) = m \cdot n \operatorname{div}(\gcd(i \cdot n + j \cdot m, m \cdot n))$, and

(ii) $\operatorname{num}(p + q) = i \cdot n + j \cdot m \operatorname{div}(\gcd(i \cdot n + j \cdot m, m \cdot n))$.

The theorem is a consequence of (21).

(36) (i) $\operatorname{den}(p + q) = \frac{m \cdot n}{\gcd(i \cdot n + j \cdot m, m \cdot n)}$, and

(ii) $\operatorname{num}(p + q) = \frac{i \cdot n + j \cdot m}{\gcd(i \cdot n + j \cdot m, m \cdot n)}$.

The theorem is a consequence of (35), (8), and (7).

(37) (i) $\operatorname{den}(p - q) = m \cdot n \operatorname{div}(\gcd(i \cdot n - j \cdot m, m \cdot n))$, and

(ii) $\operatorname{num}(p - q) = i \cdot n - j \cdot m \operatorname{div}(\gcd(i \cdot n - j \cdot m, m \cdot n))$.

The theorem is a consequence of (23).

(38) (i) $\operatorname{den}(p - q) = \frac{m \cdot n}{\gcd(i \cdot n - j \cdot m, m \cdot n)}$, and

(ii) $\operatorname{num}(p - q) = \frac{i \cdot n - j \cdot m}{\gcd(i \cdot n - j \cdot m, m \cdot n)}$.

The theorem is a consequence of (37), (8), and (7).

(39) (i) $\operatorname{den}(p \cdot q) = m \cdot n \operatorname{div}(\gcd(i \cdot j, m \cdot n))$, and

(ii) $\mathrm{num}(p \cdot q) = i \cdot j \,\mathrm{div}(\gcd(i \cdot j, m \cdot n))$.

The theorem is a consequence of (25).

(40) (i) $\mathrm{den}(p \cdot q) = \frac{m \cdot n}{\gcd(i \cdot j, m \cdot n)}$, and

(ii) $\mathrm{num}(p \cdot q) = \frac{i \cdot j}{\gcd(i \cdot j, m \cdot n)}$.

The theorem is a consequence of (39), (8), and (7).

Let us assume that $m_1 = \mathrm{den}\, p$ and $m_2 = \mathrm{den}\, q$ and $n_1 = \mathrm{num}\, p$ and $n_2 = \mathrm{num}\, q$ and $n_2 \neq 0$. Now we state the propositions:

(41) (i) $\mathrm{den}(\frac{p}{q}) = m_1 \cdot n_2 \,\mathrm{div}(\gcd(n_1 \cdot m_2, m_1 \cdot n_2))$, and

(ii) $\mathrm{num}(\frac{p}{q}) = n_1 \cdot m_2 \,\mathrm{div}(\gcd(n_1 \cdot m_2, m_1 \cdot n_2))$.

The theorem is a consequence of (27).

(42) (i) $\mathrm{den}(\frac{p}{q}) = \frac{m_1 \cdot n_2}{\gcd(n_1 \cdot m_2, m_1 \cdot n_2)}$, and

(ii) $\mathrm{num}(\frac{p}{q}) = \frac{n_1 \cdot m_2}{\gcd(n_1 \cdot m_2, m_1 \cdot n_2)}$.

The theorem is a consequence of (41), (8), and (7).

3. Preliminaries about Rings and Fields

In the sequel R denotes a ring and F denotes a field.

Let us note that there exists an element of $\mathbb{Z}^{\mathrm{R}}$ which is positive and there exists an element of $\mathbb{Z}^{\mathrm{R}}$ which is negative.

Let a, b be elements of $\mathbb{F}_{\mathbb{Q}}$ and x, y be rational numbers. We identify $x + y$ with $a + b$. We identify $x \cdot y$ with $a \cdot b$. Let a be an element of $\mathbb{F}_{\mathbb{Q}}$ and x be a rational number. We identify $-x$ with $-a$. Let a be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. We identify x^{-1} with a^{-1}. Let a, b be elements of $\mathbb{F}_{\mathbb{Q}}$ and x, y be rational numbers. We identify $x - y$ with $a - b$. Let a be an element of $\mathbb{F}_{\mathbb{Q}}$ and b be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. We identify $\frac{x}{y}$ with $\frac{a}{b}$. Let F be a field. Let us observe that $(1_F)^{-1}$ reduces to 1_F.

Let R, S be rings. We say that R includes an isomorphic copy of S if and only if

(Def. 1) there exists a strict subring T of R such that T and S are isomorphic.

We introduce the notation R includes S as a synonym of R includes an isomorphic copy of S.

Let us observe that the predicate R and S are isomorphic is reflexive.

Now we state the propositions:

(43) Let us consider a field E. Then every subfield of E is a subring of E.

(44) Let us consider rings R, S, T. If R and S are isomorphic and S and T are isomorphic, then R and T are isomorphic.

(45) Let us consider a field F, and a subring R of F. Then R is a subfield of F if and only if R is a field.

(46) Let us consider a field E, and a strict subfield F of E. Then E includes F.

(47) $\mathbb{Z}^{\mathrm{R}}$ is a subring of $\mathbb{F}_{\mathbb{Q}}$.

(48) $\mathbb{R}_{\mathrm{F}}$ is a subfield of $\mathbb{C}_{\mathrm{F}}$.

Let R be an integral domain. Observe that there exists an integral domain which is R-homomorphic and there exists a commutative ring which is R-homomorphic and there exists a ring which is R-homomorphic.

Let R be a field. Let us note that there exists an integral domain which is R-homomorphic.

Let F be a field, R be an F-homomorphic ring, and f be a homomorphism from F to R. Note that $\operatorname{Im} f$ is almost left invertible.

Let F be an integral domain, E be an F-homomorphic integral domain, and f be a homomorphism from F to E. Note that $\operatorname{Im} f$ is non degenerated.

Let us consider a ring R, an R-homomorphic ring E, a subring K of R, a function f from R into E, and a function g from K into E. Now we state the propositions:

(49) If $g = f\restriction$(the carrier of K) and f is additive, then g is additive. The theorem is a consequence of (1).

(50) If $g = f\restriction$(the carrier of K) and f is multiplicative, then g is multiplicative. The theorem is a consequence of (1).

(51) If $g = f\restriction$(the carrier of K) and f is unity-preserving, then g is unity-preserving.

Now we state the propositions:

(52) Let us consider a ring R, an R-homomorphic ring E, and a subring K of R. Then E is K-homomorphic. The theorem is a consequence of (49), (50), and (51).

(53) Let us consider a ring R, an R-homomorphic ring E, a subring K of R, a K-homomorphic ring E_1, and a homomorphism f from R to E. If $E = E_1$, then $f\restriction K$ is a homomorphism from K to E_1. The theorem is a consequence of (49), (50), and (51).

Let us consider a field F, an F-homomorphic field E, a subfield K of F, a function f from F into E, and a function g from K into E. Now we state the propositions:

(54) If $g = f\restriction$(the carrier of K) and f is additive, then g is additive. The theorem is a consequence of (1).

(55) If $g = f{\restriction}$(the carrier of K) and f is multiplicative, then g is multiplicative. The theorem is a consequence of (1).

(56) If $g = f{\restriction}$(the carrier of K) and f is unity-preserving, then g is unity-preserving.

Now we state the propositions:

(57) Let us consider a field F, an F-homomorphic field E, and a subfield K of F. Then E is K-homomorphic. The theorem is a consequence of (54), (55), and (56).

(58) Let us consider a field F, an F-homomorphic field E, a subfield K of F, a K-homomorphic field E_1, and a homomorphism f from F to E. If $E = E_1$, then $f{\restriction}K$ is a homomorphism from K to E_1. The theorem is a consequence of (54), (55), and (56).

Let n be a natural number. We introduce the notation $\mathbb{Z}/n$ as a synonym of $\mathbb{Z}_n^{\mathrm{R}}$.

One can verify that $\mathbb{Z}/n$ is finite.

Let n be a non trivial natural number. One can check that $\mathbb{Z}/n$ is non degenerated.

Let n be a positive natural number. Note that $\mathbb{Z}/n$ is Abelian, add-associative, right zeroed, and right complementable and $\mathbb{Z}/n$ is associative, well unital, distributive, and commutative.

Let p be a prime number. Observe that $\mathbb{Z}/p$ is almost left invertible.

4. Embedding the Integers in Rings

Let R be an add-associative, right zeroed, right complementable, non empty double loop structure, a be an element of R, and i be an integer. The functor $i \star a$ yielding an element of R is defined by

(Def. 2) there exists a natural number n such that $i = n$ and $it = n \cdot a$ or $i = -n$ and $it = -n \cdot a$.

Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure R and an element a of R. Now we state the propositions:

(59) $0 \star a = 0_R$.

(60) $1 \star a = a$.

(61) $(-1) \star a = -a$.

Now we state the propositions:

(62) Let us consider an add-associative, right zeroed, right complementable, Abelian, non empty double loop structure R, an element a of R, and integers i, j. Then $(i+j)\star a = i\star a + j\star a$.

PROOF: Define $\mathcal{P}$[integer] $\equiv$ for every integer k such that $k = \$_1$ holds $(i+k)\star a = i\star a + k\star a$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$ by [36, (8)]. For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

(63) Let us consider an add-associative, right zeroed, right complementable, Abelian, non empty double loop structure R, an element a of R, and an integer i. Then $(-i)\star a = -i\star a$.

PROOF: Define $\mathcal{P}$[integer] $\equiv$ for every integer k such that $k = \$_1$ holds $(-k)\star a = -k\star a$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$ by [36, (33), (30)]. For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

Let us consider an add-associative, right zeroed, right complementable, Abelian, non empty double loop structure R, an element a of R, and integers i, j. Now we state the propositions:

(64) $(i-j)\star a = i\star a - j\star a$. The theorem is a consequence of (62) and (63).

(65) $i\cdot j\star a = i\star(j\star a)$.

PROOF: Define $\mathcal{P}$[integer] $\equiv$ for every integer k such that $k = \$_1$ holds $k\cdot j\star a = k\star(j\star a)$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$. For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

(66) $i\star(j\star a) = j\star(i\star a)$. The theorem is a consequence of (65).

Now we state the propositions:

(67) Let us consider an add-associative, right zeroed, right complementable, Abelian, left unital, distributive, non empty double loop structure R, and integers i, j. Then $i\cdot j\star 1_R = (i\star 1_R)\cdot(j\star 1_R)$.

PROOF: Define $\mathcal{P}$[integer] $\equiv$ for every integer k such that $k = \$_1$ holds $k\cdot j\star 1_R = (k\star 1_R)\cdot(j\star 1_R)$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$ by (64), [18, (9)], (60), (62). For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

(68) Let us consider a ring R, an R-homomorphic ring S, a homomorphism f from R to S, an element a of R, and an integer i. Then $f(i\star a) = i\star f(a)$.

PROOF: Define $\mathcal{P}$[integer] $\equiv$ for every integer j such that $j = \$_1$ holds $f(j\star a) = j\star f(a)$. For every integer i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i-1]$ and $\mathcal{P}[i+1]$ by (62), (60), [36, (8)], (61). For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

5. Mono- and Isomorphisms of Rings

Let R, S be rings. We say that S is R-monomorphic if and only if

(Def. 3) there exists a function f from R into S such that f is monomorphic.

Let R be a ring. Note that there exists a ring which is R-monomorphic.

Let R be a commutative ring. One can check that there exists a commutative ring which is R-monomorphic and there exists a ring which is R-monomorphic.

Let R be an integral domain. One can verify that there exists an integral domain which is R-monomorphic and there exists a commutative ring which is R-monomorphic and there exists a ring which is R-monomorphic.

Let R be a field. Let us observe that there exists a field which is R-monomorphic and there exists an integral domain which is R-monomorphic and there exists a commutative ring which is R-monomorphic and there exists a ring which is R-monomorphic.

Let R be a ring and S be an R-monomorphic ring. Let us note that there exists a function from R into S which is additive, multiplicative, unity-preserving, and monomorphic.

A monomorphism of R and S is an additive, multiplicative, unity-preserving, monomorphic function from R into S. One can check that every S-monomorphic ring is R-monomorphic and every R-monomorphic ring is R-homomorphic.

Let S be an R-monomorphic ring and f be a monomorphism of R and S. Let us note that $(f^{-1})^{-1}$ reduces to f.

Now we state the propositions:

(69) Let us consider a ring R, an R-homomorphic ring S, an S-homomorphic ring T, a homomorphism f from R to S, and a homomorphism g from S to T. Then $\ker f \subseteq \ker g \cdot f$.

(70) Let us consider a ring R, an R-homomorphic ring S, an S-monomorphic ring T, a homomorphism f from R to S, and a monomorphism g of S and T. Then $\ker f = \ker g \cdot f$. The theorem is a consequence of (69).

(71) Let us consider a ring R, and a subring S of R. Then R is S-monomorphic.

(72) Let us consider rings R, S. Then S is an R-monomorphic ring if and only if S includes R. The theorem is a consequence of (44).

Let R, S be rings. We say that S is R-isomorphic if and only if

(Def. 4) there exists a function f from R into S such that f is isomorphism.

Let R be a ring. Let us note that there exists a ring which is R-isomorphic.

Let R be a commutative ring. Note that there exists a commutative ring which is R-isomorphic and there exists a ring which is R-isomorphic.

Let R be an integral domain. One can check that there exists an integral domain which is R-isomorphic and there exists a commutative ring which is

R-isomorphic and there exists a ring which is R-isomorphic.

Let R be a field. One can verify that there exists a field which is R-isomorphic and there exists an integral domain which is R-isomorphic and there exists a commutative ring which is R-isomorphic and there exists a ring which is R-isomorphic.

Let R be a ring and S be an R-isomorphic ring. Observe that there exists a function from R into S which is additive, multiplicative, unity-preserving, and isomorphism.

An isomorphism between R and S is an additive, multiplicative, unity-preserving, isomorphism function from R into S. Let f be an isomorphism between R and S. Let us note that the functor f^{-1} yields a function from S into R. One can check that there exists a function from S into R which is additive, multiplicative, unity-preserving, and isomorphism.

An isomorphism between S and R is an additive, multiplicative, unity-preserving, isomorphism function from S into R. One can check that every S-isomorphic ring is R-isomorphic and every R-isomorphic ring is R-monomorphic.

Now we state the propositions:

(73) Let us consider a ring R, an R-isomorphic ring S, and an isomorphism f between R and S. Then f^{-1} is an isomorphism between S and R.

(74) Let us consider a ring R, and an R-isomorphic ring S. Then R is S-isomorphic. The theorem is a consequence of (73).

Let R be a commutative ring. Let us note that every R-isomorphic ring is commutative. Let R be an integral domain. One can check that every R-isomorphic ring is non degenerated and integral domain-like.

Let F be a field. One can verify that every F-isomorphic ring is almost left invertible.

(75) Let us consider fields E, F. Then E includes F if and only if there exists a strict subfield K of E such that K and F are isomorphic.

6. Characteristic of Rings

Let R be a ring. The functor $\operatorname{char}(R)$ yielding a natural number is defined by

(Def. 5) $it \star 1_R = 0_R$ and $it \neq 0$ and for every positive natural number m such that $m < it$ holds $m \star 1_R \neq 0_R$ or $it = 0$ and for every positive natural number m, $m \star 1_R \neq 0_R$.

Let n be a natural number. We say that R has characteristic n if and only if

(Def. 6) $\operatorname{char}(R) = n$.

Now we state the propositions:

(76) $\mathrm{char}(\mathbb{Z}^{\mathrm{R}}) = 0$.

(77) Let us consider a positive natural number n. Then $\mathrm{char}(\mathbb{Z}/n) = n$. The theorem is a consequence of (60) and (59).

Observe that $\mathbb{Z}^{\mathrm{R}}$ has characteristic 0.

Let n be a positive natural number. Note that $\mathbb{Z}/n$ has characteristic n.

Let n be a natural number. One can check that there exists a commutative ring which has characteristic n.

Let n be a positive natural number and R be a ring with characteristic n. Let us note that $\mathrm{char}(R)$ is positive.

Let R be a ring. The functor $\mathrm{charSet}\,R$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 7) $\{n$, where n is a positive natural number : $n \star 1_R = 0_R\}$.

Let n be a positive natural number and R be a ring with characteristic n. Note that $\mathrm{charSet}\,R$ is non empty.

Now we state the propositions:

(78) Let us consider a ring R. Then $\mathrm{char}(R) = 0$ if and only if $\mathrm{charSet}\,R = \emptyset$.

(79) Let us consider a positive natural number n, and a ring R with characteristic n. Then $\mathrm{char}(R) = \min \mathrm{charSet}\,R$.

(80) Let us consider a ring R. Then $\mathrm{char}(R) = \min^* \mathrm{charSet}\,R$. The theorem is a consequence of (78) and (79).

(81) Let us consider a prime number p, a ring R with characteristic p, and a positive natural number n. Then n is an element of $\mathrm{charSet}\,R$ if and only if $p \mid n$. The theorem is a consequence of (67), (62), and (79).

Let R be a ring. The functor $\mathrm{canHom}\mathbb{Z}(R)$ yielding a function from $\mathbb{Z}^{\mathrm{R}}$ into R is defined by

(Def. 8) for every element x of $\mathbb{Z}^{\mathrm{R}}$, $it(x) = x \star 1_R$.

Observe that $\mathrm{canHom}\mathbb{Z}(R)$ is additive, multiplicative, and unity-preserving and every ring is $(\mathbb{Z}^{\mathrm{R}})$-homomorphic.

Now we state the propositions:

(82) Let us consider a ring R, and a non negative element n of $\mathbb{Z}^{\mathrm{R}}$. Then $\mathrm{char}(R) = n$ if and only if $\ker \mathrm{canHom}\mathbb{Z}(R) = \{n\}$–ideal. The theorem is a consequence of (64), (63), and (80).

(83) Let us consider a ring R. Then $\mathrm{char}(R) = 0$ if and only if $\mathrm{canHom}\mathbb{Z}(R)$ is monomorphic. The theorem is a consequence of (82).

Let R be a ring with characteristic 0. Observe that $\mathrm{canHom}\mathbb{Z}(R)$ is monomorphic and there exists a function from $\mathbb{Z}^{\mathrm{R}}$ into R which is additive, multiplicative, unity-preserving, and monomorphic.

Now we state the propositions:

(84) Let us consider a ring R, and a homomorphism f from $\mathbb{Z}^{\mathrm{R}}$ to R. Then $f = \mathrm{canHom}\mathbb{Z}(R)$.
PROOF: Define $\mathcal{P}[\text{integer}] \equiv$ for every integer j such that $j = \$_1$ holds $f(j) = j \star 1_R$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$ by [16, (8)], (60), (64), (62). For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

(85) Let us consider a homomorphism f from $\mathbb{Z}^{\mathrm{R}}$ to $\mathbb{Z}^{\mathrm{R}}$. Then $f = \mathrm{id}_{\mathbb{Z}^{\mathrm{R}}}$. The theorem is a consequence of (84).

(86) Let us consider an integral domain R. Then

(i) $\mathrm{char}(R) = 0$, or

(ii) $\mathrm{char}(R)$ is prime.

The theorem is a consequence of (60) and (67).

(87) Let us consider a ring R, and an R-homomorphic ring S. Then $\mathrm{char}(S) \mid \mathrm{char}(R)$. The theorem is a consequence of (84), (69), and (82).

(88) Let us consider a ring R, and an R-monomorphic ring S. Then $\mathrm{char}(S) = \mathrm{char}(R)$. The theorem is a consequence of (84), (70), and (82).

(89) Let us consider a ring R, and a subring S of R. Then $\mathrm{char}(S) = \mathrm{char}(R)$. The theorem is a consequence of (71) and (88).

Let n be a natural number and R be a ring with characteristic n. One can verify that every ring which is R-monomorphic has also characteristic n and every subring of R has characteristic n and $\mathbb{C}_{\mathrm{F}}$ has characteristic 0 and $\mathbb{R}_{\mathrm{F}}$ has characteristic 0 and $\mathbb{F}_{\mathbb{Q}}$ has characteristic 0 and there exists a field which has characteristic 0.

Let p be a prime number. Let us note that there exists a field which has characteristic p. Let R be an integral domain with characteristic p. One can verify that $\mathrm{char}(R)$ is prime.

Let F be a field with characteristic 0. Note that every subfield of F has characteristic 0. Let p be a prime number and F be a field with characteristic p. Note that every subfield of F has characteristic p.

7. Prime Fields

Let F be a field. The functor carrier $\cap F$ yielding a subset of F is defined by the term

(Def. 9) $\{x$, where x is an element of F : for every subfield K of F, $x \in K\}$.

The functor PrimeField F yielding a strict double loop structure is defined by

(Def. 10) the carrier of *it* = carrier $\cap F$ and the addition of *it* = (the addition of F) $\restriction$ carrier $\cap F$ and the multiplication of *it* = (the multiplication of F) $\restriction$ carrier $\cap F$ and the one of *it* = 1_F and the zero of *it* = 0_F.

One can verify that PrimeField F is non degenerated and PrimeField F is Abelian, add-associative, right zeroed, and right complementable and PrimeField F is commutative and PrimeField F is associative, well unital, distributive, and almost left invertible.

Let us note that the functor PrimeField F yields a strict subfield of F. Now we state the propositions:

(90) Let us consider a field F, and a strict subfield E of PrimeField F. Then $E =$ PrimeField F.

(91) Let us consider a field F, and a subfield E of F. Then PrimeField F is a subfield of E.

