FORMALIZED MATHEMATICS
Volume 9, Number 1, 2001
University of Białystok

Multivariate Polynomials with Arbitrary Number of Variables[1]

Piotr Rudnicki
University of Alberta
Edmonton

Andrzej Trybulec
University of Białystok

Summary. The goal of this article is to define multivariate polynomials in arbitrary number of indeterminates and then to prove that they constitute a ring (over appropriate structure of coefficients).

The introductory section includes quite a number of auxiliary lemmas related to many different parts of the MML. The second section characterizes the sequence flattening operation, introduced in [7], but so far lacking theorems about its fundamental properties.

We first define formal power series in arbitrary number of variables. The auxiliary concept on which the construction of formal power series is based is the notion of a bag. A bag of a set X is a natural function on X which is zero almost everywhere. The elements of X play the role of formal variables and a bag gives their exponents thus forming a power product. Series are defined for an ordered set of variables (we use ordinal numbers). A series in o variables over a structure S is a function assigning an element of the carrier of S (coefficient) to each bag of o.

We define the operations of addition, complement and multiplication for formal power series and prove their properties which depend on assumed properties of the structure from which the coefficients are taken. (We would like to note that proving associativity of multiplication turned out to be technically complicated.)

Polynomial is defined as a formal power series with finite number of non zero coefficients. In conclusion, the ring of polynomials is defined.

MML Identifier: `POLYNOM1`.

The terminology and notation used in this paper are introduced in the following articles: [24], [23], [10], [35], [1], [3], [7], [6], [11], [31], [15], [25], [12], [13], [8],

[1]This work has been supported by NSERC Grant OGP9207 and NATO CRG 951368.

ISSN 1426–2630

[38], [29], [22], [5], [18], [2], [30], [33], [4], [28], [9], [36], [37], [32], [19], [26], [34], [27], [16], [21], [20], [17], and [14].

1. Basics

The following propositions are true:

(1) For all natural numbers i, j holds $\cdot_{\mathbb{N}}(i, j) = i \cdot j$.

(2) Let X be a set, A be a non empty set, F be a binary operation on A, f be a function from X into A, and x be an element of A. Then $\mathrm{dom}(F^{\circ}(f, x)) = X$.

(3) For all natural numbers a, b, c holds $a -' b -' c = a -' (b + c)$.

(4) For every set X and for every binary relation R such that $\mathrm{field}\, R \subseteq X$ holds R is a binary relation on X.

(5) Let K be a non empty loop structure and p_1, p_2 be finite sequences of elements of the carrier of K. If $\mathrm{dom}\, p_1 = \mathrm{dom}\, p_2$, then $\mathrm{dom}(p_1 + p_2) = \mathrm{dom}\, p_1$.

(6) For every function f and for all sets x, y holds $\mathrm{rng}(f +\cdot (x, y)) \subseteq \mathrm{rng}\, f \cup \{y\}$.

Let A, B be sets, let f be a function from A into B, let x be a set, and let y be an element of B. Then $f +\cdot (x, y)$ is a function from A into B.

Let X be a set, let f be a many sorted set indexed by X, and let x, y be sets. Then $f +\cdot (x, y)$ is a many sorted set indexed by X.

Next we state the proposition

(7) For every one-to-one function f holds $\overline{\overline{(f\ \mathbf{qua}\ \mathrm{set})}} = \overline{\overline{\mathrm{rng}\, f}}$.

Let A be a non empty set, let F, G be binary operations on A, and let z, u be elements of A. Observe that $\langle A, F, G, z, u \rangle$ is non empty.

Let A be a set, let X be a set, let D be a non empty set of finite sequences of A, let p be a partial function from X to D, and let i be a set. Then $\pi_i p$ is an element of D.

Let X be a set and let S be a 1-sorted structure.

(Def. 1) A function from X into the carrier of S is said to be a function from X into S.

Let X be a set. Note that there exists an order in X which is linear-order and well-ordering.

The following propositions are true:

(8) Let X be a non empty set, A be a non empty finite subset of X, R be an order in X, and x be an element of X. Suppose $x \in A$ and R linearly orders A and for every element y of X such that $y \in A$ holds $\langle x, y \rangle \in R$. Then $\pi_1\, \mathrm{SgmX}(R, A) = x$.

