FORMALIZED MATHEMATICS
Volume 9, Number 2, 2001
University of Białystok

The Ring of Polynomials

Robert Milewski
University of Białystok

MML Identifier: POLYNOM3.

The papers [12], [16], [13], [21], [2], [3], [7], [17], [4], [5], [10], [18], [1], [14], [15], [22], [23], [19], [6], [20], [8], [11], and [9] provide the notation and terminology for this paper.

1. Preliminaries

The following four propositions are true:

(1) Let L be an add-associative right zeroed right complementable non empty loop structure and p be a finite sequence of elements of the carrier of L. If for every natural number i such that $i \in \operatorname{dom} p$ holds $p(i) = 0_L$, then $\sum p = 0_L$.

(2) Let V be an Abelian add-associative right zeroed non empty loop structure and p be a finite sequence of elements of the carrier of V. Then $\sum p = \sum \operatorname{Rev}(p)$.

(3) For every finite sequence p of elements of $\mathbb{R}$ holds $\sum p = \sum \operatorname{Rev}(p)$.

(4) For every finite sequence p of elements of $\mathbb{N}$ and for every natural number i such that $i \in \operatorname{dom} p$ holds $\sum p \geqslant p(i)$.

Let D be a non empty set, let i be a natural number, and let p be a finite sequence of elements of D. Then $p_{\restriction i}$ is a finite sequence of elements of D.

Let D be a non empty set and let a, b be elements of D. Then $\langle a, b \rangle$ is an element of D^2.

Let D be a non empty set, let k, n be natural numbers, let p be an element of D^k, and let q be an element of D^n. Then $p \mathbin{^\frown} q$ is an element of D^{k+n}.

Let D be a non empty set and let n be a natural number. One can check that every finite sequence of elements of D^n is finite sequence yielding.

ISSN 1426–2630

Let D be a non empty set, let k, n be natural numbers, let p be a finite sequence of elements of D^k, and let q be a finite sequence of elements of D^n. Then $p \frown q$ is an element of $(D^{k+n})^*$.

In this article we present several logical schemes. The scheme *NonUniqPiSeqExD* deals with a non empty set $\mathcal{A}$, a natural number $\mathcal{B}$, and a binary predicate $\mathcal{P}$, and states that:

> There exists a finite sequence p of elements of $\mathcal{A}$ such that $\operatorname{dom} p = \operatorname{Seg} \mathcal{B}$ and for every natural number k such that $k \in \operatorname{Seg} \mathcal{B}$ holds $\mathcal{P}[k, \pi_k p]$

provided the following condition is satisfied:

- For every natural number k such that $k \in \operatorname{Seg} \mathcal{B}$ there exists an element d of $\mathcal{A}$ such that $\mathcal{P}[k, d]$.

The scheme *SeqOfSeqLambdaD* deals with a non empty set $\mathcal{A}$, a natural number $\mathcal{B}$, a unary functor $\mathcal{F}$ yielding a natural number, and a binary functor $\mathcal{G}$ yielding an element of $\mathcal{A}$, and states that:

> There exists a finite sequence p of elements of $\mathcal{A}^*$ such that
> (i) $\operatorname{len} p = \mathcal{B}$, and
> (ii) for every natural number k such that $k \in \operatorname{Seg} \mathcal{B}$ holds $\operatorname{len} \pi_k p = \mathcal{F}(k)$ and for every natural number n such that $n \in \operatorname{dom} \pi_k p$ holds $(\pi_k p)(n) = \mathcal{G}(k, n)$

for all values of the parameters.

2. The Lexicographic Order of Finite Sequences

Let n be a natural number and let p, q be elements of $\mathbb{N}^n$. The predicate $p < q$ is defined by the condition (Def. 1).

(Def. 1) There exists a natural number i such that $i \in \operatorname{Seg} n$ and $p(i) < q(i)$ and for every natural number k such that $1 \leqslant k$ and $k < i$ holds $p(k) = q(k)$.