Let us consider fields F, K. Now we state the propositions:

(92) $K =$ PrimeField F if and only if K is a strict subfield of F and for every strict subfield E of K, $E = K$. The theorem is a consequence of (91) and (90).

(93) $K =$ PrimeField F if and only if K is a strict subfield of F and for every subfield E of F, K is a subfield of E. The theorem is a consequence of (91).

Now we state the propositions:

(94) Let us consider a field E, and a subfield F of E. Then PrimeField $F =$ PrimeField E. The theorem is a consequence of (93) and (92).

(95) Let us consider a field F. Then PrimeField PrimeField $F =$ PrimeField F.

Let F be a field. Let us observe that PrimeField F is prime.

Now we state the propositions:

(96) Let us consider a field F. Then F is prime if and only if $F =$ PrimeField F.

(97) Let us consider a field F with characteristic 0, and non zero integers i, j. Suppose $j \mid i$. Then $(i \operatorname{div} j) \star 1_F = (i \star 1_F) \cdot (j \star 1_F)^{-1}$.

Proof: Consider k being an integer such that $i = j \cdot k$. $j \star 1_F \neq 0_F$ by [34, (3)], (63), [36, (17)]. $i \star 1_F \neq 0_F$ by [34, (3)], (63), [36, (17)]. □

Let x be an element of $\mathbb{F}_{\mathbb{Q}}$. Note that the functor den x yields a positive element of $\mathbb{Z}^{\mathrm{R}}$. One can check that the functor num x yields an element of $\mathbb{Z}^{\mathrm{R}}$. Let F be a field. The functor canHom$\mathbb{Q}(F)$ yielding a function from $\mathbb{F}_{\mathbb{Q}}$ into F is defined by

(Def. 11) for every element x of $\mathbb{F}_{\mathbb{Q}}$, $it(x) = \frac{(\mathrm{canHom}\mathbb{Z}(F))(\mathrm{num}\, x)}{(\mathrm{canHom}\mathbb{Z}(F))(\mathrm{den}\, x)}$.

Observe that canHom$\mathbb{Q}(F)$ is unity-preserving.

Let F be a field with characteristic 0. One can check that canHom$\mathbb{Q}(F)$ is additive and multiplicative and every field with characteristic 0 is $(\mathbb{F}_{\mathbb{Q}})$-monomorphic.

Now we state the proposition:

(98) Let us consider a field F. Then canHom$\mathbb{Z}(F) =$ canHom$\mathbb{Q}(F){\restriction}\mathbb{Z}$.

Let us observe that there exists a field which is $(\mathbb{F}_{\mathbb{Q}})$-homomorphic and has characteristic 0.

Now we state the proposition:

(99) Let us consider an $(\mathbb{F}_{\mathbb{Q}})$-homomorphic field F with characteristic 0, and a homomorphism f from $\mathbb{F}_{\mathbb{Q}}$ to F. Then $f =$ canHom$\mathbb{Q}(F)$.
PROOF: Set $g =$ canHom$\mathbb{Q}(F)$. Define $\mathcal{P}[\text{integer}] \equiv$ for every element j of $\mathbb{F}_{\mathbb{Q}}$ such that $j = \$_1$ holds $f(j) = g(j)$. For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. For every integer i and for every element j of $\mathbb{F}_{\mathbb{Q}}$ such that $j = i$ holds $f(j) = (\text{canHom}\mathbb{Z}(F))(i)$ by (98), [7, (49)]. □

One can verify that $\mathbb{F}_{\mathbb{Q}}$ is $(\mathbb{F}_{\mathbb{Q}})$-homomorphic.

Let F be a field with characteristic 0. One can verify that PrimeField F is $(\mathbb{F}_{\mathbb{Q}})$-homomorphic.

Now we state the proposition:

(100) Let us consider a homomorphism f from $\mathbb{F}_{\mathbb{Q}}$ to $\mathbb{F}_{\mathbb{Q}}$. Then $f = \text{id}_{\mathbb{F}_{\mathbb{Q}}}$. The theorem is a consequence of (99).

Let F be a field, S be an F-homomorphic field, and f be a homomorphism from F to S. One can verify that the functor Im f yields a strict subfield of S. Let F be a field with characteristic 0. Let us note that canHom$\mathbb{Q}$(PrimeField F) is onto.

Now we state the propositions:

(101) Let us consider a field F with characteristic 0. Then $\mathbb{F}_{\mathbb{Q}}$ and PrimeField F are isomorphic.

(102) PrimeField $\mathbb{F}_{\mathbb{Q}} = \mathbb{F}_{\mathbb{Q}}$.

(103) Let us consider a field F with characteristic 0. Then F includes $\mathbb{F}_{\mathbb{Q}}$.

(104) Let us consider a field F with characteristic 0, and a field E. If F includes E, then E includes $\mathbb{F}_{\mathbb{Q}}$. The theorem is a consequence of (72) and (88).

(105) Let us consider a prime number p, a ring R with characteristic p, and an integer i. Then $i \star 1_R = (i \bmod p) \star 1_R$. The theorem is a consequence of (67) and (62).

Let p be a prime number and F be a field. The functor canHom$\mathbb{Z}/p(F)$ yielding a function from $\mathbb{Z}/p$ into F is defined by the term

(Def. 12) canHom$\mathbb{Z}(F){\restriction}$(the carrier of $\mathbb{Z}/p$).

Note that canHom$\mathbb{Z}/p(F)$ is unity-preserving.

Let F be a field with characteristic p. One can verify that canHom$\mathbb{Z}/p(F)$ is additive and multiplicative and every field with characteristic p is $(\mathbb{Z}/p)$-monomorphic and there exists a field which is $(\mathbb{Z}/p)$-homomorphic and has characteristic p and $\mathbb{Z}/p$ is $(\mathbb{Z}/p)$-homomorphic.

Now we state the propositions:

(106) Let us consider a prime number p, a $(\mathbb{Z}/p)$-homomorphic field F with characteristic p, and a homomorphism f from $\mathbb{Z}/p$ to F. Then $f =$ canHom$\mathbb{Z}/p(F)$.

Proof: Set $g =$ canHom$\mathbb{Z}/p(F)$. Reconsider $p_1 = p - 1$ as an element of $\mathbb{N}$. Define $\mathcal{P}$[natural number] $\equiv$ for every element j of $\mathbb{Z}/p$ such that $j = \$_1$ holds $f(j) = g(j)$. For every element k of $\mathbb{N}$ such that $0 \leqslant k < p_1$ holds if $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$ by [3, (13), (44)], [29, (14), (7)]. For every element k of $\mathbb{N}$ such that $0 \leqslant k \leqslant p_1$ holds $\mathcal{P}[k]$ from [34, Sch. 7]. □

(107) Let us consider a prime number p, and a homomorphism f from $\mathbb{Z}/p$ to $\mathbb{Z}/p$. Then $f = \mathrm{id}_{\mathbb{Z}/p}$. The theorem is a consequence of (106).

Let p be a prime number and F be a field with characteristic p. Observe that PrimeField F is $(\mathbb{Z}/p)$-homomorphic and canHom$\mathbb{Z}/p$(PrimeField F) is onto.

Now we state the propositions:

(108) Let us consider a prime number p, and a field F with characteristic p. Then $\mathbb{Z}/p$ and PrimeField F are isomorphic.

(109) Let us consider a prime number p, and a strict subfield F of $\mathbb{Z}/p$. Then $F = \mathbb{Z}/p$.

(110) Let us consider a prime number p. Then PrimeField $\mathbb{Z}/p = \mathbb{Z}/p$.

(111) Let us consider a prime number p, and a field F with characteristic p. Then F includes $\mathbb{Z}/p$.

(112) Let us consider a prime number p, a field F with characteristic p, and a field E. If F includes E, then E includes $\mathbb{Z}/p$. The theorem is a consequence of (72) and (88).

Let p be a prime number. One can check that $\mathbb{Z}/p$ is prime.

Now we state the propositions:

(113) Let us consider a field F. Then $\mathrm{char}(F) = 0$ if and only if PrimeField F and $\mathbb{F}_{\mathbb{Q}}$ are isomorphic. The theorem is a consequence of (101), (43), and (89).

(114) Let us consider a prime number p, and a field F. Then $\mathrm{char}(F) = p$ if and only if PrimeField F and $\mathbb{Z}/p$ are isomorphic. The theorem is a consequence of (108), (43), and (89).

(115) Let us consider a strict field F. Then F is prime if and only if F and $\mathbb{F}_{\mathbb{Q}}$ are isomorphic or there exists a prime number p such that F and $\mathbb{Z}/p$

are isomorphic. The theorem is a consequence of (86), (101), (108), (44), (57), and (58).

References

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

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

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

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

[5] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

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

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

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

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

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

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

[12] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Set of points on elliptic curve in projective coordinates. *Formalized Mathematics*, 19(**3**):131–138, 2011. doi:10.2478/v10037-011-0021-6.

[13] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Gaussian integers. *Formalized Mathematics*, 21(**2**):115–125, 2013. doi:10.2478/forma-2013-0013.

[14] Nathan Jacobson. *Basic Algebra I*. 2nd edition. Dover Publications Inc., 2009.

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

[16] Artur Korniłowicz and Christoph Schwarzweller. The first isomorphism theorem and other properties of rings. *Formalized Mathematics*, 22(**4**):291–301, 2014. doi:10.2478/forma-2014-0029.

[17] Jarosław Kotowicz. Quotient vector spaces and functionals. *Formalized Mathematics*, 11 (**1**):59–68, 2003.

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

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

[20] Heinz Lüneburg. *Die grundlegenden Strukturen der Algebra (in German)*. Oldenbourg Wisenschaftsverlag, 1999.

[21] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**): 265–269, 2001.

[22] Michał Muzalewski. Opposite rings, modules and their morphisms. *Formalized Mathematics*, 3(**1**):57–65, 1992.

[23] Michał Muzalewski. Category of rings. *Formalized Mathematics*, 2(**5**):643–648, 1991.

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

[25] Michał Muzalewski and Wojciech Skaba. From loops to Abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.

[26] Karol Pąk. Linear map of matrices. *Formalized Mathematics*, 16(**3**):269–275, 2008. doi:10.2478/v10037-008-0032-0.

[27] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

[28] Christoph Schwarzweller. The correctness of the generic algorithms of Brown and Henrici concerning addition and multiplication in fraction fields. *Formalized Mathematics*, 6(**3**): 381–388, 1997.

[29] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.

[30] Christoph Schwarzweller. The field of quotients over an integral domain. *Formalized Mathematics*, 7(**1**):69–79, 1998.

[31] Yasunari Shidama, Hikofumi Suzuki, and Noboru Endou. Banach algebra of bounded functionals. *Formalized Mathematics*, 16(**2**):115–122, 2008. doi:10.2478/v10037-008-0017-z.

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

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

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

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

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

[37] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.

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

[39] B.L. van der Waerden. *Algebra I*. 4th edition. Springer, 2003.

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

Received August 14, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 351–369, 2015
DOI: 10.1515/forma-2015-0028

DE GRUYTER OPEN
degruyter.com/view/j/forma

Exponential Objects

Marco Riccardi
Via del Pero 102
54038 Montignoso
Italy

Summary. In the first part of this article we formalize the concepts of terminal and initial object, categorical product [4] and natural transformation within a free-object category [1]. In particular, we show that this definition of natural transformation is equivalent to the standard definition [13]. Then we introduce the exponential object using its universal property and we show the isomorphism between the exponential object of categories and the functor category [12].

MSC: 18A99 18A25 03B35

Keywords: exponential objects; functor category; natural transformation

MML identifier: `CAT_8`, version: `8.1.04 5.33.1254`

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

1. Preliminaries

Now we state the propositions:

(1) Let us consider a composable, associative category structure $\mathscr{C}$, and morphisms f_1, f_2, f_3 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$ and $f_2 \triangleright f_3$. Then $(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$.

(2) Let us consider a composable, associative category structure $\mathscr{C}$, and morphisms f_1, f_2, f_3, f_4 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$ and $f_2 \triangleright f_3$ and $f_3 \triangleright f_4$. Then

(i) $((f_1 \circ f_2) \circ f_3) \circ f_4 = (f_1 \circ f_2) \circ (f_3 \circ f_4)$, and

(ii) $((f_1 \circ f_2) \circ f_3) \circ f_4 = (f_1 \circ (f_2 \circ f_3)) \circ f_4$, and

ISSN 1426–2630(Print), 1898-9934(Online)

(iii) $((f_1 \circ f_2) \circ f_3) \circ f_4 = f_1 \circ ((f_2 \circ f_3) \circ f_4)$, and

(iv) $((f_1 \circ f_2) \circ f_3) \circ f_4 = f_1 \circ (f_2 \circ (f_3 \circ f_4))$.

The theorem is a consequence of (1).

(3) Let us consider a composable category structure $\mathscr{C}$, and morphisms f, f_1, f_2 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$. Then

(i) $f_1 \circ f_2 \triangleright f$ iff $f_2 \triangleright f$, and

(ii) $f \triangleright f_1 \circ f_2$ iff $f \triangleright f_1$.

(4) Let us consider a composable category structure $\mathscr{C}$ with identities, and morphisms f_1, f_2 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$. Then

(i) if f_1 is identity, then $f_1 \circ f_2 = f_2$, and

(ii) if f_2 is identity, then $f_1 \circ f_2 = f_1$.

PROOF: If f_1 is identity, then $f_1 \circ f_2 = f_2$ by [16, (6), (5), (9)]. $\square$

(5) Let us consider a non empty category structure $\mathscr{C}$ with identities, and a morphism f of $\mathscr{C}$. Then there exist morphisms f_1, f_2 of $\mathscr{C}$ such that

(i) f_1 is identity, and

(ii) f_2 is identity, and

(iii) $f_1 \triangleright f$, and

(iv) $f \triangleright f_2$.

(6) Let us consider a category structure $\mathscr{C}$, objects a, b of $\mathscr{C}$, and a morphism f from a to b. Suppose $\hom(a, b) = \{f\}$. Let us consider a morphism g from a to b. Then $f = g$.

(7) Let us consider a category structure $\mathscr{C}$, objects a, b of $\mathscr{C}$, and a morphism f from a to b. Suppose $\hom(a, b) \neq \emptyset$ and for every morphism g from a to b, $f = g$. Then $\hom(a, b) = \{f\}$.

(8) Let us consider an object x, and a category structure $\mathscr{C}$. Suppose the carrier of $\mathscr{C} = \{x\}$ and the composition of $\mathscr{C} = \{\langle\langle x, x\rangle, x\rangle\}$. Then $\mathscr{C}$ is a non empty category.

PROOF: For every object y, $y \in$ the composition of the discrete category of $\{x\}$ iff $y \in \{\langle\langle x, x\rangle, x\rangle\}$ by [22, (2)], [9, (29)], [15, (24)], (4). $\square$

(9) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$, and a functor $\mathcal{F}$ from $\mathscr{C}_1$ to $\mathscr{C}_2$. If $\mathcal{F}$ is isomorphism, then $\mathcal{F}$ is bijective.

(10) Let us consider composable category structures $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{C}_3$ with identities. Suppose $\mathscr{C}_1 \cong \mathscr{C}_2$ and $\mathscr{C}_2 \cong \mathscr{C}_3$. Then $\mathscr{C}_1 \cong \mathscr{C}_3$.

(11) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$. Suppose $\mathscr{C}_1 \cong \mathscr{C}_2$. Then $\mathscr{C}_1$ is empty if and only if $\mathscr{C}_2$ is empty.

Let $\mathscr{C}_1$ be an empty category structure with identities and $\mathscr{C}_2$ be category structure with identities. Note that every functor from $\mathscr{C}_1$ to $\mathscr{C}_2$ is covariant.

Now we state the propositions:

(12) Let us consider category structures $\mathscr{C}_1$, $\mathscr{C}_2$ with identities, a morphism f of $\mathscr{C}_1$, and a functor $\mathcal{F}$ from $\mathscr{C}_1$ to $\mathscr{C}_2$. Suppose $\mathcal{F}$ is covariant and f is identity. Then $\mathcal{F}(f)$ is identity.

(13) Let us consider category structures $\mathscr{C}_1$, $\mathscr{C}_2$ with identities, morphisms f_1, f_2 of $\mathscr{C}_1$, and a functor $\mathcal{F}$ from $\mathscr{C}_1$ to $\mathscr{C}_2$. Suppose $\mathcal{F}$ is covariant and $f_1 \triangleright f_2$. Then

(i) $\mathcal{F}(f_1) \triangleright \mathcal{F}(f_2)$, and

(ii) $\mathcal{F}(f_1 \circ f_2) = \mathcal{F}(f_1) \circ \mathcal{F}(f_2)$.

(14) Let us consider an object-category $\mathscr{C}$, a morphism f of $\mathscr{C}$, and a morphism g of alter $\mathscr{C}$. Suppose $f = g$. Then

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

(ii) $\operatorname{cod} g = \mathrm{id}_{\operatorname{cod} f}$.

PROOF: Consider d_1 being a morphism of alter $\mathscr{C}$ such that $\operatorname{dom} g = d_1$ and $g \triangleright d_1$ and d_1 is identity. Reconsider $d_2 = \mathrm{id}_{\operatorname{dom} f}$ as a morphism of alter $\mathscr{C}$. For every morphism f_1 of alter $\mathscr{C}$ such that $f_1 \triangleright d_2$ holds $f_1 \circ d_2 = f_1$ by [15, (40)], [5, (22)]. Consider c_1 being a morphism of alter $\mathscr{C}$ such that $\operatorname{cod} g = c_1$ and $c_1 \triangleright g$ and c_1 is identity. Reconsider $c_2 = \mathrm{id}_{\operatorname{cod} f}$ as a morphism of alter $\mathscr{C}$. For every morphism f_1 of alter $\mathscr{C}$ such that $f_1 \triangleright c_2$ holds $f_1 \circ c_2 = f_1$ by [15, (40)], [5, (22)]. □

(15) There exists a morphism f of $\mathbf{1}$ such that

(i) f is identity, and

(ii) $\operatorname{Ob} \mathbf{1} = \{f\}$, and

(iii) $\operatorname{Mor} \mathbf{1} = \{f\}$.

PROOF: Consider $\mathscr{C}$ being a strict, a preorder category such that $\operatorname{Ob} \mathscr{C} = 1$ and for every objects o_1, o_2 of $\mathscr{C}$ such that $o_1 \in o_2$ holds $\hom(o_1, o_2) = \{\langle o_1, o_2 \rangle\}$ and $\operatorname{RelOb} \mathscr{C} = \subseteq_1$ and $\operatorname{Mor} \mathscr{C} = 1 \cup \{\langle o_1, o_2 \rangle$, where o_1, o_2 are elements of $1 : o_1 \in o_2\}$. Consider $\mathcal{F}$ being a functor from $\mathscr{C}$ to $\mathbf{1}$, $\mathcal{G}$ being a functor from $\mathbf{1}$ to $\mathscr{C}$ such that $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathcal{G} \circ \mathcal{F} = \mathrm{id}_{\mathscr{C}}$ and $\mathcal{F} \circ \mathcal{G} = \mathrm{id}_{\mathbf{1}}$. Reconsider $g = 0$ as a morphism of $\mathscr{C}$. Set $f = \mathcal{F}(g)$. Consider x being an object such that $\operatorname{Ob} \mathbf{1} = \{x\}$. For every object x, $x \in \operatorname{Mor} \mathbf{1}$ iff $x \in \{f\}$ by [15, (22)], [6, (18)], [15, (34)], [2, (49)]. □

(16) Let us consider a non empty category $\mathscr{C}$, and morphisms f_1, f_2 of $\mathscr{C}$. If $\mathcal{M}_{\mathrm{f}_1} = \mathcal{M}_{\mathrm{f}_2}$, then $f_1 = f_2$.

(17) Let us consider a non empty category $\mathscr{C}$, covariant functors $\mathcal{F}_1$, $\mathcal{F}_2$ from **2** to $\mathscr{C}$, and a morphism f of **2**. Suppose f is not identity and $\mathcal{F}_1(f) = \mathcal{F}_2(f)$. Then $\mathcal{F}_1 = \mathcal{F}_2$.

PROOF: Consider f_1 being a morphism of **2** such that f_1 is not identity and $\mathrm{Ob}\,\mathbf{2} = \{\mathrm{dom}\, f_1, \mathrm{cod}\, f_1\}$ and $\mathrm{Mor}\,\mathbf{2} = \{\mathrm{dom}\, f_1, \mathrm{cod}\, f_1, f_1\}$ and $\mathrm{dom}\, f_1$, $\mathrm{cod}\, f_1$, f_1 are mutually different. For every object x such that $x \in \mathrm{dom}\,\mathcal{F}_1$ holds $\mathcal{F}_1(x) = \mathcal{F}_2(x)$ by [15, (22), (32)]. □

(18) There exist morphisms f_1, f_2 of **3** such that

(i) f_1 is not identity, and

(ii) f_2 is not identity, and

(iii) $\mathrm{cod}\, f_1 = \mathrm{dom}\, f_2$, and

(iv) $\mathrm{Ob}\,\mathbf{3} = \{\mathrm{dom}\, f_1, \mathrm{cod}\, f_1, \mathrm{cod}\, f_2\}$, and

(v) $\mathrm{Mor}\,\mathbf{3} = \{\mathrm{dom}\, f_1, \mathrm{cod}\, f_1, \mathrm{cod}\, f_2, f_1, f_2, f_2 \circ f_1\}$, and

(vi) $\mathrm{dom}\, f_1$,$\mathrm{cod}\, f_1$,$\mathrm{cod}\, f_2$,f_1,f_2,$f_2 \circ f_1$ are mutually different.