(9) Let X be a non empty set, A be a non empty finite subset of X, R be an order in X, and x be an element of X. Suppose $x \in A$ and R linearly orders A and for every element y of X such that $y \in A$ holds $\langle y, x\rangle \in R$. Then $\pi_{\mathrm{len}\,\mathrm{SgmX}(R,A)}\,\mathrm{SgmX}(R, A) = x$.

Let X be a non empty set, let A be a non empty finite subset of X, and let R be linear-order order in X. One can verify that $\mathrm{SgmX}(R, A)$ is non empty and one-to-one.

Let us observe that $\emptyset$ is finite sequence yielding.

Let us observe that there exists a finite sequence which is finite sequence yielding.

Let F, G be finite sequence yielding finite sequences. Then $F \frown G$ is a finite sequence yielding finite sequence.

Let D be a set. Note that every finite sequence of elements of D^* is finite sequence yielding.

Let i be a natural number and let f be a finite sequence. Note that $i \mapsto f$ is finite sequence yielding.

Let us observe that every function which is finite sequence yielding is also function yielding.

Let F be a finite sequence yielding finite sequence and let x be a set. Note that $F(x)$ is finite sequence-like.

Let F be a finite sequence. Observe that $\overline{\overline{F}}$ is finite sequence-like.

Let us observe that there exists a finite sequence which is cardinal yielding.

We now state the proposition

(10) Let f be a function. Then f is cardinal yielding if and only if for every set y such that $y \in \mathrm{rng}\, f$ holds y is a cardinal number.

Let F, G be cardinal yielding finite sequences. Note that $F \frown G$ is cardinal yielding.

Let us note that every finite sequence of elements of $\mathbb{N}$ is cardinal yielding.

Let us observe that there exists a finite sequence of elements of $\mathbb{N}$ which is cardinal yielding.

Let D be a set and let F be a finite sequence of elements of D^*. Then $\overline{\overline{F}}$ is a cardinal yielding finite sequence of elements of $\mathbb{N}$.

Let F be a finite sequence of elements of $\mathbb{N}$ and let i be a natural number. Observe that $F{\restriction}i$ is cardinal yielding.

We now state the proposition

(11) For every function F and for every set X holds $\overline{\overline{F{\restriction}X}} = \overline{\overline{F}}{\restriction}X$.

Let F be an empty function. One can verify that $\overline{\overline{F}}$ is empty.

Next we state two propositions:

(12) For every set p holds $\overline{\overline{\langle p\rangle}} = \langle \overline{\overline{p}}\rangle$.

(13) For all finite sequences F, G holds $\overline{\overline{F \frown G}} = \overline{\overline{F}} \frown \overline{\overline{G}}$.

Let X be a set. Note that ε_X is finite sequence yielding.

Let f be a finite sequence. Observe that $\langle f \rangle$ is finite sequence yielding.

One can prove the following proposition

(14) Let f be a function. Then f is finite sequence yielding if and only if for every set y such that $y \in \operatorname{rng} f$ holds y is a finite sequence.

Let F, G be finite sequence yielding finite sequences. One can verify that $F \frown G$ is finite sequence yielding.

Next we state four propositions:

(15) Let L be a non empty loop structure and F be a finite sequence of elements of (the carrier of L)*. Then $\operatorname{dom} \sum F = \operatorname{dom} F$.

(16) Let L be a non empty loop structure and F be a finite sequence of elements of (the carrier of L)*. Then $\sum(\varepsilon_{(\text{the carrier of } L)^*}) = \varepsilon_{(\text{the carrier of } L)}$.

(17) For every non empty loop structure L and for every element p of (the carrier of L)* holds $\langle \sum p \rangle = \sum \langle p \rangle$.

(18) Let L be a non empty loop structure and F, G be finite sequences of elements of (the carrier of L)*. Then $\sum(F \frown G) = (\sum F) \frown \sum G$.

Let L be a non empty groupoid, let a be an element of the carrier of L, and let p be a finite sequence of elements of the carrier of L. The functor $a \cdot p$ yielding a finite sequence of elements of the carrier of L is defined by:

(Def. 2) $\operatorname{dom}(a \cdot p) = \operatorname{dom} p$ and for every set i such that $i \in \operatorname{dom} p$ holds $\pi_i(a \cdot p) = a \cdot \pi_i p$.

The functor $p \cdot a$ yielding a finite sequence of elements of the carrier of L is defined as follows:

(Def. 3) $\operatorname{dom}(p \cdot a) = \operatorname{dom} p$ and for every set i such that $i \in \operatorname{dom} p$ holds $\pi_i(p \cdot a) = \pi_i p \cdot a$.

