JOURNAL OF FORMALIZED MATHEMATICS
Volume 12, Released 2000, Published 2003
Inst. of Computer Science, Univ. of Białystok

The Ring of Polynomials

Robert Milewski
University of Białystok

MML Identifier: POLYNOM3.

WWW: http://mizar.org/JFM/Vol12/polynom3.html

The articles [25], [10], [32], [26], [2], [33], [35], [34], [1], [14], [7], [9], [8], [27], [19], [4], [11], [31], [13], [29], [15], [6], [12], [36], [17], [3], [16], [20], [22], [30], [5], [28], [18], [23], [24], and [21] 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 $\sum p \geq p(i)$.

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 $p \frown q$ is an element of D^{k+n}.

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

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 $(D^{k+n})^*$.

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 $\operatorname{len}(p_k) = \mathcal{F}(k)$ and for every natural number n such that $n \in \operatorname{dom}(p_k)$ holds $p_k(n) = \mathcal{G}(k, n)$

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 $i \in \mathrm{Seg}\, n$ and $p(i) < q(i)$ and for every natural number k such that $1 \leq k$ 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 $p \leq q$ is defined as follows:

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

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

One can prove the following 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 $q \leq r$ or $p \leq q$ and $q < r$ or $p \leq q$ and $q \leq r$, then $p \leq r$.

(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 $i \in \mathrm{Seg}\, n$ and $p(i) \neq q(i)$ and for every natural number k such that $1 \leq k$ 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 $p \leq q$ or $p > q$.

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

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

Let n be a natural number. Observe that $\mathrm{TuplesOrder}\, n$ 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 $\mathrm{Decomp}(n, i)$ 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 $\mathrm{Decomp}(n, i) = \mathrm{SgmX}(\mathrm{TuplesOrder}\, i, A)$ 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 $\mathrm{Decomp}(n, i)$ is non empty, one-to-one, and finite sequence yielding.

One can prove the following propositions:

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

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

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

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

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

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

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

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 $\mathrm{prodTuples}(p,q,r,t)$ yielding an element of (the carrier of $L)^*$ is defined as follows:

(Def. 5) $\mathrm{len}\,\mathrm{prodTuples}(p,q,r,t) = \mathrm{len}\,t$ and for every natural number k such that $k \in \mathrm{dom}\,t$ holds $(\mathrm{prodTuples}(p,q,r,t))(k) = p((t_k)_1) \cdot q((t_k)_2) \cdot r((t_k)_3)$.

The following propositions are true:

(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 $\mathrm{dom}\,t$, and t_1 be a finite sequence of elements of $\mathbb{N}^3$. If $t_1 = t \cdot P$, then $\mathrm{prodTuples}(p,q,r,t_1) = \mathrm{prodTuples}(p,q,r,t) \cdot P$.

(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 $i \leq j$ holds $\sum(p \restriction i) \leq \sum(p \restriction j)$.

(19) Let D be a set, p be a finite sequence of elements of D, and i be a natural number. If $i < \mathrm{len}\,p$, 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 $i < \mathrm{len}\,p$, 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 $i < \mathrm{len}\,p$ and $j < \mathrm{len}\,p$ and $1 \leq k_1$ and $1 \leq k_2$ and $k_1 \leq p(i+1)$ and $k_2 \leq p(j+1)$ 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 $i_1 \in \mathrm{dom}\,f_1$ and $i_2 \in \mathrm{dom}\,f_2$ and $j_1 \in \mathrm{dom}\,f_1(i_1)$ and $j_2 \in \mathrm{dom}\,f_2(i_2)$ 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.

Next we state the proposition

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

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

There exists a polynomial p of $\mathcal{A}$ such that $\mathrm{len}\,p \leq \mathcal{B}$ 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 $\mathcal{A}$, 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 as follows:

(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. Observe 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 $\mathrm{support}(p+q) \subseteq \mathrm{support}\, p \cup \mathrm{support}\, q$.

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.

The following proposition is true

(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 as follows:

(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. One can check that $-p$ is finite-Support.

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

(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.

One can prove the following 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 by:

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

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

We now 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.

One can prove the following 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 notice that the functor $p*q$ is commutative.

One can prove the following 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 yielding a strict non empty double loop structure 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 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 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. One can verify 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. One can verify 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. One can verify 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. One can check that Polynom-Ring L is distributive.

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/card_1.html.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[3] Grzegorz Bancerek. Joining of decorated trees. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/trees_4.html.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finseq_1.html.

[5] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on trees. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/dtconstr.html.

[6] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/binop_1.html.

[7] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_1.html.

[8] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[9] Czesław Byliński. Partial functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/partfun1.html.

[10] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/zfmisc_1.html.

[11] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseq_2.html.

[12] Czesław Byliński. The sum and product of finite sequences of real numbers. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/rvsum_1.html.

[13] Czesław Byliński. Some properties of restrictions of finite sequences. *Journal of Formalized Mathematics*, 7, 1995. http://mizar.org/JFM/Vol7/finseq_5.html.

[14] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finset_1.html.

[15] Agata Darmochwał and Yatsuka Nakamura. The topological space $\mathcal{E}^2_{\mathrm{T}}$. Arcs, line segments and special polygonal arcs. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/topreal1.html.

[16] Andrzej Kondracki. The Chinese Remainder Theorem. *Journal of Formalized Mathematics*, 9, 1997. http://mizar.org/JFM/Vol9/wsierp_1.html.

[17] Jarosław Kotowicz and Yatsuka Nakamura. Introduction to Go-Board — part I. *Journal of Formalized Mathematics*, 4, 1992. http://mizar.org/JFM/Vol4/goboard1.html.

[18] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/vectsp_1.html.

[19] Beata Madras. On the concept of the triangulation. *Journal of Formalized Mathematics*, 7, 1995. http://mizar.org/JFM/Vol7/triang_1.html.

[20] Robert Milewski. Associated matrix of linear map. *Journal of Formalized Mathematics*, 7, 1995. http://mizar.org/JFM/Vol7/matrlin.html.

[21] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequence over ring and left-, right-, and bi-modules over a ring. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/algseq_1.html.

[22] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/binarith.html.

[23] Jan Popiołek. Real normed space. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/normsp_1.html.

[24] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Journal of Formalized Mathematics*, 11, 1999. http://mizar.org/JFM/Vol11/polynom1.html.

[25] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. `http://mizar.org/JFM/Axiomatics/tarski.html`.

[26] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. `http://mizar.org/JFM/Addenda/numbers.html`.

[27] Wojciech A. Trybulec. Partially ordered sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/orders_1.html`.

[28] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/rlvect_1.html`.

[29] Wojciech A. Trybulec. Binary operations on finite sequences. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finsop_1.html`.

[30] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/group_1.html`.

[31] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseq_4.html`.

[32] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/subset_1.html`.

[33] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relat_1.html`.

[34] Edmund Woronowicz. Relations defined on sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relset_1.html`.

[35] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relat_2.html`.

[36] Katarzyna Zawadzka. Sum and product of finite sequences of elements of a field. *Journal of Formalized Mathematics*, 4, 1992. `http://mizar.org/JFM/Vol4/fvsum_1.html`.

Received April 17, 2000

Published January 2, 2004