Let us note that the predicate $p < q$ is antisymmetric. We introduce $q > p$ as a synonym of $p < q$.

Let n be a natural number and let p, q be elements of $\mathbb{N}^n$. The predicate $p \leqslant q$ is defined by:

(Def. 2) $p < q$ or $p = q$.

Let us note that the predicate $p \leqslant q$ is reflexive. We introduce $q \geqslant p$ as a synonym of $p \leqslant q$.

We now state three propositions:

(5) Let n be a natural number and p, q, r be elements of $\mathbb{N}^n$. Then
(i) if $p < q$ and $q < r$, then $p < r$, and
(ii) if $p < q$ and $q \leqslant r$ or $p \leqslant q$ and $q < r$ or $p \leqslant q$ and $q \leqslant r$, then $p \leqslant r$.

(6) Let n be a natural number and p, q be elements of $\mathbb{N}^n$. Suppose $p \neq q$. Then there exists a natural number i such that $i \in \operatorname{Seg} n$ and $p(i) \neq q(i)$ and for every natural number k such that $1 \leqslant k$ and $k < i$ holds $p(k) = q(k)$.

(7) For every natural number n and for all elements p, q of $\mathbb{N}^n$ holds $p \leqslant q$ or $p > q$.

Let n be a natural number. The functor TuplesOrder n yielding an order in $\mathbb{N}^n$ is defined by:

(Def. 3) For all elements p, q of $\mathbb{N}^n$ holds $\langle p, q \rangle \in \text{TuplesOrder}\, n$ iff $p \leqslant q$.

Let n be a natural number. Note that TuplesOrder n is linear-order.

3. Decomposition of Natural Numbers

Let i be a non empty natural number and let n be a natural number. The functor $\text{Decomp}(n, i)$ yielding a finite sequence of elements of $\mathbb{N}^i$ is defined by:

(Def. 4) There exists a finite subset A of $\mathbb{N}^i$ such that $\text{Decomp}(n, i) = \text{SgmX}(\text{TuplesOrder}\, i, A)$ and for every element p of $\mathbb{N}^i$ holds $p \in A$ iff $\sum p = n$.

Let i be a non empty natural number and let n be a natural number. Note that $\text{Decomp}(n, i)$ is non empty one-to-one and finite sequence yielding.

The following propositions are true:

(8) For every natural number n holds $\operatorname{len} \text{Decomp}(n, 1) = 1$.

(9) For every natural number n holds $\operatorname{len} \text{Decomp}(n, 2) = n + 1$.

(10) For every natural number n holds $\text{Decomp}(n, 1) = \langle \langle n \rangle \rangle$.

(11) For all natural numbers i, j, n, k_1, k_2 such that $(\text{Decomp}(n, 2))(i) = \langle k_1, n -' k_1 \rangle$ and $(\text{Decomp}(n, 2))(j) = \langle k_2, n -' k_2 \rangle$ holds $i < j$ iff $k_1 < k_2$.

(12) For all natural numbers i, n, k_1, k_2 such that $(\text{Decomp}(n, 2))(i) = \langle k_1, n -' k_1 \rangle$ and $(\text{Decomp}(n, 2))(i + 1) = \langle k_2, n -' k_2 \rangle$ holds $k_2 = k_1 + 1$.

(13) For every natural number n holds $(\text{Decomp}(n, 2))(1) = \langle 0, n \rangle$.

(14) For all natural numbers n, i such that $i \in \operatorname{Seg}(n + 1)$ holds $(\text{Decomp}(n, 2))(i) = \langle i -' 1, (n + 1) -' i \rangle$.

Let L be a non empty groupoid, let p, q, r be sequences of L, and let t be a finite sequence of elements of $\mathbb{N}^3$. The functor $\text{prodTuples}(p, q, r, t)$ yielding an element of (the carrier of L)* is defined by:

(Def. 5) $\operatorname{len} \text{prodTuples}(p, q, r, t) = \operatorname{len} t$ and for every natural number k such that $k \in \operatorname{Seg} \operatorname{len} t$ holds $(\text{prodTuples}(p, q, r, t))(k) = p(\pi_1 \pi_k t) \cdot q(\pi_2 \pi_k t) \cdot r(\pi_3 \pi_k t)$.