The following propositions are true:

(19) Let L be a non empty groupoid and a be an element of the carrier of L. Then $a \cdot \varepsilon_{(\text{the carrier of } L)} = \varepsilon_{(\text{the carrier of } L)}$.

(20) Let L be a non empty groupoid and a be an element of the carrier of L. Then $\varepsilon_{(\text{the carrier of } L)} \cdot a = \varepsilon_{(\text{the carrier of } L)}$.

(21) For every non empty groupoid L and for all elements a, b of the carrier of L holds $a \cdot \langle b \rangle = \langle a \cdot b \rangle$.

(22) For every non empty groupoid L and for all elements a, b of the carrier of L holds $\langle b \rangle \cdot a = \langle b \cdot a \rangle$.

(23) Let L be a non empty groupoid, a be an element of the carrier of L, and p, q be finite sequences of elements of the carrier of L. Then $a \cdot (p \frown q) = (a \cdot p) \frown (a \cdot q)$.

(24) Let L be a non empty groupoid, a be an element of the carrier of L, and p, q be finite sequences of elements of the carrier of L. Then $(p \frown q) \cdot a =$

$(p \cdot a) \frown (q \cdot a)$.

We now state two propositions:

(25) Let L be an add-associative right zeroed right complementable left-distributive non empty double loop structure and x be an element of the carrier of L. Then $0_L \cdot x = 0_L$.

(26) Let L be an add-associative right zeroed right complementable right-distributive non empty double loop structure and x be an element of the carrier of L. Then $x \cdot 0_L = 0_L$.

One can verify that every non empty multiplicative loop with zero structure which is non degenerated is also non trivial.

Let us mention that there exists a non empty strict multiplicative loop with zero structure which is unital.

Let us observe that there exists a non empty strict double loop structure which is Abelian, add-associative, right zeroed, right complementable, associative, commutative, distributive, unital, and non trivial.

Next we state three propositions:

(27) Let L be an add-associative right zeroed right complementable unital right-distributive non empty double loop structure. If $0_L = 1_L$, then L is trivial.

(28) Let L be an add-associative right zeroed right complementable unital distributive non empty double loop structure, a be an element of the carrier of L, and p be a finite sequence of elements of the carrier of L. Then $\sum(a \cdot p) = a \cdot \sum p$.

(29) Let L be an add-associative right zeroed right complementable unital distributive non empty double loop structure, a be an element of the carrier of L, and p be a finite sequence of elements of the carrier of L. Then $\sum(p \cdot a) = \sum p \cdot a$.

2. Sequence Flattening

Let D be a set and let F be an empty finite sequence of elements of D^*. Observe that $\mathrm{Flat}(F)$ is empty.

One can prove the following propositions:

(30) For every set D and for every finite sequence F of elements of D^* holds $\mathrm{len}\,\mathrm{Flat}(F) = \sum \overline{\overline{F}}$.

(31) Let D, E be sets, F be a finite sequence of elements of D^*, and G be a finite sequence of elements of E^*. If $\overline{\overline{F}} = \overline{\overline{G}}$, then $\mathrm{len}\,\mathrm{Flat}(F) = \mathrm{len}\,\mathrm{Flat}(G)$.

(32) Let D be a set, F be a finite sequence of elements of D^*, and k be a set. Suppose $k \in \operatorname{dom} \operatorname{Flat}(F)$. Then there exist natural numbers i, j such that $i \in \operatorname{dom} F$ and $j \in \operatorname{dom} F(i)$ and $k = \sum \overline{\overline{F \restriction (i -' 1)}} + j$ and $F(i)(j) = \operatorname{Flat}(F)(k)$.

(33) Let D be a set, F be a finite sequence of elements of D^*, and i, j be natural numbers. If $i \in \operatorname{dom} F$ and $j \in \operatorname{dom} F(i)$, then $\sum \overline{\overline{F \restriction (i -' 1)}} + j \in \operatorname{dom} \operatorname{Flat}(F)$ and $F(i)(j) = \operatorname{Flat}(F)(\sum \overline{\overline{F \restriction (i -' 1)}} + j)$.

(34) Let L be an add-associative right zeroed right complementable non empty loop structure and F be a finite sequence of elements of (the carrier of $L)^*$. Then $\sum \operatorname{Flat}(F) = \sum \sum F$.

(35) Let X, Y be non empty sets, f be a finite sequence of elements of X^*, and v be a function from X into Y. Then $(\operatorname{dom} f \longmapsto v) \circ f$ is a finite sequence of elements of Y^*.