PROOF: Consider $\mathscr{C}$ being a strict, a preorder category such that $\mathrm{Ob}\,\mathscr{C} = 3$ and for every objects o_1, o_2 of $\mathscr{C}$ such that $o_1 \in o_2$ holds $\hom(o_1, o_2) = \{\langle o_1, o_2\rangle\}$ and $\mathrm{RelOb}\,\mathscr{C} = {}^{\subseteq}{}_3$ and $\mathrm{Mor}\,\mathscr{C} = 3 \cup \{\langle o_1, o_2\rangle$, where o_1, o_2 are elements of $3 : o_1 \in o_2\}$. Consider $\mathcal{F}$ being a functor from $\mathscr{C}$ to **3**, $\mathcal{G}$ being a functor from **3** to $\mathscr{C}$ such that $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathcal{G} \circ \mathcal{F} = \mathrm{id}_{\mathscr{C}}$ and $\mathcal{F} \circ \mathcal{G} = \mathrm{id}_{\mathbf{3}}$. Reconsider $g_1 = \langle 0, 1\rangle$ as a morphism of $\mathscr{C}$. g_1 is not identity by [15, (22)]. Set $f_1 = \mathcal{F}(g_1)$. Reconsider $g_2 = \langle 1, 2\rangle$ as a morphism of $\mathscr{C}$. g_2 is not identity by [15, (22)]. Set $f_2 = \mathcal{F}(g_2)$. f_1 is not identity by [6, (18)], [15, (34)]. f_2 is not identity by [6, (18)], [15, (34)]. For every object x, $x \in \mathrm{Ob}\,\mathbf{3}$ iff $x \in \{\mathrm{dom}\, f_1, \mathrm{cod}\, f_1, \mathrm{cod}\, f_2\}$ by [15, (34)], [6, (18)], [15, (22)], [2, (51)]. For every object x, $x \in \mathrm{Mor}\,\mathbf{3}$ iff $x \in \{\mathrm{dom}\, f_1, \mathrm{cod}\, f_1, \mathrm{cod}\, f_2, f_1, f_2, f_2 \circ f_1\}$ by [15, (22)], [6, (18)], [15, (34)], [2, (51), (49), (50)]. $g_2 \circ g_1$ is not identity by [15, (22)]. $f_2 \circ f_1$ is not identity by [6, (18)], [15, (34)]. $\mathcal{F}$ is bijective. □

Let $\mathscr{C}$ be a non empty category and f_1, f_2 be morphisms of $\mathscr{C}$. Assume $f_1 \triangleright f_2$. The functor $\mathcal{C}_{f_1,f_2}$ yielding a covariant functor from **3** to $\mathscr{C}$ is defined by

(Def. 1) for every morphisms g_1, g_2 of **3** such that $g_1 \triangleright g_2$ and g_1 is not identity and g_2 is not identity holds $it(g_1) = f_1$ and $it(g_2) = f_2$.

2. Terminal Objects

Let $\mathscr{C}$ be a category structure and a be an object of $\mathscr{C}$. We say that a is terminal if and only if

(Def. 2) for every object b of $\mathscr{C}$, $\hom(b, a) \neq \emptyset$ and there exists a morphism f from b to a such that for every morphism g from b to a, $f = g$.

Now we state the propositions:

(19) Let us consider a category structure $\mathscr{C}$, and an object b of $\mathscr{C}$. Then b is terminal if and only if for every object a of $\mathscr{C}$, there exists a morphism f from a to b such that $\hom(a, b) = \{f\}$. The theorem is a consequence of (7) and (6).

(20) Let us consider category structure $\mathscr{C}$ with identities, and an object a of $\mathscr{C}$. Suppose a is terminal. Let us consider a morphism h from a to a. Then id-$a = h$.

(21) Let us consider a composable category structure $\mathscr{C}$ with identities, and objects a, b of $\mathscr{C}$. If a is terminal and b is terminal, then a and b are isomorphic. The theorem is a consequence of (20).

(22) Let us consider a category $\mathscr{C}$, and objects a, b of $\mathscr{C}$. If b is terminal and a and b are isomorphic, then a is terminal.

(23) Let us consider a composable category structure $\mathscr{C}$ with identities, objects a, b of $\mathscr{C}$, and a morphism f from a to b. Suppose $\hom(a, b) \neq \emptyset$ and a is terminal. Then f is monomorphic.

Let $\mathscr{C}$ be a category. We say that $\mathscr{C}$ has terminal objects if and only if

(Def. 3) there exists an object a of $\mathscr{C}$ such that a is terminal.

Now we state the proposition:

(24) $\mathbf{1}$ has terminal objects.

Proof: Consider f being a morphism of $\mathbf{1}$ such that f is identity and $\mathrm{Ob}\,\mathbf{1} = \{f\}$ and $\mathrm{Mor}\,\mathbf{1} = \{f\}$. For every objects a, b of $\mathbf{1}$, every morphism of $\mathbf{1}$ is a morphism from a to b by [16, (20)]. □

One can verify that there exists a category which has terminal objects.

Let $\mathscr{C}$ be a category. We say that $\mathscr{C}$ is terminal if and only if

(Def. 4) for every category $\mathscr{B}$, there exists a functor $\mathcal{F}$ from $\mathscr{B}$ to $\mathscr{C}$ such that $\mathcal{F}$ is covariant and for every functor $\mathcal{G}$ from $\mathscr{B}$ to $\mathscr{C}$ such that $\mathcal{G}$ is covariant holds $\mathcal{F} = \mathcal{G}$.

Let us note that $\mathbf{1}$ is non empty and terminal and there exists a category which is strict, non empty, and terminal and there exists a category which is strict and non terminal.

Now we state the propositions:

(25) Let us consider terminal categories $\mathscr{C}$, $\mathscr{D}$. Then $\mathscr{C} \cong \mathscr{D}$.

PROOF: There exists a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$ and there exists a functor $\mathcal{G}$ from $\mathscr{D}$ to $\mathscr{C}$ such that $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathcal{G} \circ \mathcal{F} = \mathrm{id}_{\mathscr{C}}$ and $\mathcal{F} \circ \mathcal{G} = \mathrm{id}_{\mathscr{D}}$ by [15, (35)]. □

(26) Let us consider categories $\mathscr{C}$, $\mathscr{D}$. Suppose $\mathscr{C}$ is terminal and $\mathscr{C} \cong \mathscr{D}$. Then $\mathscr{D}$ is terminal.

PROOF: Consider $\mathcal{F}$ being a functor from $\mathscr{C}$ to $\mathscr{D}$, $\mathcal{G}$ being a functor from $\mathscr{D}$ to $\mathscr{C}$ such that $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathcal{G} \circ \mathcal{F} = \mathrm{id}_{\mathscr{C}}$ and $\mathcal{F} \circ \mathcal{G} = \mathrm{id}_{\mathscr{D}}$. Consider $\mathcal{F}_1$ being a functor from $\mathscr{B}$ to $\mathscr{C}$ such that $\mathcal{F}_1$ is covariant and for every functor $\mathcal{G}$ from $\mathscr{B}$ to $\mathscr{C}$ such that $\mathcal{G}$ is covariant holds $\mathcal{F}_1 = \mathcal{G}$. Set $\mathcal{F}_2 = \mathcal{F} \circ \mathcal{F}_1$. For every functor $\mathcal{G}_1$ from $\mathscr{B}$ to $\mathscr{D}$ such that $\mathcal{G}_1$ is covariant holds $\mathcal{F}_2 = \mathcal{G}_1$ by [15, (35)], [16, (10), (11)]. □

(27) Let us consider a category $\mathscr{C}$. Then $\mathscr{C}$ is non empty and trivial if and only if $\mathscr{C} \cong \mathbf{1}$. The theorem is a consequence of (15), (4), and (26).

(28) Let us consider non empty categories $\mathscr{C}$, $\mathscr{D}$. Suppose $\mathscr{C}$ is trivial and $\mathscr{D}$ is trivial. Then $\mathscr{C} \cong \mathscr{D}$. The theorem is a consequence of (27) and (10).

Note that every category which is non empty and trivial is also terminal and every category which is terminal is also non empty and trivial.

Let $\mathscr{C}$ be a category. The functor $\mathscr{C} \to \mathbf{1}$ yielding a covariant functor from $\mathscr{C}$ to $\mathbf{1}$ is defined by

(Def. 5) not contradiction.

Now we state the proposition:

(29) Let us consider categories $\mathscr{C}$, $\mathscr{C}_1$, $\mathscr{C}_2$, a functor $\mathcal{F}_1$ from $\mathscr{C}$ to $\mathscr{C}_1$, and a functor $\mathcal{F}_2$ from $\mathscr{C}$ to $\mathscr{C}_2$. Suppose $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant. Then $\mathscr{C}_1 \to \mathbf{1} \circ \mathcal{F}_1 = \mathscr{C}_2 \to \mathbf{1} \circ \mathcal{F}_2$.

3. Initial Objects

Let $\mathscr{C}$ be a category structure and a be an object of $\mathscr{C}$. We say that a is initial if and only if

(Def. 6) for every object b of $\mathscr{C}$, $\hom(a, b) \neq \emptyset$ and there exists a morphism f from a to b such that for every morphism g from a to b, $f = g$.

Now we state the propositions:

(30) Let us consider a category structure $\mathscr{C}$, and an object b of $\mathscr{C}$. Then b is initial if and only if for every object a of $\mathscr{C}$, there exists a morphism f from b to a such that $\hom(b, a) = \{f\}$. The theorem is a consequence of (7) and (6).

(31) Let us consider category structure $\mathscr{C}$ with identities, and an object a of $\mathscr{C}$. Suppose a is initial. Let us consider a morphism h from a to a. Then id-$a = h$.

(32) Let us consider a composable category structure $\mathscr{C}$ with identities, and objects a, b of $\mathscr{C}$. If a is initial and b is initial, then a and b are isomorphic. The theorem is a consequence of (31).

(33) Let us consider a category $\mathscr{C}$, and objects a, b of $\mathscr{C}$. If b is initial and b and a are isomorphic, then a is initial.

(34) Let us consider a composable category structure $\mathscr{C}$ with identities, objects a, b of $\mathscr{C}$, and a morphism f from a to b. Suppose $\hom(a, b) \neq \emptyset$ and b is initial. Then f is epimorphic.

Let $\mathscr{C}$ be a category. We say that $\mathscr{C}$ has initial objects if and only if

(Def. 7) there exists an object a of $\mathscr{C}$ such that a is initial.

Now we state the proposition:

(35) $\mathbf{1}$ has initial objects.

Proof: Consider f being a morphism of $\mathbf{1}$ such that f is identity and $\operatorname{Ob}\mathbf{1} = \{f\}$ and $\operatorname{Mor}\mathbf{1} = \{f\}$. For every objects a, b of $\mathbf{1}$, every morphism of $\mathbf{1}$ is a morphism from a to b by [16, (20)]. □

Let us note that there exists a category which has initial objects.

Let $\mathscr{C}$ be a category. We say that $\mathscr{C}$ is initial if and only if

(Def. 8) for every category $\mathscr{C}_1$, there exists a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{C}_1$ such that $\mathcal{F}$ is covariant and for every functor $\mathcal{F}_1$ from $\mathscr{C}$ to $\mathscr{C}_1$ such that $\mathcal{F}_1$ is covariant holds $\mathcal{F} = \mathcal{F}_1$.

One can verify that $\mathbf{0}$ is empty and initial and there exists a category which is strict, empty, and initial and there exists a category which is strict and non initial.

Now we state the propositions:

(36) Let us consider initial categories $\mathscr{C}$, $\mathscr{D}$. Then $\mathscr{C} \cong \mathscr{D}$.

Proof: There exists a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$ and there exists a functor $\mathcal{G}$ from $\mathscr{D}$ to $\mathscr{C}$ such that $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathcal{G} \circ \mathcal{F} = \mathrm{id}_{\mathscr{C}}$ and $\mathcal{F} \circ \mathcal{G} = \mathrm{id}_{\mathscr{D}}$ by [15, (35)]. □

(37) Let us consider categories $\mathscr{C}$, $\mathscr{D}$. Suppose $\mathscr{C}$ is initial and $\mathscr{C} \cong \mathscr{D}$. Then $\mathscr{D}$ is initial.

Proof: Consider $\mathcal{F}$ being a functor from $\mathscr{C}$ to $\mathscr{D}$, $\mathcal{G}$ being a functor from $\mathscr{D}$ to $\mathscr{C}$ such that $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathcal{G} \circ \mathcal{F} = \mathrm{id}_{\mathscr{C}}$ and $\mathcal{F} \circ \mathcal{G} = \mathrm{id}_{\mathscr{D}}$. Consider $\mathcal{F}_1$ being a functor from $\mathscr{C}$ to $\mathscr{B}$ such that $\mathcal{F}_1$ is covariant and for every functor $\mathcal{G}$ from $\mathscr{C}$ to $\mathscr{B}$ such that $\mathcal{G}$ is covariant holds $\mathcal{F}_1 = \mathcal{G}$. Set $\mathcal{F}_2 = \mathcal{F}_1 \circ \mathcal{G}$. For every functor $\mathcal{G}_1$ from $\mathscr{D}$ to $\mathscr{B}$ such that $\mathcal{G}_1$ is covariant holds $\mathcal{F}_2 = \mathcal{G}_1$ by [15, (35)], [16, (10), (11)]. □

Let us note that every category which is empty is also initial.

Let $\mathscr{C}$ be a category. The functor $\mathbf{0} \to \mathscr{C}$ yielding a covariant functor from $\mathbf{0}$ to $\mathscr{C}$ is defined by

(Def. 9) not contradiction.

Now we state the proposition:

(38) Let us consider categories $\mathscr{C}$, $\mathscr{C}_1$, $\mathscr{C}_2$, a functor $\mathcal{F}_1$ from $\mathscr{C}_1$ to $\mathscr{C}$, and a functor $\mathcal{F}_2$ from $\mathscr{C}_2$ to $\mathscr{C}$. Suppose $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant. Then $\mathcal{F}_1 \circ \mathbf{0} \to \mathscr{C}_1 = \mathcal{F}_2 \circ \mathbf{0} \to \mathscr{C}_2$.

4. Categorical Products

Let $\mathscr{C}$ be a category, a, b, c be objects of $\mathscr{C}$, and p_1 be a morphism from c to a. Assume $\hom(c, a) \neq \emptyset$. Let p_2 be a morphism from c to b. Assume $\hom(c, b) \neq \emptyset$. We say that $\langle c, p_1, p_2\rangle$ is a product of a and b if and only if

(Def. 10) for every object c_1 of $\mathscr{C}$ and for every morphism q_1 from c_1 to a and for every morphism q_2 from c_1 to b such that $\hom(c_1, a) \neq \emptyset$ and $\hom(c_1, b) \neq \emptyset$ holds $\hom(c_1, c) \neq \emptyset$ and there exists a morphism h from c_1 to c such that $p_1 \cdot h = q_1$ and $p_2 \cdot h = q_2$ and for every morphism h_1 from c_1 to c such that $p_1 \cdot h_1 = q_1$ and $p_2 \cdot h_1 = q_2$ holds $h = h_1$.

Now we state the propositions:

(39) Let us consider a category $\mathscr{C}$, objects c_1, c_2, a, b of $\mathscr{C}$, a morphism p_1 from a to c_1, a morphism p_2 from a to c_2, a morphism q_1 from b to c_1, and a morphism q_2 from b to c_2. Suppose $\hom(a, c_1) \neq \emptyset$ and $\hom(a, c_2) \neq \emptyset$ and $\hom(b, c_1) \neq \emptyset$ and $\hom(b, c_2) \neq \emptyset$ and $\langle a, p_1, p_2\rangle$ is a product of c_1 and c_2 and $\langle b, q_1, q_2\rangle$ is a product of c_1 and c_2. Then a and b are isomorphic.

Proof: There exists a morphism f from a to b and there exists a morphism g from b to a such that $\hom(a, b) \neq \emptyset$ and $\hom(b, a) \neq \emptyset$ and $g \cdot f = \text{id-}a$ and $f \cdot g = \text{id-}b$ by [16, (23), (18)]. □

(40) Let us consider a category $\mathscr{C}$, objects c_1, c_2, d of $\mathscr{C}$, a morphism p_1 from d to c_1, and a morphism p_2 from d to c_2. Suppose $\hom(d, c_1) \neq \emptyset$ and $\hom(d, c_2) \neq \emptyset$ and $\langle d, p_1, p_2\rangle$ is a product of c_1 and c_2. Then $\langle d, p_2, p_1\rangle$ is a product of c_2 and c_1.

Let $\mathscr{C}$ be a category. We say that $\mathscr{C}$ has binary products if and only if

(Def. 11) for every objects a, b of $\mathscr{C}$, there exists an object d of $\mathscr{C}$ and there exists a morphism p_1 from d to a and there exists a morphism p_2 from d to b

such that $\hom(d, a) \neq \emptyset$ and $\hom(d, b) \neq \emptyset$ and $\langle d, p_1, p_2 \rangle$ is a product of a and b.

Now we state the proposition:

(41) $\mathbf{1}$ has binary products.

Proof: Set $\mathscr{C} = \mathbf{1}$. Consider f being a morphism of $\mathbf{1}$ such that f is identity and $\mathrm{Ob}\,\mathbf{1} = \{f\}$ and $\mathrm{Mor}\,\mathbf{1} = \{f\}$. For every objects o_1, o_2 of $\mathscr{C}$, every morphism of $\mathscr{C}$ is a morphism from o_1 to o_2 by [16, (20)]. Reconsider $p_1 = f$ as a morphism from a to a. Reconsider $p_2 = f$ as a morphism from a to b. For every object c_1 of $\mathscr{C}$ and for every morphism q_1 from c_1 to a and for every morphism q_2 from c_1 to b such that $\hom(c_1, a) \neq \emptyset$ and $\hom(c_1, b) \neq \emptyset$ holds $\hom(c_1, a) \neq \emptyset$ and there exists a morphism h from c_1 to a such that $p_1 \cdot h = q_1$ and $p_2 \cdot h = q_2$ and for every morphism h_1 from c_1 to a such that $p_1 \cdot h_1 = q_1$ and $p_2 \cdot h_1 = q_2$ holds $h = h_1$. □

Observe that there exists a category which has binary products.

Let $\mathscr{C}$ be a category with binary products and c_1, c_2 be objects of $\mathscr{C}$.

A categorical product of c_1 and c_2 is a triple object and is defined by

(Def. 12) there exists an object d of $\mathscr{C}$ and there exists a morphism p_1 from d to c_1 and there exists a morphism p_2 from d to c_2 such that $it = \langle d, p_1, p_2 \rangle$ and $\hom(d, c_1) \neq \emptyset$ and $\hom(d, c_2) \neq \emptyset$ and $\langle d, p_1, p_2 \rangle$ is a product of c_1 and c_2.

The functor $c_1 \times c_2$ yielding an object of $\mathscr{C}$ is defined by the term

(Def. 13) (the categorical product of c_1 and $c_2)_{\mathbf{1},3}$.

The functor $\pi_1(c_1 \boxtimes c_2)$ yielding a morphism from $c_1 \times c_2$ to c_1 is defined by the term

(Def. 14) (the categorical product of c_1 and $c_2)_{\mathbf{2},3}$.

The functor $\pi_2(c_1 \boxtimes c_2)$ yielding a morphism from $c_1 \times c_2$ to c_2 is defined by the term

(Def. 15) (the categorical product of c_1 and $c_2)_{\mathbf{3},3}$.

Now we state the propositions:

(42) Let us consider a category $\mathscr{C}$ with binary products, and objects a, b of $\mathscr{C}$. Then

(i) $\langle a \times b, \pi_1(a \boxtimes b), \pi_2(a \boxtimes b) \rangle$ is a product of a and b, and

(ii) $\hom(a \times b, a) \neq \emptyset$, and

(iii) $\hom(a \times b, b) \neq \emptyset$.

(43) Let us consider a category $\mathscr{C}$ with binary products, and objects a, b, c of $\mathscr{C}$. Suppose $\hom(c, a) \neq \emptyset$ and $\hom(c, b) \neq \emptyset$. Then $\hom(c, a \times b) \neq \emptyset$. The theorem is a consequence of (42).

(44) Let us consider a category $\mathscr{C}$ with binary products, and objects a, b, c, d of $\mathscr{C}$. Suppose $\hom(a, b) \neq \emptyset$ and $\hom(c, d) \neq \emptyset$. Then $\hom(a \times c, b \times d) \neq \emptyset$. The theorem is a consequence of (42).

Let $\mathscr{C}$ be a category with binary products, a, b, c, d be objects of $\mathscr{C}$, and f be a morphism from a to b. Assume $\hom(a, b) \neq \emptyset$. Let g be a morphism from c to d. Assume $\hom(c, d) \neq \emptyset$. The functor $f \times g$ yielding a morphism from $a \times c$ to $b \times d$ is defined by

(Def. 16) $f \cdot \pi_1(a \boxtimes c) = \pi_1(b \boxtimes d) \cdot it$ and $g \cdot \pi_2(a \boxtimes c) = \pi_2(b \boxtimes d) \cdot it$.