One can prove the following propositions:

(15) Let L be a non empty groupoid, p, q, r be sequences of L, t be a finite sequence of elements of $\mathbb{N}^3$, P be a permutation of $\operatorname{dom} t$, and t_1 be a finite sequence of elements of $\mathbb{N}^3$. If $t_1 = t \cdot P$, then $\operatorname{prodTuples}(p, q, r, t_1) = \operatorname{prodTuples}(p, q, r, t) \cdot P$.

(16) For every set D and for every finite sequence f of elements of D^* and for every natural number i holds $\overline{\overline{f \restriction i}} = \overline{\overline{f}} \restriction i$.

(17) Let p be a finite sequence of elements of $\mathbb{R}$ and q be a finite sequence of elements of $\mathbb{N}$. If $p = q$, then for every natural number i holds $p \restriction i = q \restriction i$.

(18) For every finite sequence p of elements of $\mathbb{N}$ and for all natural numbers i, j such that $i \leqslant j$ holds $\sum(p \restriction i) \leqslant \sum(p \restriction j)$.

(19) Let p be a finite sequence of elements of $\mathbb{R}$ and i be a natural number. If $i < \operatorname{len} p$, then $p \restriction (i+1) = (p \restriction i) \frown \langle p(i+1) \rangle$.

(20) Let p be a finite sequence of elements of $\mathbb{R}$ and i be a natural number. If $i < \operatorname{len} p$, then $\sum(p \restriction (i+1)) = \sum(p \restriction i) + p(i+1)$.

(21) Let p be a finite sequence of elements of $\mathbb{N}$ and i, j, k_1, k_2 be natural numbers. Suppose $i < \operatorname{len} p$ and $j < \operatorname{len} p$ and $p(i+1) \neq 0$ and $p(j+1) \neq 0$ and $1 \leqslant k_1$ and $1 \leqslant k_2$ and $k_1 \leqslant p(i+1)$ and $k_2 \leqslant p(j+1)$ and $\sum(p \restriction i) + k_1 = \sum(p \restriction j) + k_2$. Then $i = j$ and $k_1 = k_2$.

(22) Let D_1, D_2 be sets, f_1 be a finite sequence of elements of ${D_1}^*$, f_2 be a finite sequence of elements of ${D_2}^*$, and i_1, i_2, j_1, j_2 be natural numbers. Suppose $i_1 \in \operatorname{dom} f_1$ and $i_2 \in \operatorname{dom} f_2$ and $j_1 \in \operatorname{dom} f_1(i_1)$ and $j_2 \in \operatorname{dom} f_2(i_2)$ and $\overline{\overline{f_1}} = \overline{\overline{f_2}}$ and $\sum(\overline{\overline{f_1}} \restriction (i_1 -' 1)) + j_1 = \sum(\overline{\overline{f_2}} \restriction (i_2 -' 1)) + j_2$. Then $i_1 = i_2$ and $j_1 = j_2$.

4. Polynomials

Let L be a non empty zero structure. A Polynomial of L is an algebraic sequence of L.

The following proposition is true

(23) Let L be a non empty zero structure, p be a Polynomial of L, and n be a natural number. Then $n \geqslant \operatorname{len} p$ if and only if the length of p is at most n.

Now we present two schemes. The scheme *PolynomialLambda* deals with a non empty loop structure $\mathcal{A}$, a natural number $\mathcal{B}$, and a unary functor $\mathcal{F}$ yielding an element of the carrier of $\mathcal{A}$, and states that:

> There exists a Polynomial p of $\mathcal{A}$ such that $\operatorname{len} p \leqslant \mathcal{B}$ and for every natural number n such that $n < \mathcal{B}$ holds $p(n) = \mathcal{F}(n)$

for all values of the parameters.