(36) Let X, Y be non empty sets, f be a finite sequence of elements of X^*, and v be a function from X into Y. Then there exists a finite sequence F of elements of Y^* such that $F = (\operatorname{dom} f \longmapsto v) \circ f$ and $v \cdot \operatorname{Flat}(f) = \operatorname{Flat}(F)$.

3. Functions Yielding Natural Numbers

Let us note that $\emptyset$ is natural-yielding.

One can check that there exists a function which is natural-yielding.

Let f be a natural-yielding function and let x be a set. Then $f(x)$ is a natural number.

Let f be a natural-yielding function, let x be a set, and let n be a natural number. Observe that $f +\cdot (x, n)$ is natural-yielding.

Let X be a set. One can check that every function from X into $\mathbb{N}$ is natural-yielding.

Let X be a set. Observe that there exists a many sorted set indexed by X which is natural-yielding.

Let X be a set and let b_1, b_2 be natural-yielding many sorted sets indexed by X. The functor $b_1 + b_2$ yields a many sorted set indexed by X and is defined as follows:

(Def. 5)[2] For every set x holds $(b_1 + b_2)(x) = b_1(x) + b_2(x)$.

Let us note that the functor $b_1 + b_2$ is commutative. The functor $b_1 -' b_2$ yields a many sorted set indexed by X and is defined by:

(Def. 6) For every set x holds $(b_1 -' b_2)(x) = b_1(x) -' b_2(x)$.

Next we state two propositions:

[2]The definition (Def. 4) has been removed.

(37) Let X be a set and b, b_1, b_2 be natural-yielding many sorted sets indexed by X. If for every set x such that $x \in X$ holds $b(x) = b_1(x) + b_2(x)$, then $b = b_1 + b_2$.

(38) Let X be a set and b, b_1, b_2 be natural-yielding many sorted sets indexed by X. If for every set x such that $x \in X$ holds $b(x) = b_1(x) -' b_2(x)$, then $b = b_1 -' b_2$.

Let X be a set and let b_1, b_2 be natural-yielding many sorted sets indexed by X. Observe that $b_1 + b_2$ is natural-yielding and $b_1 -' b_2$ is natural-yielding.

The following two propositions are true:

(39) For every set X and for all natural-yielding many sorted sets b_1, b_2, b_3 indexed by X holds $(b_1 + b_2) + b_3 = b_1 + (b_2 + b_3)$.

(40) For every set X and for all natural-yielding many sorted sets b, c, d indexed by X holds $b -' c -' d = b -' (c + d)$.

4. The Support of a Function

Let f be a function. The functor support f is defined as follows:

(Def. 7) For every set x holds $x \in \mathrm{support}\, f$ iff $f(x) \neq 0$.

One can prove the following proposition

(41) For every function f holds $\mathrm{support}\, f \subseteq \mathrm{dom}\, f$.

Let f be a function. We say that f is finite-support if and only if:

(Def. 8) support f is finite.

We introduce f has finite-support as a synonym of f is finite-support.

Let us mention that $\emptyset$ is finite-support.

Let us note that every function which is finite is also finite-support.

Let us observe that there exists a function which is natural-yielding, finite-support, and non empty.

Let f be a finite-support function. Observe that support f is finite.

Let X be a set. Note that there exists a function from X into $\mathbb{N}$ which is finite-support.

Let f be a finite-support function and let x, y be sets. Observe that $f {+\cdot} (x, y)$ is finite-support.

Let X be a set. One can verify that there exists a many sorted set indexed by X which is natural-yielding and finite-support.

One can prove the following propositions:

(42) For every set X and for all natural-yielding many sorted sets b_1, b_2 indexed by X holds $\mathrm{support}(b_1 + b_2) = \mathrm{support}\, b_1 \cup \mathrm{support}\, b_2$.

(43) For every set X and for all natural-yielding many sorted sets b_1, b_2 indexed by X holds $\mathrm{support}(b_1 -' b_2) \subseteq \mathrm{support}\, b_1$.

Let X be a non empty set, let S be a zero structure, and let f be a function from X into S. The functor Support f yielding a subset of X is defined by:

(Def. 9) For every element x of X holds $x \in \operatorname{Support} f$ iff $f(x) \neq 0_S$.

Let X be a non empty set, let S be a zero structure, and let p be a function from X into S. We say that p is finite-Support if and only if:

(Def. 10) Support p is finite.