Let $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{D}$ be categories and $\mathcal{P}_1$ be a functor from $\mathscr{D}$ to $\mathscr{C}_1$. Assume $\mathcal{P}_1$ is covariant. Let $\mathcal{P}_2$ be a functor from $\mathscr{D}$ to $\mathscr{C}_2$. Assume $\mathcal{P}_2$ is covariant. We say that $\langle \mathscr{D}, \mathcal{P}_1, \mathcal{P}_2 \rangle$ is a product of $\mathscr{C}_1$ and $\mathscr{C}_2$ if and only if

(Def. 17) for every category $\mathscr{D}_1$ and for every functor $\mathcal{G}_1$ from $\mathscr{D}_1$ to $\mathscr{C}_1$ and for every functor $\mathcal{G}_2$ from $\mathscr{D}_1$ to $\mathscr{C}_2$ such that $\mathcal{G}_1$ is covariant and $\mathcal{G}_2$ is covariant there exists a functor $\mathcal{H}$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{H}$ is covariant and $\mathcal{P}_1 \circ \mathcal{H} = \mathcal{G}_1$ and $\mathcal{P}_2 \circ \mathcal{H} = \mathcal{G}_2$ and for every functor $\mathcal{H}_1$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{H}_1$ is covariant and $\mathcal{P}_1 \circ \mathcal{H}_1 = \mathcal{G}_1$ and $\mathcal{P}_2 \circ \mathcal{H}_1 = \mathcal{G}_2$ holds $\mathcal{H} = \mathcal{H}_1$.

Now we state the propositions:

(45) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{A}$, $\mathscr{B}$, a functor $\mathcal{P}_1$ from $\mathscr{A}$ to $\mathscr{C}_1$, a functor $\mathcal{P}_2$ from $\mathscr{A}$ to $\mathscr{C}_2$, a functor $\mathcal{Q}_1$ from $\mathscr{B}$ to $\mathscr{C}_1$, and a functor $\mathcal{Q}_2$ from $\mathscr{B}$ to $\mathscr{C}_2$. Suppose $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\mathcal{Q}_1$ is covariant and $\mathcal{Q}_2$ is covariant and $\langle \mathscr{A}, \mathcal{P}_1, \mathcal{P}_2 \rangle$ is a product of $\mathscr{C}_1$ and $\mathscr{C}_2$ and $\langle \mathscr{B}, \mathcal{Q}_1, \mathcal{Q}_2 \rangle$ is a product of $\mathscr{C}_1$ and $\mathscr{C}_2$. Then $\mathscr{A} \cong \mathscr{B}$.
PROOF: There exists a functor $\mathcal{F}_4$ from $\mathscr{A}$ to $\mathscr{B}$ and there exists a functor $\mathcal{G}_3$ from $\mathscr{B}$ to $\mathscr{A}$ such that $\mathcal{F}_4$ is covariant and $\mathcal{G}_3$ is covariant and $\mathcal{G}_3 \circ \mathcal{F}_4 = \mathrm{id}_{\mathscr{A}}$ and $\mathcal{F}_4 \circ \mathcal{G}_3 = \mathrm{id}_{\mathscr{B}}$ by [16, (10), (11)], [15, (35)]. □

(46) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{D}$, a functor $\mathcal{P}_1$ from $\mathscr{D}$ to $\mathscr{C}_1$, and a functor $\mathcal{P}_2$ from $\mathscr{D}$ to $\mathscr{C}_2$. Suppose $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\langle \mathscr{D}, \mathcal{P}_1, \mathcal{P}_2 \rangle$ is a product of $\mathscr{C}_1$ and $\mathscr{C}_2$. Then $\langle \mathscr{D}, \mathcal{P}_2, \mathcal{P}_1 \rangle$ is a product of $\mathscr{C}_2$ and $\mathscr{C}_1$.

Let $\mathscr{C}$, $\mathscr{C}_1$, $\mathscr{C}_2$ be categories, $\mathcal{F}_1$ be a functor from $\mathscr{C}_1$ to $\mathscr{C}$, and $\mathcal{F}_2$ be a functor from $\mathscr{C}_2$ to $\mathscr{C}$. We introduce the notation $\mathcal{F}_1 \boxtimes \mathcal{F}_2$ as a synonym of $[\![\mathcal{F}_1, \mathcal{F}_2]\!]$.

Now we state the proposition:

(47) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$. Then $\langle \mathscr{C}_1 \to \mathbf{1} \boxtimes \mathscr{C}_2 \to \mathbf{1}, \pi_1((\mathscr{C}_1 \to \mathbf{1}) \boxtimes (\mathscr{C}_2 \to \mathbf{1})), \pi_2((\mathscr{C}_1 \to \mathbf{1}) \boxtimes (\mathscr{C}_2 \to \mathbf{1})) \rangle$ is a product of $\mathscr{C}_1$ and $\mathscr{C}_2$.
PROOF: Set $\mathcal{F}_1 = \mathscr{C}_1 \to \mathbf{1}$. Set $\mathcal{F}_2 = \mathscr{C}_2 \to \mathbf{1}$. For every category $\mathscr{D}_1$ and for every functor $\mathcal{G}_1$ from $\mathscr{D}_1$ to $\mathscr{C}_1$ and for every functor $\mathcal{G}_2$ from $\mathscr{D}_1$ to $\mathscr{C}_2$ such that $\mathcal{G}_1$ is covariant and $\mathcal{G}_2$ is covariant there exists a functor $\mathcal{H}$ from $\mathscr{D}_1$ to $\mathcal{F}_1 \boxtimes \mathcal{F}_2$ such that $\mathcal{H}$ is covariant and $\pi_1(\mathcal{F}_1 \boxtimes \mathcal{F}_2) \circ \mathcal{H} = \mathcal{G}_1$ and

$\pi_2(\mathcal{F}_1 \boxtimes \mathcal{F}_2) \circ \mathcal{H} = \mathcal{G}_2$ and for every functor $\mathcal{H}_1$ from $\mathscr{D}_1$ to $\mathcal{F}_1 \boxtimes \mathcal{F}_2$ such that $\mathcal{H}_1$ is covariant and $\pi_1(\mathcal{F}_1 \boxtimes \mathcal{F}_2) \circ \mathcal{H}_1 = \mathcal{G}_1$ and $\pi_2(\mathcal{F}_1 \boxtimes \mathcal{F}_2) \circ \mathcal{H}_1 = \mathcal{G}_2$ holds $\mathcal{H} = \mathcal{H}_1$ by [16, (52)], (29). □

Let $\mathscr{C}_1$, $\mathscr{C}_2$ be categories.

A categorical product of $\mathscr{C}_1$ and $\mathscr{C}_2$ is a triple object and is defined by

(Def. 18) there exists a strict category $\mathscr{D}$ and there exists a functor $\mathcal{P}_1$ from $\mathscr{D}$ to $\mathscr{C}_1$ and there exists a functor $\mathcal{P}_2$ from $\mathscr{D}$ to $\mathscr{C}_2$ such that *it* $= \langle\mathscr{D}, \mathcal{P}_1, \mathcal{P}_2\rangle$ and $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\langle\mathscr{D}, \mathcal{P}_1, \mathcal{P}_2\rangle$ is a product of $\mathscr{C}_1$ and $\mathscr{C}_2$.

The functor $\mathscr{C}_1 \times \mathscr{C}_2$ yielding a strict category is defined by the term

(Def. 19) (the categorical product of $\mathscr{C}_1$ and $\mathscr{C}_2)_{\mathbf{1},3}$.

The functor $\pi_1(\mathscr{C}_1 \boxtimes \mathscr{C}_2)$ yielding a functor from $\mathscr{C}_1 \times \mathscr{C}_2$ to $\mathscr{C}_1$ is defined by the term

(Def. 20) (the categorical product of $\mathscr{C}_1$ and $\mathscr{C}_2)_{\mathbf{2},3}$.

The functor $\pi_2(\mathscr{C}_1 \boxtimes \mathscr{C}_2)$ yielding a functor from $\mathscr{C}_1 \times \mathscr{C}_2$ to $\mathscr{C}_2$ is defined by the term

(Def. 21) (the categorical product of $\mathscr{C}_1$ and $\mathscr{C}_2)_{\mathbf{3},3}$.

Now we state the proposition:

(48) Let us consider categories $\mathscr{C}_1, \mathscr{C}_2$. Then $\langle\mathscr{C}_1 \times \mathscr{C}_2, \pi_1(\mathscr{C}_1 \boxtimes \mathscr{C}_2), \pi_2(\mathscr{C}_1 \boxtimes \mathscr{C}_2)\rangle$ is a product of $\mathscr{C}_1$ and $\mathscr{C}_2$.

Let $\mathscr{C}_1$, $\mathscr{C}_2$ be categories. Note that $\pi_1(\mathscr{C}_1 \boxtimes \mathscr{C}_2)$ is covariant and $\pi_2(\mathscr{C}_1 \boxtimes \mathscr{C}_2)$ is covariant.

Now we state the proposition:

(49) Let us consider categories $\mathscr{C}_1, \mathscr{C}_2$. Then $\mathscr{C}_1 \times \mathscr{C}_2$ is not empty if and only if $\mathscr{C}_1$ is not empty and $\mathscr{C}_2$ is not empty. The theorem is a consequence of (48).

Let $\mathscr{C}_1$ be an empty category and $\mathscr{C}_2$ be a category. One can verify that $\mathscr{C}_1 \times \mathscr{C}_2$ is empty.

Let $\mathscr{C}_1$ be a category and $\mathscr{C}_2$ be an empty category. Observe that $\mathscr{C}_1 \times \mathscr{C}_2$ is empty.

Let $\mathscr{C}_1$ be a non empty category and $\mathscr{C}_2$ be a non empty category. One can verify that $\mathscr{C}_1 \times \mathscr{C}_2$ is non empty.

Let $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{D}_1$, $\mathscr{D}_2$ be categories, $\mathcal{F}_1$ be a functor from $\mathscr{C}_1$ to $\mathscr{D}_1$, and $\mathcal{F}_2$ be a functor from $\mathscr{C}_2$ to $\mathscr{D}_2$. Assume $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant. The functor $\mathcal{F}_1 \times \mathcal{F}_2$ yielding a functor from $\mathscr{C}_1 \times \mathscr{C}_2$ to $\mathscr{D}_1 \times \mathscr{D}_2$ is defined by

(Def. 22) *it* is covariant and $\mathcal{F}_1 \circ \pi_1(\mathscr{C}_1 \boxtimes \mathscr{C}_2) = \pi_1(\mathscr{D}_1 \boxtimes \mathscr{D}_2) \circ it$ and $\mathcal{F}_2 \circ \pi_2(\mathscr{C}_1 \boxtimes \mathscr{C}_2) = \pi_2(\mathscr{D}_1 \boxtimes \mathscr{D}_2) \circ it$.

Now we state the propositions:

(50) Let us consider categories $\mathscr{A}_1$, $\mathscr{A}_2$, $\mathscr{B}_1$, $\mathscr{B}_2$, $\mathscr{C}_1$, $\mathscr{C}_2$, a functor $\mathcal{F}_1$ from $\mathscr{A}_1$ to $\mathscr{B}_1$, a functor $\mathcal{F}_2$ from $\mathscr{A}_2$ to $\mathscr{B}_2$, a functor $\mathcal{G}_1$ from $\mathscr{B}_1$ to $\mathscr{C}_1$, and a functor $\mathcal{G}_2$ from $\mathscr{B}_2$ to $\mathscr{C}_2$. Suppose $\mathcal{F}_1$ is covariant and $\mathcal{G}_1$ is covariant and $\mathcal{F}_2$ is covariant and $\mathcal{G}_2$ is covariant. Then $(\mathcal{G}_1 \times \mathcal{G}_2) \circ (\mathcal{F}_1 \times \mathcal{F}_2) = (\mathcal{G}_1 \circ \mathcal{F}_1) \times (\mathcal{G}_2 \circ \mathcal{F}_2)$.

(51) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$. Then $\mathrm{id}_{\mathscr{C}_1} \times \mathrm{id}_{\mathscr{C}_2} = \mathrm{id}_{\mathscr{C}_1 \times \mathscr{C}_2}$.

Let x, y be objects. We introduce the notation KuratowskiPair(x, y) as a synonym of $\langle x, y \rangle$.

Let $\mathscr{C}_1$, $\mathscr{C}_2$ be categories, f_1 be a morphism of $\mathscr{C}_1$, and f_2 be a morphism of $\mathscr{C}_2$. The functor $\langle f_1, f_2 \rangle$ yielding a morphism of $\mathscr{C}_1 \times \mathscr{C}_2$ is defined by

(Def. 23) (i) $\pi_1(\mathscr{C}_1 \boxtimes \mathscr{C}_2)(it) = f_1$ and $\pi_2(\mathscr{C}_1 \boxtimes \mathscr{C}_2)(it) = f_2$, **if** $\mathscr{C}_1$ is not empty and $\mathscr{C}_2$ is not empty,

(ii) $it =$ the morphism of $\mathscr{C}_1 \times \mathscr{C}_2$, **otherwise**.

Now we state the propositions:

(52) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$, and a morphism f of $\mathscr{C}_1 \times \mathscr{C}_2$. Then there exists a morphism f_1 of $\mathscr{C}_1$ and there exists a morphism f_2 of $\mathscr{C}_2$ such that $f = \langle f_1, f_2 \rangle$.

(53) Let us consider non empty categories $\mathscr{C}_1$, $\mathscr{C}_2$, morphisms f_1, g_1 of $\mathscr{C}_1$, and morphisms f_2, g_2 of $\mathscr{C}_2$. Suppose $\langle f_1, f_2 \rangle = \langle g_1, g_2 \rangle$. Then

(i) $f_1 = g_1$, and

(ii) $f_2 = g_2$.

Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$, morphisms f_1, g_1 of $\mathscr{C}_1$, and morphisms f_2, g_2 of $\mathscr{C}_2$. Now we state the propositions:

(54) $\langle f_1, f_2 \rangle \triangleright \langle g_1, g_2 \rangle$ if and only if $f_1 \triangleright g_1$ and $f_2 \triangleright g_2$.

(55) Suppose $f_1 \triangleright g_1$ and $f_2 \triangleright g_2$. Then $\langle f_1, f_2 \rangle \circ \langle g_1, g_2 \rangle = \langle f_1 \circ g_1, f_2 \circ g_2 \rangle$. The theorem is a consequence of (54) and (13).

Now we state the propositions:

(56) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$, a morphism f_1 of $\mathscr{C}_1$, a morphism f_2 of $\mathscr{C}_2$, and a morphism f of $\mathscr{C}_1 \times \mathscr{C}_2$. Suppose $f = \langle f_1, f_2 \rangle$ and $\mathscr{C}_1$ is not empty and $\mathscr{C}_2$ is not empty. Then f is identity if and only if f_1 is identity and f_2 is identity. The theorem is a consequence of (52), (54), (55), and (4).

(57) Let us consider non empty categories $\mathscr{C}_1$, $\mathscr{C}_2$, categories $\mathscr{D}_1$, $\mathscr{D}_2$, a functor $\mathcal{F}_1$ from $\mathscr{C}_1$ to $\mathscr{D}_1$, a functor $\mathcal{F}_2$ from $\mathscr{C}_2$ to $\mathscr{D}_2$, a morphism c_1 of $\mathscr{C}_1$, and a morphism c_2 of $\mathscr{C}_2$. Suppose $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant. Then $(\mathcal{F}_1 \times \mathcal{F}_2)(\langle c_1, c_2 \rangle) = \langle \mathcal{F}_1(c_1), \mathcal{F}_2(c_2) \rangle$.

5. NATURAL TRANSFORMATIONS

Let $\mathscr{C}_1$, $\mathscr{C}_2$ be categories, $\mathcal{F}_1$, $\mathcal{F}_2$ be functors from $\mathscr{C}_1$ to $\mathscr{C}_2$, and τ be a functor from $\mathscr{C}_1$ to $\mathscr{C}_2$. We say that τ is a natural transformation of $\mathcal{F}_1$ and $\mathcal{F}_2$ if and only if

(Def. 24) for every morphisms f_1, f_2 of $\mathscr{C}_1$ such that $f_1 \triangleright f_2$ holds $\tau(f_1) \triangleright \mathcal{F}_1(f_2)$ and $\mathcal{F}_2(f_1) \triangleright \tau(f_2)$ and $\tau(f_1 \circ f_2) = \tau(f_1) \circ \mathcal{F}_1(f_2)$ and $\tau(f_1 \circ f_2) = \mathcal{F}_2(f_1) \circ \tau(f_2)$.

Now we state the propositions:

(58) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$, functors $\mathcal{F}_1$, $\mathcal{F}_2$ from $\mathscr{C}_1$ to $\mathscr{C}_2$, and a functor τ from $\mathscr{C}_1$ to $\mathscr{C}_2$. Suppose $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant. Then τ is a natural transformation of $\mathcal{F}_1$ and $\mathcal{F}_2$ if and only if for every morphisms f, f_1, f_2 of $\mathscr{C}_1$ such that f_1 is identity and f_2 is identity and $f_1 \triangleright f$ and $f \triangleright f_2$ holds $\tau(f_1) \triangleright \mathcal{F}_1(f)$ and $\mathcal{F}_2(f) \triangleright \tau(f_2)$ and $\tau(f) = \tau(f_1) \circ \mathcal{F}_1(f)$ and $\tau(f) = \mathcal{F}_2(f) \circ \tau(f_2)$.

PROOF: For every morphisms g_1, g_2 of $\mathscr{C}_1$ such that $g_1 \triangleright g_2$ holds $\tau(g_1) \triangleright \mathcal{F}_1(g_2)$ and $\mathcal{F}_2(g_1) \triangleright \tau(g_2)$ and $\tau(g_1 \circ g_2) = \tau(g_1) \circ \mathcal{F}_1(g_2)$ and $\tau(g_1 \circ g_2) = \mathcal{F}_2(g_1) \circ \tau(g_2)$ by [15, (1)], (5), (3), (13). □

(59) Let us consider non empty categories $\mathscr{C}_1$, $\mathscr{C}_2$, covariant functors $\mathcal{F}_1$, $\mathcal{F}_2$ from $\mathscr{C}_1$ to $\mathscr{C}_2$, and a function τ from $\mathrm{Ob}\,\mathscr{C}_1$ into $\mathrm{Mor}\,\mathscr{C}_2$. Then there exists a functor τ_1 from $\mathscr{C}_1$ to $\mathscr{C}_2$ such that $\tau = \tau_1 \restriction \mathrm{Ob}\,\mathscr{C}_1$ and τ_1 is a natural transformation of $\mathcal{F}_1$ and $\mathcal{F}_2$ if and only if for every object a of $\mathscr{C}_1$, $\tau(a) \in \hom(\mathcal{F}_1(a), \mathcal{F}_2(a))$ and for every objects a_1, a_2 of $\mathscr{C}_1$ and for every morphism f from a_1 to a_2 such that $\hom(a_1, a_2) \neq \emptyset$ holds $\tau(a_2) \circ \mathcal{F}_1(f) = \mathcal{F}_2(f) \circ \tau(a_1)$.

PROOF: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ for every morphism f of $\mathscr{C}_1$ such that $\$_1 = f$ holds $\$_2 = \tau(\mathrm{cod}\, f) \circ \mathcal{F}_1(f)$. For every object x such that $x \in$ the carrier of $\mathscr{C}_1$ there exists an object y such that $y \in$ the carrier of $\mathscr{C}_2$ and $\mathcal{P}[x, y]$. Consider τ_1 being a function from the carrier of $\mathscr{C}_1$ into the carrier of $\mathscr{C}_2$ such that for every object x such that $x \in$ the carrier of $\mathscr{C}_1$ holds $\mathcal{P}[x, \tau_1(x)]$ from [7, Sch. 1]. For every object x such that $x \in \mathrm{dom}\,\tau$ holds $\tau(x) = (\tau_1 \restriction \mathrm{Ob}\,\mathscr{C}_1)(x)$ by [15, (22)], [16, (20)], [15, (32)], [16, (5), (6)]. For every morphisms f, f_1, f_2 of $\mathscr{C}_1$ such that f_1 is identity and f_2 is identity and $f_1 \triangleright f$ and $f \triangleright f_2$ holds $\tau_1(f_1) \triangleright \mathcal{F}_1(f)$ and $\mathcal{F}_2(f) \triangleright \tau_1(f_2)$ and $\tau_1(f) = \tau_1(f_1) \circ \mathcal{F}_1(f)$ and $\tau_1(f) = \mathcal{F}_2(f) \circ \tau_1(f_2)$ by [15, (22)], [16, (20), (6)], [15, (32)]. □

(60) Let us consider object-categories $\mathscr{C}$, $\mathscr{D}$, functors $\mathcal{F}_1$, $\mathcal{F}_2$ from $\mathscr{C}$ to $\mathscr{D}$, and functors $\mathcal{G}_1$, $\mathcal{G}_2$, τ from alter $\mathscr{C}$ to alter $\mathscr{D}$. Suppose $\mathcal{F}_1 = \mathcal{G}_1$ and $\mathcal{F}_2 = \mathcal{G}_2$ and τ is a natural transformation of $\mathcal{G}_1$ and $\mathcal{G}_2$. Then $(\mathrm{IdMap}\,\mathscr{C}) \cdot \tau$ is a natural transformation from $\mathcal{F}_1$ to $\mathcal{F}_2$.