The scheme *ExDLoopStrSeq* deals with a non empty loop structure $\mathcal{A}$ and a unary functor $\mathcal{F}$ yielding an element of the carrier of $\mathcal{A}$, and states that:

> There exists a sequence S of $\mathcal{A}$ such that for every natural number n holds $S(n) = \mathcal{F}(n)$

for all values of the parameters.

Let L be a non empty loop structure and let p, q be sequences of L. The functor $p + q$ yielding a sequence of L is defined by:

(Def. 6) For every natural number n holds $(p + q)(n) = p(n) + q(n)$.

Let L be a right zeroed non empty loop structure and let p, q be Polynomials of L. Note that $p + q$ is finite-Support.

One can prove the following two propositions:

(24) Let L be a right zeroed non empty loop structure, p, q be Polynomials of L, and n be a natural number. Suppose the length of p is at most n and the length of q is at most n. Then the length of $p + q$ is at most n.

(25) For every right zeroed non empty loop structure L and for all Polynomials p, q of L holds $\operatorname{support}(p + q) \subseteq \operatorname{support} p \cup \operatorname{support} q$.

Let L be an Abelian non empty loop structure and let p, q be sequences of L. Let us note that the functor $p + q$ is commutative.

One can prove the following proposition

(26) For every add-associative non empty loop structure L and for all sequences p, q, r of L holds $(p + q) + r = p + (q + r)$.

Let L be a non empty loop structure and let p be a sequence of L. The functor $-p$ yielding a sequence of L is defined by:

(Def. 7) For every natural number n holds $(-p)(n) = -p(n)$.

Let L be an add-associative right zeroed right complementable non empty loop structure and let p be a Polynomial of L. Observe that $-p$ is finite-Support.

Let L be a non empty loop structure and let p, q be sequences of L. The functor $p - q$ yields a sequence of L and is defined as follows:

(Def. 8) $p - q = p + -q$.

Let L be an add-associative right zeroed right complementable non empty loop structure and let p, q be Polynomials of L. Note that $p - q$ is finite-Support.

Next we state the proposition

(27) Let L be a non empty loop structure, p, q be sequences of L, and n be a natural number. Then $(p - q)(n) = p(n) - q(n)$.

Let L be a non empty zero structure. The functor $\mathbf{0}.\,L$ yielding a sequence of L is defined as follows:

(Def. 9) $\mathbf{0}.\,L = \mathbb{N} \longmapsto 0_L$.

Let L be a non empty zero structure. One can check that $\mathbf{0}.\,L$ is finite-Support.

We now state three propositions:

(28) For every non empty zero structure L and for every natural number n holds $(\mathbf{0}. L)(n) = 0_L$.

(29) For every right zeroed non empty loop structure L and for every sequence p of L holds $p + \mathbf{0}. L = p$.

(30) Let L be an add-associative right zeroed right complementable non empty loop structure and p be a sequence of L. Then $p - p = \mathbf{0}. L$.

Let L be a non empty multiplicative loop with zero structure. The functor $\mathbf{1}. L$ yielding a sequence of L is defined by:

(Def. 10) $\mathbf{1}. L = \mathbf{0}. L +\cdot (0, \mathbf{1}_L)$.

Let L be a non empty multiplicative loop with zero structure. Observe that $\mathbf{1}. L$ is finite-Support.

Next we state the proposition

(31) Let L be a non empty multiplicative loop with zero structure. Then $(\mathbf{1}. L)(0) = \mathbf{1}_L$ and for every natural number n such that $n \neq 0$ holds $(\mathbf{1}. L)(n) = 0_L$.

Let L be a non empty double loop structure and let p, q be sequences of L. The functor $p*q$ yields a sequence of L and is defined by the condition (Def. 11).

(Def. 11) Let i be a natural number. Then there exists a finite sequence r of elements of the carrier of L such that $\operatorname{len} r = i + 1$ and $(p * q)(i) = \sum r$ and for every natural number k such that $k \in \operatorname{dom} r$ holds $r(k) = p(k -' 1) \cdot q((i + 1) -' k)$.