We introduce p has finite-Support as a synonym of p is finite-Support.

5. Bags

Let X be a set. A bag of X is a natural-yielding finite-support many sorted set indexed by X.

Let X be a finite set. Observe that every many sorted set indexed by X is finite-support.

Let X be a set and let b_1, b_2 be bag of X. Note that $b_1 + b_2$ is finite-support and $b_1 -' b_2$ is finite-support.

The following proposition is true

(44) For every set X holds $X \longmapsto 0$ is a bag of X.

Let n be an ordinal number and let p, q be bag of n. The predicate $p < q$ is defined as follows:

(Def. 11) There exists an ordinal number k such that $p(k) < q(k)$ and for every ordinal number l such that $l \in k$ holds $p(l) = q(l)$.

Let us note that the predicate $p < q$ is antisymmetric.

Next we state the proposition

(45) For every ordinal number n and for all bag p, q, r of n such that $p < q$ and $q < r$ holds $p < r$.

Let n be an ordinal number and let p, q be bag of n. The predicate $p \leqslant q$ is defined as follows:

(Def. 12) $p < q$ or $p = q$.

Let us note that the predicate $p \leqslant q$ is reflexive.

The following propositions are true:

(46) For every ordinal number n and for all bag p, q, r of n such that $p \leqslant q$ and $q \leqslant r$ holds $p \leqslant r$.

(47) For every ordinal number n and for all bag p, q, r of n such that $p < q$ and $q \leqslant r$ holds $p < r$.

(48) For every ordinal number n and for all bag p, q, r of n such that $p \leqslant q$ and $q < r$ holds $p < r$.

(49) For every ordinal number n and for all bag p, q of n holds $p \leqslant q$ or $q \leqslant p$.

Let X be a set and let d, b be bag of X. We say that d divides b if and only if:

(Def. 13) For every set k holds $d(k) \leqslant b(k)$.

Let us note that the predicate d divides b is reflexive.

One can prove the following propositions:

(50) For every set n and for all bag d, b of n such that for every set k such that $k \in n$ holds $d(k) \leqslant b(k)$ holds d divides b.

(51) For every ordinal number n and for all bag b_1, b_2 of n such that b_1 divides b_2 holds $(b_2 -' b_1) + b_1 = b_2$.

(52) For every set X and for all bag b_1, b_2 of X holds $(b_2 + b_1) -' b_1 = b_2$.

(53) For every ordinal number n and for all bag d, b of n such that d divides b holds $d \leqslant b$.

(54) For every set n and for all bag b, b_1, b_2 of n such that $b = b_1 + b_2$ holds b_1 divides b.

Let X be a set. The functor $\mathrm{Bags}\, X$ is defined as follows:

(Def. 14) For every set x holds $x \in \mathrm{Bags}\, X$ iff x is a bag of X.

Let X be a set. Then $\mathrm{Bags}\, X$ is a subset of $\mathrm{Bags}\, X$.

One can prove the following proposition

(55) $\mathrm{Bags}\, \emptyset = \{\emptyset\}$.

Let X be a set. Note that $\mathrm{Bags}\, X$ is non empty.

Let X be a set and let B be a non empty subset of $\mathrm{Bags}\, X$. We see that the element of B is a bag of X.

Let n be a set, let L be a non empty 1-sorted structure, let p be a function from $\mathrm{Bags}\, n$ into L, and let x be a bag of n. Then $p(x)$ is an element of L.

Let X be a set. The functor $\mathrm{EmptyBag}\, X$ yielding an element of $\mathrm{Bags}\, X$ is defined by:

(Def. 15) $\mathrm{EmptyBag}\, X = X \longmapsto 0$.

The following propositions are true:

(56) For all sets X, x holds $(\mathrm{EmptyBag}\, X)(x) = 0$.

(57) For every set X and for every bag b of X holds $b + \mathrm{EmptyBag}\, X = b$.

(58) For every set X and for every bag b of X holds $b -' \mathrm{EmptyBag}\, X = b$.

(59) For every set X and for every bag b of X holds $\mathrm{EmptyBag}\, X -' b = \mathrm{EmptyBag}\, X$.

(60) For every set X and for every bag b of X holds $b -' b = \mathrm{EmptyBag}\, X$.

(61) For every set n and for all bag b_1, b_2 of n such that b_1 divides b_2 and $b_2 -' b_1 = \mathrm{EmptyBag}\, n$ holds $b_2 = b_1$.