Proof: For every object a of $\mathscr{C}$, $\tau(\mathrm{id}_a) \in \hom(\mathcal{F}_1(a), \mathcal{F}_2(a))$ by [15, (41), (24), (42)]. Reconsider $\tau_1 = \tau$ as a function from the carrier' of $\mathscr{C}$ into the carrier' of $\mathscr{D}$. There exists a transformation t from $\mathcal{F}_1$ to $\mathcal{F}_2$ such that $t = (\mathrm{IdMap}\,\mathscr{C}) \cdot \tau_1$ and for every objects a, b of $\mathscr{C}$ such that $\hom(a, b) \neq \emptyset$ for every morphism f from a to b, $t(b) \cdot \mathcal{F}_{1f} = \mathcal{F}_{2f} \cdot t(a)$ by [6, (13)], [5, (1), (15), (21)]. Consider t being a transformation from $\mathcal{F}_1$ to $\mathcal{F}_2$ such that $t = (\mathrm{IdMap}\,\mathscr{C}) \cdot \tau_1$ and for every objects a, b of $\mathscr{C}$ such that $\hom(a, b) \neq \emptyset$ for every morphism f from a to b, $t(b) \cdot \mathcal{F}_{1f} = \mathcal{F}_{2f} \cdot t(a)$. □

Let $\mathscr{C}$, $\mathscr{D}$ be categories and $\mathcal{F}_1$, $\mathcal{F}_2$ be functors from $\mathscr{C}$ to $\mathscr{D}$. We say that $\mathcal{F}_1$ is naturally transformable to $\mathcal{F}_2$ if and only if

(Def. 25) there exists a functor τ from $\mathscr{C}$ to $\mathscr{D}$ such that τ is a natural transformation of $\mathcal{F}_1$ and $\mathcal{F}_2$.

Assume $\mathcal{F}_1$ is naturally transformable to $\mathcal{F}_2$.

A natural transformation from $\mathcal{F}_1$ to $\mathcal{F}_2$ is a functor from $\mathscr{C}$ to $\mathscr{D}$ and is defined by

(Def. 26) *it* is a natural transformation of $\mathcal{F}_1$ and $\mathcal{F}_2$.

Now we state the proposition:

(61) Let us consider categories $\mathscr{C}$, $\mathscr{D}$, and a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$. Suppose $\mathcal{F}$ is covariant. Then $\mathcal{F}$ is a natural transformation of $\mathcal{F}$ and $\mathcal{F}$. The theorem is a consequence of (58).

Let $\mathscr{C}$, $\mathscr{D}$ be categories and $\mathcal{F}$, $\mathcal{F}_1$, $\mathcal{F}_2$ be functors from $\mathscr{C}$ to $\mathscr{D}$. Assume $\mathcal{F}_1$ is naturally transformable to $\mathcal{F}$ and $\mathcal{F}$ is naturally transformable to $\mathcal{F}_2$ and $\mathcal{F}$ is covariant and $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant. Let τ_1 be a natural transformation from $\mathcal{F}_1$ to $\mathcal{F}$ and τ_2 be a natural transformation from $\mathcal{F}$ to $\mathcal{F}_2$. The functor $\tau_2 \circ \tau_1$ yielding a natural transformation from $\mathcal{F}_1$ to $\mathcal{F}_2$ is defined by

(Def. 27) for every morphisms f, f_1, f_2 of $\mathscr{C}$ such that f_1 is identity and f_2 is identity and $f \triangleright f_1$ and $f_2 \triangleright f$ holds $it(f) = (\tau_2(f_2) \circ \mathcal{F}(f)) \circ \tau_1(f_1)$.

Now we state the proposition:

(62) Let us consider categories $\mathscr{C}$, $\mathscr{D}$, and functors $\mathcal{F}$, $\mathcal{F}_1$, $\mathcal{F}_2$ from $\mathscr{C}$ to $\mathscr{D}$. Suppose $\mathcal{F}_1$ is naturally transformable to $\mathcal{F}$ and $\mathcal{F}$ is naturally transformable to $\mathcal{F}_2$ and covariant and $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant. Then $\mathcal{F}_1$ is naturally transformable to $\mathcal{F}_2$.

Let $\mathscr{C}_1$, $\mathscr{C}_2$ be categories. The functor $\mathrm{Functors}(\mathscr{C}_2, \mathscr{C}_1)$ yielding a strict category is defined by

(Def. 28) the carrier of $it = \{\langle\langle \mathcal{F}_1, \mathcal{F}_2\rangle, \tau\rangle$, where $\mathcal{F}_1, \mathcal{F}_2$ are functors from $\mathscr{C}_1$ to $\mathscr{C}_2, \tau$ is a natural transformation from $\mathcal{F}_1$ to $\mathcal{F}_2$: $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant and $\mathcal{F}_1$ is naturally transformable to $\mathcal{F}_2\}$ and the composition of $it = \{\langle\langle x_2, x_1\rangle, x_3\rangle$, where x_1, x_2, x_3 are elements of the carrier of it : there exist functors $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ from $\mathscr{C}_1$ to $\mathscr{C}_2$ and there exists a natural transformation τ_1 from $\mathcal{F}_1$ to $\mathcal{F}_2$ and there exists a natural transformati-on τ_2 from $\mathcal{F}_2$ to $\mathcal{F}_3$ such that $x_1 = \langle\langle \mathcal{F}_1, \mathcal{F}_2\rangle, \tau_1\rangle$ and $x_2 = \langle\langle \mathcal{F}_2, \mathcal{F}_3\rangle, \tau_2\rangle$ and $x_3 = \langle\langle \mathcal{F}_1, \mathcal{F}_3\rangle, \tau_2 \circ \tau_1\rangle\}$.

Let $\mathscr{C}_1$ be a non empty category and $\mathscr{C}_2$ be an empty category. One can verify that Functors($\mathscr{C}_2, \mathscr{C}_1$) is empty.

Let $\mathscr{C}_1$ be an empty category and $\mathscr{C}_2$ be a category. Let us observe that Functors($\mathscr{C}_2, \mathscr{C}_1$) is non empty and trivial.

Let $\mathscr{C}_1$ be a non empty category and $\mathscr{C}_2$ be a non empty category. Let us note that Functors($\mathscr{C}_2, \mathscr{C}_1$) is non empty.

Now we state the proposition:

(63) Let us consider non empty categories $\mathscr{C}_1$, $\mathscr{C}_2$, and morphisms f_1, f_2 of Functors($\mathscr{C}_2, \mathscr{C}_1$). Then $f_1 \triangleright f_2$ if and only if there exist covariant functors $\mathcal{F}$, $\mathcal{F}_1$, $\mathcal{F}_2$ from $\mathscr{C}_1$ to $\mathscr{C}_2$ and there exists a natural transformation τ_1 from $\mathcal{F}_1$ to $\mathcal{F}$ and there exists a natural transformation τ_2 from $\mathcal{F}$ to $\mathcal{F}_2$ such that $f_1 = \langle\langle \mathcal{F}, \mathcal{F}_2\rangle, \tau_2\rangle$ and $f_2 = \langle\langle \mathcal{F}_1, \mathcal{F}\rangle, \tau_1\rangle$ and $f_1 \circ f_2 = \langle\langle \mathcal{F}_1, \mathcal{F}_2\rangle, \tau_2 \circ \tau_1\rangle$ and for every morphisms g_1, g_2 of $\mathscr{C}_1$ such that $g_2 \triangleright g_1$ holds $\tau_2(g_2) \triangleright \tau_1(g_1)$ and $(\tau_2 \circ \tau_1)(g_2 \circ g_1) = \tau_2(g_2) \circ \tau_1(g_1)$.

Proof: If $f_1 \triangleright f_2$, then there exist covariant functors $\mathcal{F}$, $\mathcal{F}_1$, $\mathcal{F}_2$ from $\mathscr{C}_1$ to $\mathscr{C}_2$ and there exists a natural transformation τ_1 from $\mathcal{F}_1$ to $\mathcal{F}$ and there exists a natural transformation τ_2 from $\mathcal{F}$ to $\mathcal{F}_2$ such that $f_1 = \langle\langle \mathcal{F}, \mathcal{F}_2\rangle, \tau_2\rangle$ and $f_2 = \langle\langle \mathcal{F}_1, \mathcal{F}\rangle, \tau_1\rangle$ and $f_1 \circ f_2 = \langle\langle \mathcal{F}_1, \mathcal{F}_2\rangle, \tau_2 \circ \tau_1\rangle$ and for every morphisms g_1, g_2 of $\mathscr{C}_1$ such that $g_2 \triangleright g_1$ holds $\tau_2(g_2) \triangleright \tau_1(g_1)$ and $(\tau_2 \circ \tau_1)(g_2 \circ g_1) = \tau_2(g_2) \circ \tau_1(g_1)$ by [6, (1)], (5), (58), [16, (5)]. □

Let us consider non empty categories $\mathscr{C}_1, \mathscr{C}_2$ and a morphism f of Functors($\mathscr{C}_2$, $\mathscr{C}_1$). Now we state the propositions:

(64) f is identity if and only if there exists a covariant functor $\mathcal{F}$ from $\mathscr{C}_1$ to $\mathscr{C}_2$ such that $f = \langle\langle \mathcal{F}, \mathcal{F}\rangle, \mathcal{F}\rangle$.

Proof: Set $\mathscr{C} =$ Functors($\mathscr{C}_2, \mathscr{C}_1$). If f is identity, then there exists a covariant functor $\mathcal{F}$ from $\mathscr{C}_1$ to $\mathscr{C}_2$ such that $f = \langle\langle \mathcal{F}, \mathcal{F}\rangle, \mathcal{F}\rangle$ by [15, (24)], (63), (61), (5). Consider $\mathcal{F}$ being a covariant functor from $\mathscr{C}_1$ to $\mathscr{C}_2$ such that $f = \langle\langle \mathcal{F}, \mathcal{F}\rangle, \mathcal{F}\rangle$. For every morphism f_1 of $\mathscr{C}$ such that $f \triangleright f_1$ holds $f \circ f_1 = f_1$ by (63), (5), (4), [7, (12)]. □

(65) There exist covariant functors $\mathcal{F}_1$, $\mathcal{F}_2$ from $\mathscr{C}_1$ to $\mathscr{C}_2$ and there exists a natural transformation τ from $\mathcal{F}_1$ to $\mathcal{F}_2$ such that $f = \langle\langle \mathcal{F}_1, \mathcal{F}_2\rangle, \tau\rangle$ and $\operatorname{dom} f = \langle\langle \mathcal{F}_1, \mathcal{F}_1\rangle, \mathcal{F}_1\rangle$ and $\operatorname{cod} f = \langle\langle \mathcal{F}_2, \mathcal{F}_2\rangle, \mathcal{F}_2\rangle$. The theorem is a consequence of (63) and (64).

6. Exponential Objects

Let $\mathscr{C}$ be a category with binary products, a, b, c be objects of $\mathscr{C}$, and e be a morphism from $c \times a$ to b. Assume $\hom(c \times a, b) \neq \emptyset$. We say that $\langle c, e\rangle$ is an exponent of a and b if and only if

(Def. 29) for every object d of $\mathscr{C}$ and for every morphism f from $d \times a$ to b such that $\hom(d \times a, b) \neq \emptyset$ holds $\hom(d, c) \neq \emptyset$ and there exists a morphism h from d to c such that $f = e \cdot (h \times \text{id-}a)$ and for every morphism h_1 from d to c such that $f = e \cdot (h_1 \times \text{id-}a)$ holds $h = h_1$.

Now we state the propositions:

(66) Let us consider a category $\mathscr{C}$ with binary products, objects a_1, a_2, b_1, b_2, c_1, c_2 of $\mathscr{C}$, a morphism f_1 from a_1 to b_1, a morphism f_2 from a_2 to b_2, a morphism g_1 from b_1 to c_1, and a morphism g_2 from b_2 to c_2. Suppose $\hom(a_1, b_1) \neq \emptyset$ and $\hom(b_1, c_1) \neq \emptyset$ and $\hom(a_2, b_2) \neq \emptyset$ and $\hom(b_2, c_2) \neq \emptyset$. Then $(g_1 \times g_2) \cdot (f_1 \times f_2) = g_1 \cdot f_1 \times (g_2 \cdot f_2)$. The theorem is a consequence of (42) and (44).

(67) Let us consider a category $\mathscr{C}$ with binary products, and objects a, b of $\mathscr{C}$. Then $\text{id-}a \times \text{id-}b = \text{id-}(a \times b)$. The theorem is a consequence of (42).

(68) Let us consider a category $\mathscr{C}$ with binary products, objects a, b, c_1, c_2 of $\mathscr{C}$, a morphism e_1 from $c_1 \times a$ to b, and a morphism e_2 from $c_2 \times a$ to b. Suppose $\hom(c_1 \times a, b) \neq \emptyset$ and $\hom(c_2 \times a, b) \neq \emptyset$ and $\langle c_1, e_1\rangle$ is an exponent of a and b and $\langle c_2, e_2\rangle$ is an exponent of a and b. Then c_1 and c_2 are isomorphic.

Proof: There exists a morphism f from c_1 to c_2 such that f is isomorphism by (44), [16, (23)], (66), [16, (18)]. □

Let $\mathscr{C}$ be a category with binary products. We say that $\mathscr{C}$ has exponential objects if and only if

(Def. 30) for every objects a, b of $\mathscr{C}$, there exists an object c of $\mathscr{C}$ and there exists a morphism e from $c \times a$ to b such that $\hom(c \times a, b) \neq \emptyset$ and $\langle c, e\rangle$ is an exponent of a and b.

One can check that $\mathbf{1}$ has binary products.

Now we state the proposition:

(69) $\mathbf{1}$ has exponential objects.

Proof: Set $\mathscr{C} = \mathbf{1}$. Consider f being a morphism of $\mathbf{1}$ such that f is identity and $\text{Ob}\,\mathbf{1} = \{f\}$ and $\text{Mor}\,\mathbf{1} = \{f\}$. For every objects o_1, o_2 of $\mathscr{C}$, every morphism of $\mathscr{C}$ is a morphism from o_1 to o_2 by [16, (20)]. For every objects a, b of $\mathscr{C}$, there exists an object c of $\mathscr{C}$ and there exists a morphism e from $c \times a$ to b such that $\hom(c \times a, b) \neq \emptyset$ and $\langle c, e\rangle$ is an exponent of a and b. □

Let us observe that there exists a category with binary products which has exponential objects.

Let $\mathscr{C}$ be a category with exponential objects binary products and a, b be objects of $\mathscr{C}$.

A categorical exponent of a and b is a pair object and is defined by

(Def. 31) there exists an object c of $\mathscr{C}$ and there exists a morphism e from $c \times a$ to b such that $it = \langle c, e\rangle$ and $\hom(c \times a, b) \neq \emptyset$ and $\langle c, e\rangle$ is an exponent of a and b.

The functor b^a yielding an object of $\mathscr{C}$ is defined by the term

(Def. 32) (the categorical exponent of a and $b)_{\mathbf{1}}$.

The functor $\mathrm{eval}(a, b)$ yielding a morphism from $b^a \times a$ to b is defined by the term

(Def. 33) (the categorical exponent of a and $b)_{\mathbf{2}}$.

Now we state the propositions:

(70) Let us consider a category $\mathscr{C}$ with exponential objects binary products, and objects a, b of $\mathscr{C}$. Then

(i) $\hom(b^a \times a, b) \neq \emptyset$, and

(ii) $\langle b^a, \mathrm{eval}(a, b)\rangle$ is an exponent of a and b.

(71) Let us consider a category $\mathscr{C}$ with exponential objects binary products, and objects a, b, c of $\mathscr{C}$. Suppose $\hom(c \times a, b) \neq \emptyset$. Then there exists a function L from $\hom(c \times a, b)$ into $\hom(c, b^a)$ such that

(i) for every morphism f from $c \times a$ to b and for every morphism h from c to b^a such that $h = L(f)$ holds $\mathrm{eval}(a, b) \cdot (h \times \text{id-}a) = f$, and

(ii) L is bijective.

PROOF: $\hom(b^a \times a, b) \neq \emptyset$ and $\langle b^a, \mathrm{eval}(a, b)\rangle$ is an exponent of a and b. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ for every morphism f from $c \times a$ to b such that $f = \$_1$ there exists a morphism h from c to b^a such that $h = \$_2$ and $f = \mathrm{eval}(a, b) \cdot (h \times \text{id-}a)$ and for every morphism h_1 from c to b^a such that $f = \mathrm{eval}(a, b) \cdot (h_1 \times \text{id-}a)$ holds $h = h_1$. For every object x such that $x \in \hom(c \times a, b)$ there exists an object y such that $y \in \hom(c, b^a)$ and $\mathcal{P}[x, y]$. Consider L being a function from $\hom(c \times a, b)$ into $\hom(c, b^a)$ such that for every object x such that $x \in \hom(c \times a, b)$ holds $\mathcal{P}[x, L(x)]$ from [7, Sch. 1]. There exists an object y such that $y \in \hom(c, b^a)$. For every morphism f from $c \times a$ to b and for every morphism h from c to b^a such that $h = L(f)$ holds $\mathrm{eval}(a, b) \cdot (h \times \text{id-}a) = f$. For every objects x_1, x_2 such that x_1, $x_2 \in \hom(c \times a, b)$ and $L(x_1) = L(x_2)$ holds $x_1 = x_2$. For every object y such that $y \in \hom(c, b^a)$ holds $y \in \mathrm{rng}\, L$ by [6, (3)]. □

Let $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ be categories and $\mathcal{E}$ be a functor from $\mathscr{C} \times \mathscr{A}$ to $\mathscr{B}$. Assume $\mathcal{E}$ is covariant. We say that $\langle \mathscr{C}, \mathcal{E} \rangle$ is an exponent of $\mathscr{A}$ and $\mathscr{B}$ if and only if

(Def. 34) for every category $\mathscr{D}$ and for every functor $\mathcal{F}$ from $\mathscr{D} \times \mathscr{A}$ to $\mathscr{B}$ such that $\mathcal{F}$ is covariant there exists a functor $\mathcal{H}$ from $\mathscr{D}$ to $\mathscr{C}$ such that $\mathcal{H}$ is covariant and $\mathcal{F} = \mathcal{E} \circ (\mathcal{H} \times \mathrm{id}_{\mathscr{A}})$ and for every functor $\mathcal{H}_1$ from $\mathscr{D}$ to $\mathscr{C}$ such that $\mathcal{H}_1$ is covariant and $\mathcal{F} = \mathcal{E} \circ (\mathcal{H}_1 \times \mathrm{id}_{\mathscr{A}})$ holds $\mathcal{H} = \mathcal{H}_1$.

Let $\mathscr{C}_1$, $\mathscr{C}_2$ be categories.

A categorical exponent of $\mathscr{C}_1$ and $\mathscr{C}_2$ is a pair object and is defined by

(Def. 35) there exists a category $\mathscr{C}$ and there exists a functor $\mathcal{E}$ from $\mathscr{C} \times \mathscr{C}_1$ to $\mathscr{C}_2$ such that $it = \langle \mathscr{C}, \mathcal{E} \rangle$ and $\mathcal{E}$ is covariant and $\langle \mathscr{C}, \mathcal{E} \rangle$ is an exponent of $\mathscr{C}_1$ and $\mathscr{C}_2$.

The functor ${\mathscr{C}_2}^{\mathscr{C}_1}$ yielding a category is defined by the term

(Def. 36) (the categorical exponent of $\mathscr{C}_1$ and $\mathscr{C}_2)_{\mathbf{1}}$.

The functor $\mathrm{eval}(\mathscr{C}_1, \mathscr{C}_2)$ yielding a functor from ${\mathscr{C}_2}^{\mathscr{C}_1} \times \mathscr{C}_1$ to $\mathscr{C}_2$ is defined by the term

(Def. 37) (the categorical exponent of $\mathscr{C}_1$ and $\mathscr{C}_2)_{\mathbf{2}}$.

Now we state the propositions:

(72) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$. Then $\langle {\mathscr{C}_2}^{\mathscr{C}_1}, \mathrm{eval}(\mathscr{C}_1, \mathscr{C}_2) \rangle$ is an exponent of $\mathscr{C}_1$ and $\mathscr{C}_2$.

(73) Let us consider categories $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}_1$, $\mathscr{C}_2$, a functor $\mathcal{E}_1$ from $\mathscr{C}_1 \times \mathscr{A}$ to $\mathscr{B}$, and a functor $\mathcal{E}_2$ from $\mathscr{C}_2 \times \mathscr{A}$ to $\mathscr{B}$. Suppose $\mathcal{E}_1$ is covariant and $\mathcal{E}_2$ is covariant and $\langle \mathscr{C}_1, \mathcal{E}_1 \rangle$ is an exponent of $\mathscr{A}$ and $\mathscr{B}$ and $\langle \mathscr{C}_2, \mathcal{E}_2 \rangle$ is an exponent of $\mathscr{A}$ and $\mathscr{B}$. Then $\mathscr{C}_1 \cong \mathscr{C}_2$.

PROOF: There exists a functor $\mathcal{F}$ from $\mathscr{C}_1$ to $\mathscr{C}_2$ and there exists a functor $\mathcal{G}$ from $\mathscr{C}_2$ to $\mathscr{C}_1$ such that $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathcal{G} \circ \mathcal{F} = \mathrm{id}_{\mathscr{C}_1}$ and $\mathcal{F} \circ \mathcal{G} = \mathrm{id}_{\mathscr{C}_2}$ by [16, (10)], (50), [16, (11)], [15, (35)]. □

Let $\mathscr{C}_1$, $\mathscr{C}_2$ be categories. Observe that $\mathrm{eval}(\mathscr{C}_1, \mathscr{C}_2)$ is covariant.

Let $\mathscr{C}_1$ be a non empty category and $\mathscr{C}_2$ be an empty category. Let us note that ${\mathscr{C}_2}^{\mathscr{C}_1}$ is empty.

Let $\mathscr{C}_1$ be an empty category and $\mathscr{C}_2$ be a category. Let us observe that ${\mathscr{C}_2}^{\mathscr{C}_1}$ is non empty and trivial.

Let $\mathscr{C}_1$ be a non empty category and $\mathscr{C}_2$ be a non empty category. One can verify that ${\mathscr{C}_2}^{\mathscr{C}_1}$ is non empty.