Let L be an add-associative right zeroed right complementable distributive non empty double loop structure and let p, q be Polynomials of L. Note that $p * q$ is finite-Support.

Next we state three propositions:

(32) Let L be an Abelian add-associative right zeroed right complementable right distributive non empty double loop structure and p, q, r be sequences of L. Then $p * (q + r) = p * q + p * r$.

(33) Let L be an Abelian add-associative right zeroed right complementable left distributive non empty double loop structure and p, q, r be sequences of L. Then $(p + q) * r = p * r + q * r$.

(34) Let L be an Abelian add-associative right zeroed right complementable unital associative distributive non empty double loop structure and p, q, r be sequences of L. Then $(p * q) * r = p * (q * r)$.

Let L be an Abelian add-associative right zeroed commutative non empty double loop structure and let p, q be sequences of L. Let us observe that the functor $p * q$ is commutative.

We now state two propositions:

(35) Let L be an add-associative right zeroed right complementable right distributive non empty double loop structure and p be a sequence of L.

Then $p * \mathbf{0}. L = \mathbf{0}. L$.

(36) Let L be an add-associative right zeroed right unital right complementable right distributive non empty double loop structure and p be a sequence of L. Then $p * \mathbf{1}. L = p$.

5. The Ring of Polynomials

Let L be an add-associative right zeroed right complementable distributive non empty double loop structure. The functor Polynom-Ring L yields a strict non empty double loop structure and is defined by the conditions (Def. 12).

(Def. 12)(i) For every set x holds $x \in$ the carrier of Polynom-Ring L iff x is a Polynomial of L,

(ii) for all elements x, y of the carrier of Polynom-Ring L and for all sequences p, q of L such that $x = p$ and $y = q$ holds $x + y = p + q$,

(iii) for all elements x, y of the carrier of Polynom-Ring L and for all sequences p, q of L such that $x = p$ and $y = q$ holds $x \cdot y = p * q$,

(iv) $0_{\text{Polynom-Ring}\, L} = \mathbf{0}. L$, and

(v) $\mathbf{1}_{\text{Polynom-Ring}\, L} = \mathbf{1}. L$.

Let L be an Abelian add-associative right zeroed right complementable distributive non empty double loop structure. Observe that Polynom-Ring L is Abelian.

Let L be an add-associative right zeroed right complementable distributive non empty double loop structure. One can check the following observations:

* Polynom-Ring L is add-associative,
* Polynom-Ring L is right zeroed, and
* Polynom-Ring L is right complementable.

Let L be an Abelian add-associative right zeroed right complementable commutative distributive non empty double loop structure. Note that Polynom-Ring L is commutative.

Let L be an Abelian add-associative right zeroed right complementable unital associative distributive non empty double loop structure. Observe that Polynom-Ring L is associative.

Let L be an add-associative right zeroed right complementable right unital distributive non empty double loop structure. Observe that Polynom-Ring L is right unital.

Let L be an Abelian add-associative right zeroed right complementable distributive non empty double loop structure. Note that Polynom-Ring L is right distributive and Polynom-Ring L is left distributive.

References

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

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

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

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

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

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

[7] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(**2**):241–245, 1996.

[8] Agata Darmochwał and Yatsuka Nakamura. The topological space $\mathcal{E}^2_{\mathrm{T}}$. Arcs, line segments and special polygonal arcs. *Formalized Mathematics*, 2(**5**):617–621, 1991.

[9] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[10] Jarosław Kotowicz and Yatsuka Nakamura. Introduction to Go-board - part I. *Formalized Mathematics*, 3(**1**):107–115, 1992.

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

[12] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.

[13] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

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

[15] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.

[16] Wojciech Skaba and Michał Muzalewski. From double loops to fields. *Formalized Mathematics*, 2(**1**):185–191, 1991.

[17] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.

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

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

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

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

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

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

Received April 17, 2000