(62) For every set n and for every bag b of n such that b divides $\mathrm{EmptyBag}\, n$ holds $\mathrm{EmptyBag}\, n = b$.

(63) For every set n and for every bag b of n holds $\mathrm{EmptyBag}\, n$ divides b.

(64) For every ordinal number n and for every bag b of n holds EmptyBag $n \leqslant b$.

Let n be an ordinal number. The functor BagOrder n yields an order in Bags n and is defined as follows:

(Def. 16) For all bag p, q of n holds $\langle p, q\rangle \in$ BagOrder n iff $p \leqslant q$.

Let n be an ordinal number. Note that BagOrder n is linear-order.

Let X be a set and let f be a function from X into $\mathbb{N}$. The functor NatMinor f yielding a subset of $\mathbb{N}^X$ is defined by the condition (Def. 17).

(Def. 17) Let g be a natural-yielding many sorted set indexed by X. Then $g \in$ NatMinor f if and only if for every set x such that $x \in X$ holds $g(x) \leqslant f(x)$.

Next we state the proposition

(65) For every set X and for every function f from X into $\mathbb{N}$ holds $f \in$ NatMinor f.

Let X be a set and let f be a function from X into $\mathbb{N}$. Observe that NatMinor f is non empty and functional.

Let X be a set and let f be a function from X into $\mathbb{N}$. One can verify that every element of NatMinor f is natural-yielding.

The following proposition is true

(66) For every set X and for every finite-support function f from X into $\mathbb{N}$ holds NatMinor $f \subseteq$ Bags X.

Let X be a set and let f be a finite-support function from X into $\mathbb{N}$. Then support f is an element of Fin X.

The following proposition is true

(67) For every non empty set X and for every finite-support function f from X into $\mathbb{N}$ holds $\overline{\overline{\mathrm{NatMinor}\, f}} = \cdot_{\mathbb{N}}\text{-}\sum_{\mathrm{support}\, f}(+_{\mathbb{N}})^{\circ}(f, 1)$.

Let X be a set and let f be a finite-support function from X into $\mathbb{N}$. One can verify that NatMinor f is finite.

Let n be an ordinal number and let b be a bag of n. The functor divisors b yields a finite sequence of elements of Bags n and is defined by the condition (Def. 18).

(Def. 18) There exists a non empty finite subset S of Bags n such that divisors $b =$ SgmX(BagOrder n, S) and for every bag p of n holds $p \in S$ iff p divides b.

Let n be an ordinal number and let b be a bag of n. One can check that divisors b is non empty and one-to-one.

The following four propositions are true:

(68) Let n be an ordinal number, i be a natural number, and b be a bag of n. If $i \in$ dom divisors b, then π_i divisors b **qua** element of Bags n divides b.

(69) For every ordinal number n and for every bag b of n holds π_1 divisors $b =$ EmptyBag n and $\pi_{\mathrm{len\,divisors}\,b}$ divisors $b = b$.

(70) Let n be an ordinal number, i be a natural number, and b, b_1, b_2 be bag of n. If $i > 1$ and $i <$ len divisors b, then π_i divisors $b \neq$ EmptyBag n and π_i divisors $b \neq b$.

(71) For every ordinal number n holds divisors EmptyBag $n = \langle$EmptyBag $n\rangle$.

Let n be an ordinal number and let b be a bag of n. The functor decomp b yields a finite sequence of elements of $(\mathrm{Bags}\, n)^2$ and is defined as follows:

(Def. 19) dom decomp $b =$ dom divisors b and for every natural number i and for every bag p of n such that $i \in$ dom decomp b and $p = \pi_i$ divisors b holds π_i decomp $b = \langle p, b -' p\rangle$.

One can prove the following propositions:

(72) Let n be an ordinal number, i be a natural number, and b be a bag of n. If $i \in$ dom decomp b, then there exist bag b_1, b_2 of n such that π_i decomp $b = \langle b_1, b_2\rangle$ and $b = b_1 + b_2$.

(73) Let n be an ordinal number and b, b_1, b_2 be bag of n. If $b = b_1 + b_2$, then there exists a natural number i such that $i \in$ dom decomp b and π_i decomp $b = \langle b_1, b_2\rangle$.

(74) Let n be an ordinal number, i be a natural number, and b, b_1, b_2 be bag of n. If $i \in$ dom decomp b and π_i decomp $b = \langle b_1, b_2\rangle$, then $b_1 = \pi_i$ divisors b.