Now we state the proposition:

(74) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$. Then $\mathrm{Functors}(\mathscr{C}_2, \mathscr{C}_1) \cong {\mathscr{C}_2}^{\mathscr{C}_1}$. The theorem is a consequence of (28), (72), and (73).

References

[1] Jiri Adamek, Horst Herrlich, and George E. Strecker. *Abstract and Concrete Categories: The Joy of Cats*. Dover Publication, New York, 2009.

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

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

[4] Francis Borceaux. *Handbook of Categorical Algebra I. Basic Category Theory*, volume 50 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1994.

[5] Czesław Byliński. Introduction to categories and functors. *Formalized Mathematics*, 1 (**2**):409–420, 1990.

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

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

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

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

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

[11] Krzysztof Hryniewiecki. Graphs. *Formalized Mathematics*, 2(**3**):365–370, 1991.

[12] F. William Lawvere. Functorial semantics of algebraic theories and some algebraic problems in the context of functorial semantics of algebraic theories. *Reprints in Theory and Applications of Categories*, 5:1–121, 2004.

[13] Saunders Mac Lane. *Categories for the Working Mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer Verlag, New York, Heidelberg, Berlin, 1971.

[14] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[15] Marco Riccardi. Object-free definition of categories. *Formalized Mathematics*, 21(**3**): 193–205, 2013. doi:10.2478/forma-2013-0021.

[16] Marco Riccardi. Categorical pullbacks. *Formalized Mathematics*, 23(**1**):1–14, 2015. doi:10.2478/forma-2015-0001.

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

[18] Andrzej Trybulec. Isomorphisms of categories. *Formalized Mathematics*, 2(**5**):629–634, 1991.

[19] Andrzej Trybulec. Natural transformations. Discrete categories. *Formalized Mathematics*, 2(**4**):467–474, 1991.

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

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

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

Received August 15, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 371–378, 2015
DOI: 10.1515/forma-2015-0029

DE GRUYTER OPEN
degruyter.com/view/j/forma

Algebra of Polynomially Bounded Sequences and Negligible Functions

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In this article we formalize negligible functions that play an essential role in cryptology [10], [2]. Generally, a cryptosystem is secure if the probability of succeeding any attacks against the cryptosystem is negligible. First, we formalize the algebra of polynomially bounded sequences [20]. Next, we formalize negligible functions and prove the set of negligible functions is a subset of the algebra of polynomially bounded sequences. Moreover, we then introduce equivalence relation between polynomially bounded sequences, using negligible functions.

MSC: 68Q25 94A60 03B35

Keywords: polynomially bounded function; negligible functions

MML identifier: `ASYMPT_3`, version: `8.1.04 5.33.1254`

The notation and terminology used in this paper have been introduced in the following articles: [29], [16], [17], [20], [4], [19], [9], [24], [21], [5], [6], [26], [25], [1], [7], [13], [22], [12], [3], [11], [30], [27], [14], [15], [23], [28], [18], and [8].

1. Preliminaries

Let us consider a real number r. Now we state the propositions:

(1) $r < |r| + 1$.

(2) There exists a natural number N such that for every natural number n such that $N \leqslant n$ holds $r < \frac{n}{\log_2 n}$.

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

(3) There exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $x^k < 2^x$. The theorem is a consequence of (2).

ISSN 1426–2630(Print), 1898-9934(Online)

(4) There exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $\frac{1}{2^x} < \frac{1}{x^k}$. The theorem is a consequence of (3).

Now we state the proposition:

(5) Let us consider a natural number z. Suppose $2 \leqslant z$. Let us consider a natural number k. Then there exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $\frac{1}{z^x} < \frac{1}{x^k}$. The theorem is a consequence of (4).

Observe that there exists a finite 0-sequence of $\mathbb{R}$ which is positive yielding and there exists a positive yielding finite 0-sequence of $\mathbb{R}$ which is non empty.

Now we state the proposition:

(6) Let us consider a finite 0-sequence c of $\mathbb{R}$, and a real number a. Then $a \cdot c$ is a finite 0-sequence of $\mathbb{R}$.

Let c be a finite 0-sequence of $\mathbb{R}$ and a be a real number. Observe that $a \cdot c$ is finite as a transfinite sequence of elements of $\mathbb{R}$.

Now we state the proposition:

(7) Let us consider a non empty, positive yielding finite 0-sequence c of $\mathbb{R}$, and a real number a. Suppose $0 < a$. Then $a \cdot c$ is a non empty, positive yielding finite 0-sequence of $\mathbb{R}$. The theorem is a consequence of (6).

Let c be a non empty, positive yielding finite 0-sequence of $\mathbb{R}$ and a be a positive real number. Observe that $a \cdot c$ is non empty and positive yielding as a finite 0-sequence of $\mathbb{R}$.

Let c be a finite 0-sequence of $\mathbb{R}$. We introduce the notation polynom c as a synonym of $\mathrm{Seq}_{\mathrm{poly}}(c)$.

Now we state the propositions:

(8) Let us consider a non empty, positive yielding finite 0-sequence c of $\mathbb{R}$, and a natural number x. Then $0 < (\mathrm{polynom}\, c)(x)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non empty, positive yielding finite 0-sequence c of $\mathbb{R}$ such that $\mathrm{len}\, c = \$_1$ for every natural number x, $0 < (\mathrm{polynom}\, c)(x)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [20, (28), (29)], [1, (44)], [5, (3), (47)]. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 2]. □

(9) Let us consider non empty, positive yielding finite 0-sequences c, c_1 of $\mathbb{R}$, and a real number a. Suppose $c_1 = a \cdot c$. Let us consider a natural number x. Then $(\mathrm{polynom}\, c_1)(x) = a \cdot (\mathrm{polynom}\, c)(x)$.

Proof: For every object i such that $i \in \mathrm{dom}(c_1 \cdot \{x^{1 \cdot n+0}\}_{n \in \mathbb{N}})$ holds $(c_1 \cdot \{x^{1 \cdot n+0}\}_{n \in \mathbb{N}})(i) = (a \cdot (c \cdot \{x^{1 \cdot n+0}\}_{n \in \mathbb{N}}))(i)$ by [20, (26)]. □

2. Algebra of Polynomially Bounded Sequences

Let p be a sequence of real numbers. We say that p is absolutely polynomially bounded if and only if

(Def. 1) there exists a natural number k such that $|p| \in O(\{n^k\}_{n \in \mathbb{N}})$.

One can verify that every sequence of real numbers which is polynomially bounded is also absolutely polynomially bounded.

Now we state the proposition:

(10) Let us consider an element r of $\mathbb{N}$, and a sequence s of real numbers. If $s = \mathbb{N} \longmapsto r$, then s is absolutely polynomially bounded.

One can check that there exists a function from $\mathbb{N}$ into $\mathbb{R}$ which is absolutely polynomially bounded.

Let f, g be absolutely polynomially bounded functions from $\mathbb{N}$ into $\mathbb{R}$. One can verify that $f + g$ is absolutely polynomially bounded as a function from $\mathbb{N}$ into $\mathbb{R}$ and $f \cdot g$ is absolutely polynomially bounded as a function from $\mathbb{N}$ into $\mathbb{R}$.

Let f be an absolutely polynomially bounded function from $\mathbb{N}$ into $\mathbb{R}$ and a be an element of $\mathbb{R}$. Observe that $a \cdot f$ is absolutely polynomially bounded as a function from $\mathbb{N}$ into $\mathbb{R}$.

The functor $\mathcal{O}_{\rm poly}$ yielding a subset of RAlgebra $\mathbb{N}$ is defined by

(Def. 2) for every object x, $x \in it$ iff x is an absolutely polynomially bounded function from $\mathbb{N}$ into $\mathbb{R}$.

Note that $\mathcal{O}_{\rm poly}$ is non empty.

The functor RAlgebra$\mathcal{O}_{\rm poly}$ yielding a strict algebra structure is defined by

(Def. 3) the carrier of $it = \mathcal{O}_{\rm poly}$ and the multiplication of $it = \cdot_{\mathbb{R}^{\mathbb{N}}} \restriction \mathcal{O}_{\rm poly}$ and the addition of $it = +_{\mathbb{R}^{\mathbb{N}}} \restriction \mathcal{O}_{\rm poly}$ and the external multiplication of $it = \cdot^{\mathbb{R}}_{\mathbb{R}^{\mathbb{N}}} \restriction (\mathbb{R} \times \mathcal{O}_{\rm poly})$ and the one of $it = \mathbf{1}_{\mathbb{R}^{\mathbb{N}}}$ and the zero of $it = \mathbf{0}_{\mathbb{R}^{\mathbb{N}}}$.

One can verify that RAlgebra$\mathcal{O}_{\rm poly}$ is non empty.

Now we state the propositions:

(11) The carrier of RAlgebra$\mathcal{O}_{\rm poly} \subseteq$ the carrier of RAlgebra $\mathbb{N}$.

(12) Let us consider an object f. Then $f \in$ RAlgebra$\mathcal{O}_{\rm poly}$ if and only if f is an absolutely polynomially bounded function from $\mathbb{N}$ into $\mathbb{R}$.

Let us consider points f, g of RAlgebra$\mathcal{O}_{\rm poly}$ and points f_1, g_1 of RAlgebra $\mathbb{N}$. Let us assume that $f = f_1$ and $g = g_1$. Now we state the propositions:

(13) $f \cdot g = f_1 \cdot g_1$.

(14) $f + g = f_1 + g_1$.

Now we state the propositions:

(15) Let us consider a point f of RAlgebra$\mathcal{O}_{\rm poly}$, a point f_1 of RAlgebra $\mathbb{N}$, and an element a of $\mathbb{R}$. If $f = f_1$, then $a \cdot f = a \cdot f_1$.

(16) $0_{\rm RAlgebra\mathcal{O}_{poly}} = 0_{\rm RAlgebra\,\mathbb{N}}$.

(17) $1_{\rm RAlgebra\mathcal{O}_{poly}} = 1_{\rm RAlgebra\,\mathbb{N}}$.

One can check that RAlgebra$\mathcal{O}_{\rm poly}$ is strict, Abelian, add-associative, right zeroed, right complementable, commutative, associative, right unital, right distributive, vector associative, scalar associative, vector distributive, and scalar distributive.

Now we state the proposition:

(18) RAlgebra$\mathcal{O}_{\rm poly}$ is an algebra.

Let us consider vectors f, g, h of RAlgebra$\mathcal{O}_{\rm poly}$ and functions f', g', h' from $\mathbb{N}$ into $\mathbb{R}$.

Let us assume that $f' = f$ and $g' = g$ and $h' = h$. Now we state the propositions:

(19) $h = f + g$ if and only if for every natural number x, $h'(x) = f'(x) + g'(x)$. The theorem is a consequence of (11) and (14).

(20) $h = f \cdot g$ if and only if for every natural number x, $h'(x) = f'(x) \cdot g'(x)$. The theorem is a consequence of (11) and (13).

Now we state the proposition:

(21) Let us consider vectors f, h of RAlgebra$\mathcal{O}_{\rm poly}$, and functions f', h' from $\mathbb{N}$ into $\mathbb{R}$. Suppose $f' = f$ and $h' = h$. Let us consider a real number a. Then $h = a \cdot f$ if and only if for every natural number x, $h'(x) = a \cdot f'(x)$. The theorem is a consequence of (11) and (15).

3. Negligible Functions

Definition 1.3.5 of [10], p.16: Let f be a function from $\mathbb{N}$ into $\mathbb{R}$. We say that f is negligible if and only if

(Def. 4) for every non empty, positive yielding finite 0-sequence c of $\mathbb{R}$, there exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $|f(x)| < \frac{1}{(\mathrm{polynom}\, c)(x)}$.

Now we state the propositions:

(22) Let us consider a real number r. Suppose $0 < r$. Then there exists a non empty, positive yielding finite 0-sequence c of $\mathbb{R}$ such that for every natural number x, $(\mathrm{polynom}\, c)(x) = r$.

(23) Let us consider a function f from $\mathbb{N}$ into $\mathbb{R}$. Suppose f is negligible. Let us consider a real number r. Suppose $0 < r$. Then there exists a natural

number N such that for every natural number x such that $N \leqslant x$ holds $|f(x)| < r$. The theorem is a consequence of (22).

(24) Let us consider a function f from $\mathbb{N}$ into $\mathbb{R}$. If f is negligible, then f is convergent and $\lim f = 0$. The theorem is a consequence of (23).

Let us observe that $\{0\}_{n \in \mathbb{N}}$ is negligible and there exists a function from $\mathbb{N}$ into $\mathbb{R}$ which is negligible.

Let f be a negligible function from $\mathbb{N}$ into $\mathbb{R}$. Let us observe that $|f|$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$.

Let a be a real number. One can verify that $a \cdot f$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$.

Let f, g be negligible functions from $\mathbb{N}$ into $\mathbb{R}$. One can check that $f + g$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$ and $f \cdot g$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$.

Now we state the propositions:

(25) INVERSE OF POWER OF 2 IS NEGLIGIBLE:
Let us consider a function f from $\mathbb{N}$ into $\mathbb{R}$. If for every natural number x, $f(x) = \frac{1}{2^x}$, then f is negligible.
PROOF: Set $k = \operatorname{len} c$. Define $\mathcal{F}(\text{natural number}) = 1 \cdot \$_1^k$. Consider y being a sequence of real numbers such that for every natural number x, $y(x) = \mathcal{F}(x)$ from [14, Sch. 1]. Consider N_1 being a natural number such that for every natural number x such that $N_1 \leqslant x$ holds $|(\mathrm{Seq}_{\mathrm{poly}}(c))(x)| \leqslant y(x)$. Consider N_2 being a natural number such that for every natural number x such that $N_2 \leqslant x$ holds $\frac{1}{2^x} < \frac{1}{x^k}$. Set $N = N_1 + N_2$. For every natural number x such that $N \leqslant x$ holds $|f(x)| < \frac{1}{(\operatorname{polynom} c)(x)}$ by [1, (12)], (8). □

(26) Let us consider functions f, g from $\mathbb{N}$ into $\mathbb{R}$. Suppose f is negligible and for every natural number x, $|g(x)| \leqslant |f(x)|$. Then g is negligible.

One can check that every function from $\mathbb{N}$ into $\mathbb{R}$ which is negligible is also absolutely polynomially bounded.

The functor negligible-Funcs yielding a subset of $\mathcal{O}_{\mathrm{poly}}$ is defined by

(Def. 5) for every object x, $x \in \mathit{it}$ iff x is a negligible function from $\mathbb{N}$ into $\mathbb{R}$.

Let us observe that negligible-Funcs is non empty.

Let us consider vectors v, w of RAlgebra$\mathcal{O}_{\mathrm{poly}}$ and functions v_1, w_1 from $\mathbb{N}$ into $\mathbb{R}$.

Let us assume that $v = v_1$ and $w_1 = w$. Now we state the propositions:

(27) $v + w = v_1 + w_1$. The theorem is a consequence of (19).

(28) $v \cdot w = v_1 \cdot w_1$. The theorem is a consequence of (20).

Now we state the propositions:

(29) Let us consider a real number a, a vector v of RAlgebra$\mathcal{O}_{\rm poly}$, and a function v_1 from $\mathbb{N}$ into $\mathbb{R}$. If $v = v_1$, then $a \cdot v = a \cdot v_1$. The theorem is a consequence of (21).

(30) Let us consider a real number a, and a vector v of RAlgebra$\mathcal{O}_{\rm poly}$. Suppose $v \in$ negligible-Funcs. Then $a \cdot v \in$ negligible-Funcs. The theorem is a consequence of (29).

Let us consider vectors v, u of RAlgebra$\mathcal{O}_{\rm poly}$.

Let us assume that v, $u \in$ negligible-Funcs. Now we state the propositions:

(31) $v + u \in$ negligible-Funcs. The theorem is a consequence of (27).

(32) $v \cdot u \in$ negligible-Funcs. The theorem is a consequence of (28).

Let f, g be functions from $\mathbb{N}$ into $\mathbb{R}$. We say that $f \approx_{\rm neg} g$ if and only if

(Def. 6) there exists a function h from $\mathbb{N}$ into $\mathbb{R}$ such that h is negligible and for every natural number x, $|f(x) - g(x)| \leqslant |h(x)|$.

One can verify that the predicate is reflexive and symmetric.

Now we state the propositions:

(33) Let us consider functions f, g, h from $\mathbb{N}$ into $\mathbb{R}$. Suppose $f \approx_{\rm neg} g$ and $g \approx_{\rm neg} h$. Then $f \approx_{\rm neg} h$.

(34) Let us consider functions f, g from $\mathbb{N}$ into $\mathbb{R}$. Then $f \approx_{\rm neg} g$ if and only if $f - g$ is negligible. The theorem is a consequence of (26).

(35) Let us consider a non empty, positive yielding finite 0-sequence c of $\mathbb{R}$. Then there exists a real number a and there exist natural numbers k, N such that $0 < a$ and $0 < k$ and for every natural number x such that $N \leqslant x$ holds $(\operatorname{polynom} c)(x) \leqslant a \cdot x^k$. The theorem is a consequence of (8).

Let a be a non-negative yielding finite 0-sequence of $\mathbb{R}$ and b be a non-negative yielding sequence of real numbers. Let us observe that $a \cdot b$ is non-negative yielding.

Let a, b be non-negative yielding finite 0-sequences of $\mathbb{R}$. One can check that $a \frown b$ is non-negative yielding.

Let a, b, c be non negative real numbers. Let us note that $\{a^{b \cdot n + c}\}_{n \in \mathbb{N}}$ is non-negative yielding.

Now we state the propositions:

(36) Let us consider a real number a, and a natural number k. Then there exists a non empty, positive yielding finite 0-sequence c of $\mathbb{R}$ such that for every natural number x, $a \cdot x^k \leqslant (\operatorname{polynom} c)(x)$.

Proof: Reconsider $c = \mathbb{Z}_{k+1} \longmapsto |a| + 1$ as a finite 0-sequence of $\mathbb{R}$. For every natural number x, $a \cdot x^k \leqslant (\operatorname{polynom} c)(x)$ by [14, (1)], [24, (13), (7)], [1, (44)]. $\square$

(37) Let us consider non empty, positive yielding finite 0-sequences c, s of $\mathbb{R}$. Then there exists a non empty, positive yielding finite 0-sequence d of $\mathbb{R}$ and there exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $(\mathrm{polynom}\, c)(x) \cdot (\mathrm{polynom}\, s)(x) \leqslant (\mathrm{polynom}\, d)(x)$.
PROOF: Consider a_1 being a real number, k_1, N_1 being natural numbers such that $0 < a_1$ and $0 < k_1$ and for every natural number x such that $N_1 \leqslant x$ holds $(\mathrm{polynom}\, c)(x) \leqslant a_1 \cdot x^{k_1}$. Consider a_2 being a real number, k_2, N_2 being natural numbers such that $0 < a_2$ and $0 < k_2$ and for every natural number x such that $N_2 \leqslant x$ holds $(\mathrm{polynom}\, s)(x) \leqslant a_2 \cdot x^{k_2}$. Consider d being a non empty, positive yielding finite 0-sequence of $\mathbb{R}$ such that for every natural number x, $a_1 \cdot a_2 \cdot x^{k_1+k_2} \leqslant (\mathrm{polynom}\, d)(x)$. $0 < (\mathrm{polynom}\, c)(x)$. $0 < (\mathrm{polynom}\, s)(x)$. $a_1 \cdot x^{k_1} \cdot (a_2 \cdot x^{k_2}) = (a_1 \cdot a_2) \cdot x^{k_1+k_2}$ by [22, (27)]. $\square$

Let f be a negligible function from $\mathbb{N}$ into $\mathbb{R}$ and c be a non empty, positive yielding finite 0-sequence of $\mathbb{R}$. Let us observe that $\mathrm{polynom}\, c \cdot f$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$.

Now we state the proposition:

(38) Let us consider an absolutely polynomially bounded function g from $\mathbb{N}$ into $\mathbb{R}$. Then there exists a non empty, positive yielding finite 0-sequence d of $\mathbb{R}$ and there exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $|g(x)| \leqslant (\mathrm{polynom}\, d)(x)$. The theorem is a consequence of (36).

Let f be a negligible function from $\mathbb{N}$ into $\mathbb{R}$ and g be an absolutely polynomially bounded function from $\mathbb{N}$ into $\mathbb{R}$. Let us note that $g \cdot f$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$.

Now we state the proposition:

(39) Let us consider vectors v, w of $\mathrm{RAlgebra}\mathcal{O}_{\mathrm{poly}}$. Suppose $w \in$ negligible-Funcs. Then $v \cdot w \in$ negligible-Funcs. The theorem is a consequence of (12) and (28).

Acknowledgement: The author would like to express his gratitude to Prof. Yuichi Futa and Prof. Yasunari Shidama for their support and encouragement.

References

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

[2] Mihir Bellare. A note on negligible functions, 2002.

[3] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 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] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

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

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

[10] Oded Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools.* Cambridge University Press, 2001.

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

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

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

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

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

[16] Richard Krueger, Piotr Rudnicki, and Paul Shelley. Asymptotic notation. Part I: Theory. *Formalized Mathematics*, 9(**1**):135–142, 2001.

[17] Richard Krueger, Piotr Rudnicki, and Paul Shelley. Asymptotic notation. Part II: Examples and problems. *Formalized Mathematics*, 9(**1**):143–154, 2001.

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

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

[20] Hiroyuki Okazaki and Yuichi Futa. Polynomially bounded sequences and polynomial sequences. *Formalized Mathematics*, 23(**3**):205–213, 2015. doi:10.1515/forma-2015-0017.

[21] Henryk Oryszczyszyn and Krzysztof Prażmowski. Real functions spaces. *Formalized Mathematics*, 1(**3**):555–561, 1990.