Let n be an ordinal number and let b be a bag of n. Note that decomp b is non empty one-to-one and finite sequence yielding.

Let n be an ordinal number and let b be an element of Bags n. One can verify that decomp b is non empty one-to-one and finite sequence yielding.

Next we state four propositions:

(75) For every ordinal number n and for every bag b of n holds π_1 decomp $b = \langle$EmptyBag $n, b\rangle$ and $\pi_{\mathrm{len\,decomp}\,b}$ decomp $b = \langle b,$ EmptyBag $n\rangle$.

(76) Let n be an ordinal number, i be a natural number, and b, b_1, b_2 be bag of n. If $i > 1$ and $i <$ len decomp b and π_i decomp $b = \langle b_1, b_2\rangle$, then $b_1 \neq$ EmptyBag n and $b_2 \neq$ EmptyBag n.

(77) For every ordinal number n holds decomp EmptyBag $n = \langle\langle$EmptyBag n, EmptyBag $n\rangle\rangle$.

(78) Let n be an ordinal number, b be a bag of n, and f, g be finite sequences of elements of $((\mathrm{Bags}\, n)^3)^*$. Suppose that

(i) dom $f =$ dom decomp b,

(ii) dom $g =$ dom decomp b,

(iii) for every natural number k such that $k \in$ dom f holds $f(k) =$ (decomp($\pi_1\pi_k$ decomp b **qua** element of Bags n))$^\frown$(len decomp($\pi_1\pi_k$ decomp b **qua** element of Bags n) $\mapsto \langle\pi_2\pi_k$ decomp $b\rangle$), and

(iv) for every natural number k such that $k \in \operatorname{dom} g$ holds $g(k) = (\operatorname{len} \operatorname{decomp}(\pi_2\pi_k \operatorname{decomp} b$ **qua** element of $\operatorname{Bags} n) \mapsto \langle \pi_1\pi_k \operatorname{decomp} b \rangle) \frown \operatorname{decomp}(\pi_2\pi_k \operatorname{decomp} b$ **qua** element of $\operatorname{Bags} n)$.
Then there exists a permutation p of $\operatorname{dom} \operatorname{Flat}(f)$ such that $\operatorname{Flat}(g) = \operatorname{Flat}(f) \cdot p$.

6. Formal Power Series

Let X be a set and let S be a 1-sorted structure.

(Def. 20) A function from $\operatorname{Bags} X$ into S is said to be a Series of X, S.

Let n be a set, let L be a right zeroed non empty loop structure, and let p, q be Series of n, L. The functor $p + q$ yielding a Series of n, L is defined as follows:

(Def. 21) For every bag x of n holds $(p + q)(x) = p(x) + q(x)$.

One can prove the following proposition

(79) Let n be a set, L be a right zeroed non empty loop structure, and p, q be Series of n, L. Then $\operatorname{Support} p + q \subseteq \operatorname{Support} p \cup \operatorname{Support} q$.

Let n be a set, let L be an Abelian right zeroed non empty loop structure, and let p, q be Series of n, L. Let us notice that the functor $p+q$ is commutative.

Next we state the proposition

(80) Let n be a set, L be an add-associative right zeroed non empty double loop structure, and p, q, r be Series of n, L. Then $(p+q)+r = p+(q+r)$.

Let n be a set, let L be an add-associative right zeroed right complementable non empty loop structure, and let p be a Series of n, L. The functor $-p$ yields a Series of n, L and is defined by:

(Def. 22) For every bag x of n holds $(-p)(x) = -p(x)$.

Let n be a set, let L be an add-associative right zeroed right complementable non empty loop structure, and let p, q be Series of n, L. The functor $p - q$ yields a Series of n, L and is defined by:

(Def. 23) $p - q = p + -q$.

Let n be a set and let S be a non empty zero structure. The functor $0\_(n, S)$ yields a Series of n, S and is defined by:

(Def. 24) $0\_(n, S) = \operatorname{Bags} n \longmapsto 0_S$.

One can prove the following propositions:

(81) For every set n and for every non empty zero structure S and for every bag b of n holds $(0\_(n, S))(b) = 0_S$.

(82) For every set n and for every right zeroed non empty loop structure L and for every Series p of n, L holds $p + 0\_(n, L) = p$.

Let n be a set and let L be a unital non empty multiplicative loop with zero structure. The functor $1\_(n, L)$ yielding a Series of n, L is defined as follows:

(Def. 25) $1\_(n, L) = 0\_(n, L) +\cdot (\text{EmptyBag}\, n, 1_L)$.