[22] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.

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

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

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

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

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

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

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

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

Received August 15, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 379–386, 2015
DOI: 10.1515/forma-2015-0030

DE GRUYTER
OPEN
degruyter.com/view/j/forma

Propositional Linear Temporal Logic with Initial Validity Semantics[1]

Mariusz Giero
Faculty of Economics and Informatics
University of Białystok
Kalvariju 135, LT-08221 Vilnius
Lithuania

Summary. In the article [10] a formal system for Propositional Linear Temporal Logic (in short LTLB) with normal semantics is introduced. The language of this logic consists of "until" operator in a very strict version. The very strict "until" operator enables to express all other temporal operators.

In this article we construct a formal system for LTLB with the initial semantics [12]. Initial semantics means that we define the validity of the formula in a model as satisfaction in the initial state of model while normal semantics means that we define the validity as satisfaction in all states of model. We prove the Deduction Theorem, and the soundness and completeness of the introduced formal system. We also prove some theorems to compare both formal systems, i.e., the one introduced in the article [10] and the one introduced in this article.

Formal systems for temporal logics are applied in the verification of computer programs. In order to carry out the verification one has to derive an appropriate formula within a selected formal system. The formal systems introduced in [10] and in this article can be used to carry out such verifications in Mizar [4].

MSC: 03B70 03B35

Keywords: temporal logic; very strict until operator; completeness

MML identifier: LTLAXIO5, version: 8.1.04 5.34.1256

The notation and terminology used in this paper have been introduced in the following articles: [13], [3], [9], [5], [6], [11], [14], [10], [16], [1], [2], [7], [17], [15], and [8].

[1]This work was supported by the University of Bialystok grants: BST447 *Formalization of temporal logics in a proof-assistant. Application to System Verification*, and BST225 *Database of mathematical texts checked by computer*.

ISSN 1426–2630(Print), 1898-9934(Online)

1. Preliminaries

Now we state the proposition:

(1) Let us consider a set X, a finite sequence f of elements of X, and a natural number i. If $1 \leqslant i \leqslant \operatorname{len} f$, then $f(i) = f_i$.

From now on A, B, C, p, q, r denote elements of LTLB-WFF, F, G, X denote subsets of LTLB-WFF, M denotes a LTL Model, i, j, n denote elements of $\mathbb{N}$, and f, f_1, f_2, g denote finite sequences of elements of LTLB-WFF.

Now we state the propositions:

(2) If $F \subseteq G$ and $F \vdash A$, then $G \vdash A$.

(3) $A \Rightarrow B \Rightarrow (B \Rightarrow C \Rightarrow (A \Rightarrow C))$ is tautologically valid.

(4) $A \Rightarrow (B \Rightarrow C) \Rightarrow (A \Rightarrow B \Rightarrow (A \Rightarrow C))$ is tautologically valid.

(5) $F \vdash \mathcal{G}\, A \Rightarrow A$.

(6) $\{A\} \models \mathcal{G}\, \mathcal{X}\, A$.

(7) $F \vdash \mathcal{G}\, A \Rightarrow \mathcal{G}\, \mathcal{X}\, A$. The theorem is a consequence of (6) and (2).

(8) $F \vdash \mathcal{G}(A \Rightarrow B) \Rightarrow (\mathcal{G}(A \Rightarrow \mathcal{X}\, A) \Rightarrow \mathcal{G}(A \Rightarrow \mathcal{G}\, B))$.

2. Initial Validity Semantics - Definitions

Let us consider M and A. We say that $M \overset{0}{\models} A$ if and only if

(Def. 1) $\mathrm{SAT}_M(\langle 0, A\rangle) = 1$.

Let us consider F. We say that $M \overset{0}{\models} F$ if and only if

(Def. 2) for every A such that $A \in F$ holds $M \overset{0}{\models} A$.

Let us consider A. We say that $F \overset{0}{\models} A$ if and only if

(Def. 3) for every M such that $M \overset{0}{\models} F$ holds $M \overset{0}{\models} A$.

3. The Connections between Normal Semantics and Initial Semantics

Now we state the propositions:

(9) If $M \models F$, then $M \overset{0}{\models} F$.

(10) $M \models A$ if and only if $M \overset{0}{\models} \mathcal{G}\, A$.

(11) If $F \overset{0}{\models} A$, then $F \models A$. The theorem is a consequence of (9).

Let us consider F. The functor $\mathcal{G}\, F$ yielding a subset of LTLB-WFF is defined by the term

(Def. 4) $\{\mathcal{G}\, A$, where A is an element of LTLB-WFF : $A \in F\}$.

Now we state the propositions:

(12) $M \models F$ if and only if $M \overset{0}{\models} \mathcal{G}\, F$. The theorem is a consequence of (10).

(13) $F \models A$ if and only if $\mathcal{G}\, F \overset{0}{\models} A$.

PROOF: $F \models A$ by [10, (29)], (12), [10, (28)]. □

(14) (i) $\{\mathrm{prop}\, n\} \models \mathcal{X}\, \mathrm{prop}\, n$, and

(ii) $\{\mathrm{prop}\, n\} \overset{0}{\not\models} \mathcal{X}\, \mathrm{prop}\, n$.

PROOF: $\{\mathrm{prop}\, n\} \models \mathcal{X}\, \mathrm{prop}\, n$ by [10, (23), (9)]. $\{\mathrm{prop}\, n\} \overset{0}{\not\models} \mathcal{X}\, \mathrm{prop}\, n$ by [8, (31)], [10, (9)]. □

(15) There exists F and there exists A such that $F \models A$ and $F \overset{0}{\not\models} A$. The theorem is a consequence of (14).

(16) If $F \overset{0}{\models} \mathcal{G}\, A$, then $F \models A$.

(17) (i) $\{\mathrm{prop}\, i\} \models \mathrm{prop}\, i$, and

(ii) $\{\mathrm{prop}\, i\} \overset{0}{\not\models} \mathcal{G}\, \mathrm{prop}\, i$.

The theorem is a consequence of (14).

(18) There exists F and there exists A such that $F \models A$ and $F \overset{0}{\not\models} \mathcal{G}\, A$. The theorem is a consequence of (17).

(19) $M \overset{0}{\models} F$ and $M \overset{0}{\models} G$ if and only if $M \overset{0}{\models} F \cup G$.

(20) $M \overset{0}{\models} A$ if and only if $M \overset{0}{\models} \{A\}$.

(21) $F \cup \{A\} \overset{0}{\models} B$ if and only if $F \overset{0}{\models} A \Rightarrow B$. The theorem is a consequence of (20) and (19).

(22) $\mathcal{G}\, \emptyset_{\text{LTLB-WFF}} = \emptyset_{\text{LTLB-WFF}}$.

(23) If $F \models A$ and for every B such that $B \in F$ holds $\emptyset_{\text{LTLB-WFF}} \models B$, then $\emptyset_{\text{LTLB-WFF}} \models A$.

(24) Suppose $F \models A$ and for every B such that $B \in F$ holds $\emptyset_{\text{LTLB-WFF}} \overset{0}{\models} B$. Then $\emptyset_{\text{LTLB-WFF}} \overset{0}{\models} A$. The theorem is a consequence of (13), (22), and (23).

(25) If $\emptyset_{\text{LTLB-WFF}} \overset{0}{\models} A$, then $\emptyset_{\text{LTLB-WFF}} \overset{0}{\models} \mathcal{X}\, A$. The theorem is a consequence of (24).

4. A Formal System (Hilbert-like) for LTLB with Initial Semantics

The functor LTL_0-axioms yielding a subset of LTLB-WFF is defined by the term

(Def. 5) $\mathcal{G}\, AX_{\mathrm{LTL}}$.

Let us consider p and q. We say that $p\, \mathrm{REFL}_0\text{-rule}\, q$ if and only if

(Def. 6) $p = \mathcal{G}\, q$.

We say that $p\, \mathrm{NEX}_0\text{-rule}\, q$ if and only if

(Def. 7) there exists A such that $p = \mathcal{G}\, A$ and $q = \mathcal{G}\, \mathcal{X}\, A$.

Let us consider r. We say that $p, q\, \mathrm{MP}_0\text{-rule}\, r$ if and only if

(Def. 8) there exists A and there exists B such that $p = \mathcal{G}\, A$ and $q = \mathcal{G}(A \Rightarrow B)$ and $r = \mathcal{G}\, B$.

We say that $p, q\, \mathrm{IND}_0\text{-rule}\, r$ if and only if

(Def. 9) there exists A and there exists B such that $p = \mathcal{G}(A \Rightarrow B)$ and $q = \mathcal{G}(A \Rightarrow \mathcal{X}\, A)$ and $r = \mathcal{G}(A \Rightarrow \mathcal{G}\, B)$.

Let i be a natural number. Let us consider f and X. We say that $\mathrm{prc}_0 f, X, i$ if and only if

(Def. 10) $f(i) \in \mathrm{LTL}_0$-axioms or $f(i) \in X$ or there exist natural numbers j, k such that $1 \leqslant j < i$ and $1 \leqslant k < i$ and $(\mathrm{MP}(f_j, f_k, f_i)$ or $f_j, f_k\, \mathrm{MP}_0\text{-rule}\, f_i$ or $f_j, f_k\, \mathrm{IND}_0\text{-rule}\, f_i)$ or there exists a natural number j such that $1 \leqslant j < i$ and $(f_j\, \mathrm{NEX}_0\text{-rule}\, f_i$ or $f_j\, \mathrm{REFL}_0\text{-rule}\, f_i)$.

Now we state the propositions:

(26) Let us consider natural numbers i, n. Suppose $n + \mathrm{len}\, f \leqslant \mathrm{len}\, f_2$ and for every natural number k such that $1 \leqslant k \leqslant \mathrm{len}\, f$ holds $f(k) = f_2(k+n)$ and $1 \leqslant i \leqslant \mathrm{len}\, f$. If $\mathrm{prc}_0 f, X, i$, then $\mathrm{prc}_0 f_2, X, i+n$. The theorem is a consequence of (1).

(27) Suppose $f_2 = f \frown f_1$ and $1 \leqslant \mathrm{len}\, f$ and $1 \leqslant \mathrm{len}\, f_1$ and for every natural number i such that $1 \leqslant i \leqslant \mathrm{len}\, f$ holds $\mathrm{prc}_0 f, X, i$ and for every natural number i such that $1 \leqslant i \leqslant \mathrm{len}\, f_1$ holds $\mathrm{prc}_0 f_1, X, i$. Let us consider a natural number i. If $1 \leqslant i \leqslant \mathrm{len}\, f_2$, then $\mathrm{prc}_0 f_2, X, i$. The theorem is a consequence of (1) and (26).

Let us consider X and p. We say that $X \overset{0}{\vdash} p$ if and only if

(Def. 11) there exists f such that $f(\mathrm{len}\, f) = p$ and $1 \leqslant \mathrm{len}\, f$ and for every natural number i such that $1 \leqslant i \leqslant \mathrm{len}\, f$ holds $\mathrm{prc}_0 f, X, i$.

(28) Suppose $f = f_1 \frown \langle p \rangle$ and $1 \leqslant \mathrm{len}\, f_1$ and for every natural number i such that $1 \leqslant i \leqslant \mathrm{len}\, f_1$ holds $\mathrm{prc}_0 f_1, X, i$ and $\mathrm{prc}_0 f, X, \mathrm{len}\, f$. Then

(i) for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $\operatorname{prc}_0 f, X, i$, and

(ii) $X \overset{0}{\vdash} p$.

The theorem is a consequence of (26).

5. Soundness Theorem for LTLB with Initial Semantics

Now we state the propositions:

(29) If $A \in \mathrm{LTL}_0$-axioms, then $F \overset{0}{\models} A$. The theorem is a consequence of (13) and (22).

(30) If $F \overset{0}{\models} A$ and $F \overset{0}{\models} A \Rightarrow B$, then $F \overset{0}{\models} B$.

(31) Suppose $F \overset{0}{\models} \mathcal{G}\, A$ and $F \overset{0}{\models} \mathcal{G}(A \Rightarrow B)$. Then $F \overset{0}{\models} \mathcal{G}\, B$.

Let us assume that $F \overset{0}{\models} \mathcal{G}\, A$. Now we state the propositions:

(32) $F \overset{0}{\models} \mathcal{G}\, \mathcal{X}\, A$.

(33) $F \overset{0}{\models} A$.

(34) Suppose $F \overset{0}{\models} \mathcal{G}(A \Rightarrow B)$ and $F \overset{0}{\models} \mathcal{G}(A \Rightarrow \mathcal{X}\, A)$. Then $F \overset{0}{\models} \mathcal{G}(A \Rightarrow \mathcal{G}\, B)$.

(35) Soundness Theorem for LTLB with initial semantics:
If $F \overset{0}{\vdash} A$, then $F \overset{0}{\models} A$.
Proof: Consider f such that $f(\operatorname{len} f) = A$ and $1 \leqslant \operatorname{len} f$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $\operatorname{prc}_0 f, F, i$. Define $\mathcal{P}$[natural number] $\equiv$ if $1 \leqslant \$_1 \leqslant \operatorname{len} f$, then $F \overset{0}{\models} f_{\$_1}$. For every natural number i such that for every natural number j such that $j < i$ holds $\mathcal{P}[j]$ holds $\mathcal{P}[i]$ by [1, (14)], (1), (29), (30). For every natural number i, $\mathcal{P}[i]$ from [1, Sch. 4]. $f_{\operatorname{len} f} = A$. □

6. Weak Completeness Theorem for LTLB with Initial Semantics

Now we state the proposition:

(36) If $A \in \mathrm{LTL}_0$-axioms or $A \in F$, then $F \overset{0}{\vdash} A$.
Proof: Define $\mathcal{S}$[set, set] $\equiv \$_2 = A$. Consider g such that $\operatorname{dom} g = \operatorname{Seg} 1$ and for every natural number k such that $k \in \operatorname{Seg} 1$ holds $\mathcal{S}[k, g(k)]$ from [3, Sch. 5]. For every natural number j such that $1 \leqslant j \leqslant \operatorname{len} g$ holds $\operatorname{prc}_0 g, F, j$. □

Let us assume that $F \overset{0}{\vdash} \mathcal{G}\, A$. Now we state the propositions:

(37) $F \overset{0}{\vdash} A$. The theorem is a consequence of (1) and (28).

(38) $F \overset{0}{\vdash} \mathcal{G}\,\mathcal{X}\,A$. The theorem is a consequence of (1) and (28).

(39) If $F \overset{0}{\vdash} A$ and $F \overset{0}{\vdash} A \Rightarrow B$, then $F \overset{0}{\vdash} B$. The theorem is a consequence of (27), (1), and (28).

(40) If $F \overset{0}{\vdash} \mathcal{G}\,A$ and $F \overset{0}{\vdash} \mathcal{G}(A \Rightarrow B)$, then $F \overset{0}{\vdash} \mathcal{G}\,B$. The theorem is a consequence of (27), (1), and (28).

(41) Suppose $F \overset{0}{\vdash} \mathcal{G}(A \Rightarrow B)$ and $F \overset{0}{\vdash} \mathcal{G}(A \Rightarrow \mathcal{X}\,A)$. Then $F \overset{0}{\vdash} \mathcal{G}(A \Rightarrow \mathcal{G}\,B)$. The theorem is a consequence of (27), (1), and (28).

(42) If $A \in AX_{\mathrm{LTL}}$, then $F \overset{0}{\vdash} A$. The theorem is a consequence of (36) and (37).

(43) If $A \in \mathrm{LTL}_0$-axioms, then $F \vdash A$.

(44) If $\emptyset_{\text{LTLB-WFF}} \vdash A$, then $\emptyset_{\text{LTLB-WFF}} \overset{0}{\vdash} A$.

PROOF: Consider f such that $f(\operatorname{len} f) = A$ and $1 \leqslant \operatorname{len} f$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $\operatorname{prc}(f, \emptyset_{\text{LTLB-WFF}}, i)$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $1 \leqslant \$_1 \leqslant \operatorname{len} f$, then $\emptyset_{\text{LTLB-WFF}} \overset{0}{\vdash} \mathcal{G}\,f_{\$_1}$. For every natural number i such that for every natural number j such that $j < i$ holds $\mathcal{P}[j]$ holds $\mathcal{P}[i]$ by [1, (14)], (1), (36), (40). For every natural number i, $\mathcal{P}[i]$ from [1, Sch. 4]. $A = f_{\operatorname{len} f}$. $\square$

(45) (i) $\{\operatorname{prop} i\} \vdash \mathcal{X} \operatorname{prop} i$, and

(ii) $\{\operatorname{prop} i\} \overset{0}{\nvdash} \mathcal{X} \operatorname{prop} i$.

The theorem is a consequence of (35) and (14).

(46) If $F \subseteq G$ and $F \overset{0}{\vdash} A$, then $G \overset{0}{\vdash} A$.

Let us consider f and A. The functor implications(f, A) yielding a finite sequence of elements of LTLB-WFF is defined by

(Def. 12) (i) $\operatorname{len} it = \operatorname{len} f$ and $it(1) = f_1 \Rightarrow A$ and for every i such that $1 \leqslant i < \operatorname{len} f$ holds $it(i+1) = f_{i+1} \Rightarrow it_i$, **if** $\operatorname{len} f > 0$,

(ii) $it = \varepsilon_{(\text{LTLB-WFF})}$, **otherwise**.

Now we state the proposition:

(47) WEAK COMPLETENESS THEOREM FOR LTLB WITH INITIAL SEMANTICS:

Let us consider a finite subset F of LTLB-WFF. If $F \overset{0}{\models} A$, then $F \overset{0}{\vdash} A$. The theorem is a consequence of (13), (22), (44), (21), (36), (39), and (46).

7. Deduction Theorem

Now we state the propositions:

(48) If $F \cup \{A\} \overset{0}{\vdash} B$, then $F \overset{0}{\vdash} A \Rightarrow B$.

Proof: Consider f such that $f(\operatorname{len} f) = B$ and $1 \leqslant \operatorname{len} f$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $\mathrm{prc}_0 f, F \cup \{A\}, i$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $1 \leqslant \$_1 \leqslant \operatorname{len} f$, then $F \overset{0}{\vdash} A \Rightarrow f_{\$_1}$. For every natural number i such that for every natural number j such that $j < i$ holds $\mathcal{P}[j]$ holds $\mathcal{P}[i]$ by [1, (14)], (42), [10, (34)], (1). For every natural number i, $\mathcal{P}[i]$ from [1, Sch. 4]. $B = f_{\operatorname{len} f}$. □

(49) If $F \overset{0}{\vdash} A \Rightarrow B$, then $F \cup \{A\} \overset{0}{\vdash} B$. The theorem is a consequence of (36), (46), and (39).

8. The Connections between Derivability in the Formal System for LTLB with Normal Semantics and the Formal System for LTLB with Initial Semantics

Let F be a finite subset of LTLB-WFF. Note that $\mathcal{G}\, F$ is finite.

Let us consider a finite subset F of LTLB-WFF. Now we state the propositions:

(50) $F \vdash A$ if and only if $\mathcal{G}\, F \overset{0}{\vdash} A$. The theorem is a consequence of (47), (13), and (35).

(51) If $F \overset{0}{\vdash} A$, then $F \vdash A$. The theorem is a consequence of (35) and (11).

Now we state the propositions:

(52) (i) $\{\operatorname{prop} i\} \vdash \mathcal{G} \operatorname{prop} i$, and

(ii) $\{\operatorname{prop} i\} \overset{0}{\nvdash} \mathcal{G} \operatorname{prop} i$.

Proof: $\{\operatorname{prop} i\} \vdash \mathcal{G} \operatorname{prop} i$ by [10, (42), (54)]. $\{\operatorname{prop} i\} \overset{0}{\nvdash} \mathcal{G} \operatorname{prop} i$ by (35), (47), (45), [10, (10), (9)]. □

(53) Let us consider a finite subset F of LTLB-WFF. If $F \overset{0}{\vdash} \mathcal{G}\, A$, then $F \vdash A$. The theorem is a consequence of (35) and (16).

(54) (i) $\{\operatorname{prop} i\} \vdash \operatorname{prop} i$, and

(ii) $\{\operatorname{prop} i\} \overset{0}{\nvdash} \mathcal{G} \operatorname{prop} i$.

The theorem is a consequence of (35) and (17).

References

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

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

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

[4] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

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

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

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

[10] Mariusz Giero. The axiomatization of propositional linear time temporal logic. *Formalized Mathematics*, 19(**2**):113–119, 2011. doi:10.2478/v10037-011-0018-1.

[11] Adam Grabowski. Hilbert positive propositional calculus. *Formalized Mathematics*, 8(**1**): 69–72, 1999.

[12] Fred Kröger and Stephan Merz. *Temporal Logic and State Systems.* Springer-Verlag, 2008.

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

[14] Andrzej Trybulec. Defining by structural induction in the positive propositional language. *Formalized Mathematics*, 8(**1**):133–137, 1999.

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

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

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

Received October 22, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 387–396, 2015
DOI: 10.1515/forma-2015-0031

DE GRUYTER
OPEN
degruyter.com/view/j/forma

Stone Lattices

Adam Grabowski
Institute of Informatics
University of Białystok
Ciołkowskiego 1M, 15-245 Białystok
Poland

Summary. The article continues the formalization of the lattice theory (as structures with two binary operations, not in terms of ordering relations). In the paper, the notion of a pseudocomplement in a lattice is formally introduced in Mizar, and based on this we define the notion of the skeleton and the set of dense elements in a pseudocomplemented lattice, giving the meet-decomposition of arbitrary element of a lattice as the infimum of two elements: one belonging to the skeleton, and the other which is dense.

The core of the paper is of course the idea of Stone identity

$$a^\star \sqcup a^{\star\star} = \top,$$

which is fundamental for us: Stone lattices are those lattices L, which are distributive, bounded, and satisfy Stone identity for all elements $a \in L$. Stone algebras were introduced by Grätzer and Schmidt in [18]. Of course, the pseudocomplement is unique (if exists), so in a pseudcomplemented lattice we defined $a^\star$ as the Mizar functor (unary operation mapping every element to its pseudocomplement). In Section 2 we prove formally a collection of ordinary properties of pseudocomplemented lattices.

All Boolean lattices are Stone, and a natural example of the lattice which is Stone, but not Boolean, is the lattice of all natural divisors of p^2 for arbitrary prime number p (Section 6). At the end we formalize the notion of the Stone lattice $B^{[2]}$ (of pairs of elements a, b of B such that $a \leqslant b$) constructed as a sublattice of B^2, where B is arbitrary Boolean algebra (and we describe skeleton and the set of dense elements in such lattices). In a natural way, we deal with Cartesian product of pseudocomplemented lattices.

Our formalization was inspired by [17], and is an important step in formalizing Jouni Järvinen *Lattice theory for rough sets* [19], so it follows rather the latter paper. We deal essentially with Section 4.3, pages 423–426. The description of handling complemented structures in Mizar [6] can be found in [12]. The

ISSN 1426–2630(Print), 1898-9934(Online)

current article together with [15] establishes the formal background for algebraic structures which are important for [10], [16] by means of mechanisms of merging theories as described in [11].

MSC: 06D15 06E75 03B35

Keywords: pseudocomplemented lattices; Stone lattices; Boolean lattices; lattice of natural divisors

MML identifier: LATSTONE, version: 8.1.04 5.34.1256

The notation and terminology used in this paper have been introduced in the following articles: [1], [25], [2], [3], [9], [26], [23], [4], [13], [28], [20], [14], [8], [5], [27], and [7].

1. Preliminaries

Now we state the proposition:

(1) Let us consider a distributive lattice L. Then every sublattice of L is distributive.

Let L be a distributive lattice. One can verify that every sublattice of L is distributive.

Let L_1, L_2 be bounded lattices. One can check that $L_1 \times L_2$ is bounded.

From now on L denotes a lattice and I, P denote non empty closed subset of L.

Now we state the propositions:

(2) If L is lower-bounded and $\bot_L \in I$, then $\mathbb{L}_I^L$ is lower-bounded and $\bot_{\mathbb{L}_I^L} = \bot_L$.

PROOF: Set $c = \bot_L$. Reconsider $c' = c$ as an element of $\mathbb{L}_I^L$. There exists an element c' of $\mathbb{L}_I^L$ such that for every element a' of $\mathbb{L}_I^L$, $c' \sqcap a' = c'$ and $a' \sqcap c' = c'$ by [3, (68), (73)]. For every element a' of $\mathbb{L}_I^L$, $c' \sqcap a' = c'$ and $a' \sqcap c' = c'$ by [3, (68), (73)]. □

(3) If L is upper-bounded and $\top_L \in I$, then $\mathbb{L}_I^L$ is upper-bounded and $\top_{\mathbb{L}_I^L} = \top_L$.

PROOF: Set $c = \top_L$. Reconsider $c' = c$ as an element of $\mathbb{L}_I^L$. There exists an element c' of $\mathbb{L}_I^L$ such that for every element a' of $\mathbb{L}_I^L$, $c' \sqcup a' = c'$ and $a' \sqcup c' = c'$ by [3, (68), (73)]. For every element a' of $\mathbb{L}_I^L$, $c' \sqcup a' = c'$ and $a' \sqcup c' = c'$ by [3, (68), (73)]. □

2. PSEUDOCOMPLEMENTS IN LATTICES

Let L be a non empty lattice structure and a, b be elements of L. We say that a is a pseudocomplement of b if and only if

(Def. 1) $a \sqcap b = \bot_L$ and for every element x of L such that $b \sqcap x = \bot_L$ holds $x \sqsubseteq a$.

We say that L is pseudocomplemented if and only if

(Def. 2) for every element x of L, there exists an element y of L such that y is a pseudocomplement of x.

Now we state the proposition:

(4) Every Boolean lattice is pseudocomplemented.

Let us note that every lattice which is Boolean is also pseudocomplemented and there exists a lattice which is Boolean, pseudocomplemented, and bounded.

Now we state the proposition:

(5) Let us consider a pseudocomplemented, lower-bounded lattice L, and elements a, b, x of L. If a is a pseudocomplement of x and b is a pseudocomplement of x, then $a = b$.

Let L be a non empty lattice structure and x be an element of L. Assume L is a pseudocomplemented, lower-bounded lattice. The functor x^* yielding an element of L is defined by

(Def. 3) *it* is a pseudocomplement of x.

Now we state the proposition:

(6) Let us consider a pseudocomplemented, lower-bounded lattice L, and an element x of L. Then $x^* \sqcap x = \bot_L$.

From now on L denotes a lower-bounded, pseudocomplemented lattice.

Now we state the propositions:

(7) Let us consider an element a of L. Then $a \sqsubseteq (a^*)^*$.

(8) Let us consider elements a, b of L. If $a \sqsubseteq b$, then $b^* \sqsubseteq a^*$. The theorem is a consequence of (6).

(9) Let us consider an element a of L. Then $a^* = ((a^*)^*)^*$. The theorem is a consequence of (8) and (7).

Let us consider a pseudocomplemented, bounded lattice L. Now we state the propositions:

(10) $(\bot_L)^* = \top_L$.

(11) $(\top_L)^* = \bot_L$.

(12) Let us consider a Boolean lattice L, and an element x of L. Then $x^{\mathrm{c}} = x^*$.
PROOF: $x^* \sqsubseteq x^{\mathrm{c}}$ by (6), [28, (25)]. $x^{\mathrm{c}} \sqsubseteq x^*$ by [28, (20)]. □

(13) Let us consider a pseudocomplemented, bounded lattice L, and elements x, y of L. Suppose y is a pseudocomplement of x. Then $y \in$ the set of pseudo-complements of x.

(14) Let us consider a pseudocomplemented, bounded lattice L, and an element x of L. Then $x^* \in$ the set of pseudo-complements of x. The theorem is a consequence of (13).

3. Skeleton of a Pseudocomplemented Lattice

Let L be a lower-bounded, pseudocomplemented lattice. The functor Skeleton L yielding a subset of L is defined by the term

(Def. 4) the set of all a^* where a is an element of L.

Now we state the propositions:

(15) Let us consider a lower-bounded, pseudocomplemented lattice L. Then $\mathrm{Skeleton}\, L = \{a$, where a is an element of $L : (a^*)^* = a\}$. The theorem is a consequence of (9).

(16) Let us consider a lower-bounded, pseudocomplemented lattice L, and an element x of L. Then $x \in \mathrm{Skeleton}\, L$ if and only if $(x^*)^* = x$. The theorem is a consequence of (9).

Let L be a bounded, pseudocomplemented lattice. Let us note that Skeleton L is non empty.

Now we state the proposition:

(17) Let us consider a pseudocomplemented, distributive, lower-bounded lattice L, and elements a, b of L. If $a, b \in \mathrm{Skeleton}\, L$, then $a \sqcap b \in \mathrm{Skeleton}\, L$. The theorem is a consequence of (16), (8), and (7).

4. Stone Identity

Let L be a non empty lattice structure. We say that L satisfies the Stone identity if and only if

(Def. 5) for every element x of L, $x^* \sqcup (x^*)^* = \top_L$.

Now we state the proposition:

(18) Every Boolean lattice satisfies the Stone identity.

Proof: $x^* \sqcup (x^*)^* = \top_L$ by (12), [28, (21)]. □

Let us note that every lattice which is Boolean satisfies also the Stone identity and there exists a lattice which is pseudocomplemented and Boolean and satisfies the Stone identity.

Now we state the proposition:

(19) Let us consider a pseudocomplemented, distributive, bounded lattice L. Then L satisfies the Stone identity if and only if for every elements a, b of L, $(a \sqcap b)^* = a^* \sqcup b^*$. The theorem is a consequence of (6) and (10).

Let L be a lattice. We say that L is Stone if and only if

(Def. 6) L is pseudocomplemented, distributive, and bounded and satisfies the Stone identity.

Let us note that every lattice which is Stone is also pseudocomplemented, distributive, and bounded and satisfies also the Stone identity and every lattice which is pseudocomplemented, distributive, and bounded and satisfies the Stone identity is also Stone.

Now we state the proposition:

(20) Let us consider a pseudocomplemented, distributive, bounded lattice L. Then L satisfies the Stone identity if and only if for every elements a, b of L such that $a, b \in \mathrm{Skeleton}\, L$ holds $a \sqcup b \in \mathrm{Skeleton}\, L$. The theorem is a consequence of (19), (16), (8), (9), (6), and (10).

In the sequel L denotes a Stone lattice.

Now we state the proposition:

(21) $\top_L, \bot_L \in \mathrm{Skeleton}\, L$. The theorem is a consequence of (11) and (10).

Let L be a Stone lattice and a be an element of L. We say that a is skeletal if and only if

(Def. 7) $a \in \mathrm{Skeleton}\, L$.

One can verify that $\top_L$ is skeletal and $\bot_L$ is skeletal and Skeleton L is join-closed and meet-closed.

Let us observe that the functor Skeleton L yields a closed subset of L. The functor SkelLatt L yielding a sublattice of L is defined by the term

(Def. 8) $\mathbb{L}^{L}_{\mathrm{Skeleton}\, L}$.

Observe that SkelLatt L is distributive.

Now we state the proposition:

(22) (i) $\bot_L = \bot_{\mathrm{SkelLatt}\, L}$, and

(ii) $\top_L = \top_{\mathrm{SkelLatt}\, L}$.

The theorem is a consequence of (21), (2), and (3).

Let L be a Stone lattice. Observe that SkelLatt L is Boolean.

5. Dense Elements in Lattices

Let L be a lower-bounded lattice. The functor DenseElements L yielding a subset of L is defined by the term

(Def. 9) $\{a$, where a is an element of $L : a^* = \bot_L\}$.

Now we state the proposition:

(23) $\top_L \in$ DenseElements L. The theorem is a consequence of (11).

Let L be a Stone lattice. Note that DenseElements L is non empty.

Let a be an element of L. We say that a is dense if and only if

(Def. 10) $a \in$ DenseElements L.

Note that $\top_L$ is dense.

Now we state the proposition:

(24) Let us consider a Stone lattice L, and an element x of L. If $x \in$ DenseElements L, then $x^* = \bot_L$.

Let L be a Stone lattice. Note that DenseElements L is join-closed and meet-closed.

Let us note that the functor DenseElements L yields a closed subset of L. The functor DenseLatt L yielding a sublattice of L is defined by the term

(Def. 11) $\mathbb{L}^L_{\text{DenseElements}\,L}$.

Note that DenseLatt L is distributive.

Now we state the proposition:

(25) Let us consider a Stone lattice L, and an element a of L. Then there exist elements b, c of L such that

(i) $a = b \sqcap c$, and

(ii) $b \in$ Skeleton L, and

(iii) $c \in$ DenseElements L.

The theorem is a consequence of (7), (6), and (8).

6. An Example: Lattice of Natural Divisors

Let us consider a prime number p. Now we state the propositions:

(26) The set of positive divisors of $p = \{1, p\}$.
PROOF: $\{p^k$, where k is an element of $\mathbb{N} : k \leqslant 1\} = \{1, p\}$ by [22, (4)]. □

(27) The set of positive divisors of $p \cdot p = \{1, p, p \cdot p\}$.
PROOF: $\{p^k$, where k is an element of $\mathbb{N} : k \leqslant 2\} = \{1, p, p \cdot p\}$ by [22, (81), (4)]. □

Let n be a non zero natural number. Let us observe that the lattice of positive divisors of n is finite and there exists a Boolean lattice which is complete.

Let p be a prime number. One can check that the lattice of positive divisors of p is Boolean and the lattice of positive divisors of $p \cdot p$ is pseudocomplemented.

Now we state the proposition:

(28) Let us consider a lattice L, a prime number p, and an element x of L. Suppose $L =$ the lattice of positive divisors of $p \cdot p$ and $x = p$. Then $x^* = \bot_L$.

Proof: Reconsider $y_1 = \bot_L$ as an element of L. For every element y of L such that $x \sqcap y = \bot_L$ holds $y \sqsubseteq y_1$ by (27), [14, (64)]. □

Let p be a prime number. Observe that the lattice of positive divisors of $p \cdot p$ satisfies the Stone identity and the lattice of positive divisors of $p \cdot p$ is non Boolean and Stone and there exists a lattice which is Stone and non Boolean.

7. Products of Pseudocomplemented Lattices

From now on L_1, L_2 denote lattices, p_1, q_1 denote elements of L_1, and p_2, q_2 denote elements of L_2.

Let us assume that L_1 is a bounded lattice and L_2 is a bounded lattice. Now we state the propositions:

(29) p_1 is a pseudocomplement of q_1 and p_2 is a pseudocomplement of q_2 if and only if $\langle p_1, p_2 \rangle$ is a pseudocomplement of $\langle q_1, q_2 \rangle$.

Proof: If p_1 is a pseudocomplement of q_1 and p_2 is a pseudocomplement of q_2, then $\langle p_1, p_2 \rangle$ is a pseudocomplement of $\langle q_1, q_2 \rangle$ by [2, (35), (42), (36)]. For every element x_3 of L_1 such that $q_1 \sqcap x_3 = \bot_{L_1}$ holds $x_3 \sqsubseteq p_1$ by [2, (42), (35), (36)]. For every element x_4 of L_2 such that $q_2 \sqcap x_4 = \bot_{L_2}$ holds $x_4 \sqsubseteq p_2$ by [2, (42), (35), (36)]. □

(30) L_1 is pseudocomplemented and L_2 is pseudocomplemented if and only if $L_1 \times L_2$ is pseudocomplemented. The theorem is a consequence of (29).

Let L_1, L_2 be pseudocomplemented bounded lattices. Let us observe that $L_1 \times L_2$ is pseudocomplemented.

Now we state the proposition:

(31) Suppose L_1 is a pseudocomplemented bounded lattice and L_2 is a pseudocomplemented bounded lattice. Then $\langle p_1, p_2 \rangle^* = \langle {p_1}^*, {p_2}^* \rangle$. The theorem is a consequence of (29).

In the sequel L_1, L_2 denote non empty lattices.

Now we state the propositions:

(32) If L_1 is a pseudocomplemented bounded lattice and L_2 is a pseudocomplemented bounded lattice, then $L_1 \times L_2$ satisfies the Stone identity.

Proof: Set $L = L_1 \times L_2$. For every element x of L, $x^* \sqcup (x^*)^* = \top_L$ by (31), [2, (43), (35)]. □

(33) If L_1 is Stone and L_2 is Stone, then $L_1 \times L_2$ is Stone.

Let L_1, L_2 be Stone lattices. Let us observe that $L_1 \times L_2$ is Stone.

8. Special Construction: $B^{[2]}$

From now on B denotes a Boolean lattice.

Let B be a Boolean lattice. The functor carrier($B^{[2]}$) yielding a subset of $B \times B$ is defined by the term

(Def. 12) $\{\langle a, b \rangle$, where a, b are elements of $B : a \sqsubseteq b\}$.

Let us note that carrier($B^{[2]}$) is non empty and carrier($B^{[2]}$) is join-closed and meet-closed.

Observe that the functor carrier($B^{[2]}$) yields a non empty closed subset of $B \times B$. The functor $B^{[2]}$ yielding a lattice is defined by the term

(Def. 13) $\mathbb{L}^{B \times B}_{\mathrm{carrier}(B^{[2]})}$.

Now we state the propositions:

(34) The carrier of $B^{[2]} = \mathrm{carrier}(B^{[2]})$.

(35) $\langle \bot_B, \bot_B \rangle \in$ the carrier of $B^{[2]}$. The theorem is a consequence of (34).

(36) $\langle \top_B, \top_B \rangle \in$ the carrier of $B^{[2]}$. The theorem is a consequence of (34).

Let B be a Boolean lattice. One can verify that $B^{[2]}$ is lower-bounded and $B^{[2]}$ is upper-bounded.

Now we state the propositions:

(37) $\bot_{B^{[2]}} = \langle \bot_B, \bot_B \rangle$. The theorem is a consequence of (2).

(38) $\top_{B^{[2]}} = \langle \top_B, \top_B \rangle$. The theorem is a consequence of (3).

Let B be a Boolean lattice. One can check that $B^{[2]}$ is pseudocomplemented.

Now we state the proposition:

(39) Let us consider a lattice L, elements x_1, x_2 of B, and an element x of L. Suppose $L = B^{[2]}$ and $x = \langle x_1, x_2 \rangle$. Then $x^* = \langle {x_2}^{\mathrm{c}}, {x_2}^{\mathrm{c}} \rangle$.

Proof: $x \in \mathrm{carrier}(B^{[2]})$. Consider x_3, x_4 being elements of B such that $x = \langle x_3, x_4 \rangle$ and $x_3 \sqsubseteq x_4$. Reconsider $y = \langle {x_2}^{\mathrm{c}}, {x_2}^{\mathrm{c}} \rangle$ as an element of L. For every element w of L such that $x \sqcap w = \bot_L$ holds $w \sqsubseteq y$ by (34), [24, (11)], (37), [2, (35)]. y is a pseudocomplement of x. □

Let B be a Boolean lattice. One can verify that $B^{[2]}$ satisfies the Stone identity and $B^{[2]}$ is Stone.

Now we state the propositions:

(40) Skeleton $B^{[2]}$ = the set of all $\langle a, a\rangle$ where a is an element of B.

Proof: Skeleton $B^{[2]}$ = the set of all $\langle a, a\rangle$ where a is an element of B by (34), (39), [3, (72)]. □

(41) DenseElements $B^{[2]}$ = the set of all $\langle a, \top_B\rangle$ where a is an element of B.

Proof: Set $L = B^{[2]}$. DenseElements $L \subseteq$ the set of all $\langle a, \top_B\rangle$ where a is an element of B by (34), (37), (39), [21, (30)]. Consider a being an element of B such that $x = \langle a, \top_B\rangle$. Reconsider $y = x$ as an element of L. $y^* = \langle(\top_B)^{\rm c}, (\top_B)^{\rm c}\rangle$. □

References

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

[2] Grzegorz Bancerek. Filters – part II. Quotient lattices modulo filters and direct product of two lattices. *Formalized Mathematics*, 2(**3**):433–438, 1991.

[3] Grzegorz Bancerek. Ideals. *Formalized Mathematics*, 5(**2**):149–156, 1996.

[4] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.

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

[6] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

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

[8] Marek Chmur. The lattice of natural numbers and the sublattice of it. The set of prime numbers. *Formalized Mathematics*, 2(**4**):453–459, 1991.

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

[10] Adam Grabowski. On the computer-assisted reasoning about rough sets. In B. Dunin-Kęplicz, A. Jankowski, A. Skowron, and M. Szczuka, editors, *International Workshop on Monitoring, Security, and Rescue Techniques in Multiagent Systems Location*, volume 28 of *Advances in Soft Computing*, pages 215–226, Berlin, Heidelberg, 2005. Springer-Verlag. doi:10.1007/3-540-32370-8_15.

[11] Adam Grabowski. Efficient rough set theory merging. *Fundamenta Informaticae*, 135(4): 371–385, 2014. doi:10.3233/FI-2014-1129.

[12] Adam Grabowski. Mechanizing complemented lattices within Mizar system. *Journal of Automated Reasoning*, 55:211–221, 2015. doi:10.1007/s10817-015-9333-5.

[13] Adam Grabowski. Prime filters and ideals in distributive lattices. *Formalized Mathematics*, 21(**3**):213–221, 2013. doi:10.2478/forma-2013-0023.

[14] Adam Grabowski. On square-free numbers. *Formalized Mathematics*, 21(**2**):153–162, 2013. doi:10.2478/forma-2013-0017.

[15] Adam Grabowski. Two axiomatizations of Nelson algebras. *Formalized Mathematics*, 23 (**2**):115–125, 2015. doi:10.1515/forma-2015-0012.

[16] Adam Grabowski and Magdalena Jastrzębska. Rough set theory from a math-assistant perspective. In *Rough Sets and Intelligent Systems Paradigms, International Conference, RSEISP 2007, Warsaw, Poland, June 28–30, 2007, Proceedings*, pages 152–161, 2007. doi:10.1007/978-3-540-73451-2_17.

[17] George Grätzer. *Lattice Theory: Foundation*. Birkhäuser, 2011.

[18] George Grätzer and E.T. Schmidt. On a problem of M.H. Stone. *Acta Mathematica Academiae Scientarum Hungaricae*, (8):455–460, 1957.

[19] Jouni Järvinen. Lattice theory for rough sets. *Transactions of Rough Sets, VI, Lecture Notes in Computer Science*, 4374:400–498, 2007.

[20] Magdalena Jastrzębska and Adam Grabowski. On the properties of the Möbius function. *Formalized Mathematics*, 14(**1**):29–36, 2006. doi:10.2478/v10037-006-0005-0.

[21] Jolanta Kamieńska and Jarosław Stanisław Walijewski. Homomorphisms of lattices, finite join and finite meet. *Formalized Mathematics*, 4(**1**):35–40, 1993.

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

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

[24] Robert Milewski. More on the lattice of many sorted equivalence relations. *Formalized Mathematics*, 5(**4**):565–569, 1996.

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

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

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

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

Received October 22, 2015