We now state two propositions:

(83) Let n be a set, L be an add-associative right zeroed right complementable non empty loop structure, and p be a Series of n, L. Then $p - p = 0\_(n, L)$.

(84) Let n be a set and L be a unital non empty multiplicative loop with zero structure. Then $(1\_(n, L))(\text{EmptyBag}\, n) = 1_L$ and for every bag b of n such that $b \neq \text{EmptyBag}\, n$ holds $(1\_(n, L))(b) = 0_L$.

Let n be an ordinal number, let L be an add-associative right complementable right zeroed non empty double loop structure, and let p, q be Series of n, L. The functor $p * q$ yields a Series of n, L and is defined by the condition (Def. 26).

(Def. 26) Let b be a bag of n. Then there exists a finite sequence s of elements of the carrier of L such that

(i) $(p * q)(b) = \sum s$,

(ii) $\text{len}\, s = \text{len}\, \text{decomp}\, b$, and

(iii) for every natural number k such that $k \in \text{dom}\, s$ there exist bag b_1, b_2 of n such that $\pi_k \text{decomp}\, b = \langle b_1, b_2 \rangle$ and $\pi_k s = p(b_1) \cdot q(b_2)$.

One can prove the following two propositions:

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

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

Let n be an ordinal number, let L be an Abelian add-associative right zeroed right complementable commutative non empty double loop structure, and let p, q be Series of n, L. Let us note that the functor $p * q$ is commutative.

One can prove the following three propositions:

(87) Let n be an ordinal number, L be an add-associative right complementable right zeroed unital distributive non empty double loop structure, and p be a Series of n, L. Then $p * 0\_(n, L) = 0\_(n, L)$.

(88) Let n be an ordinal number, L be an add-associative right complementable right zeroed distributive unital non trivial non empty double loop structure, and p be a Series of n, L. Then $p * 1\_(n, L) = p$.

(89) Let n be an ordinal number, L be an add-associative right complementable right zeroed distributive unital non trivial non empty double loop structure, and p be a Series of n, L. Then $1\_(n, L) * p = p$.

7. Polynomials

Let n be a set and let S be a non empty zero structure. Note that there exists a Series of n, S which is finite-Support.

Let n be an ordinal number and let S be a non empty zero structure. A Polynomial of n, S is a finite-Support Series of n, S.

Let n be an ordinal number, let L be a right zeroed non empty loop structure, and let p, q be Polynomial of n, L. Observe that $p+q$ is finite-Support.

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

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

Let n be an ordinal number and let S be a non empty zero structure. Observe that $0\_(n, S)$ is finite-Support.

Let n be an ordinal number and let L be an add-associative right zeroed right complementable unital right-distributive non trivial non empty double loop structure. Observe that $1\_(n, L)$ is finite-Support.

Let n be an ordinal number, let L be an add-associative right complementable right zeroed unital distributive non empty double loop structure, and let p, q be Polynomial of n, L. One can check that $p * q$ is finite-Support.

8. The Ring of Polynomials

Let n be an ordinal number and let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure. The functor Polynom-Ring(n, L) yields a strict non empty double loop structure and is defined by the conditions (Def. 27).

(Def. 27)(i) For every set x holds $x \in$ the carrier of Polynom-Ring(n, L) iff x is a Polynomial of n, L,

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

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

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

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

Let n be an ordinal number and let L be an Abelian right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure. One can check that Polynom-Ring(n, L) is Abelian.

Let n be an ordinal number and let L be an add-associative right zeroed right complementable unital distributive non trivial non empty double loop structure. Observe that Polynom-Ring(n, L) is add-associative.

Let n be an ordinal number and let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure. Note that Polynom-Ring(n, L) is right zeroed.

Let n be an ordinal number and let L be a right complementable right zeroed add-associative unital distributive non trivial non empty double loop structure. Observe that Polynom-Ring(n, L) is right complementable.

Let n be an ordinal number and let L be an Abelian add-associative right zeroed right complementable commutative unital distributive non trivial non empty double loop structure. Note that Polynom-Ring(n, L) is commutative.

Let n be an ordinal number and let L be an Abelian add-associative right zeroed right complementable unital distributive associative non trivial non empty double loop structure. Note that Polynom-Ring(n, L) is associative.

Let n be an ordinal number and let L be a right zeroed Abelian add-associative right complementable unital distributive associative non trivial non empty double loop structure. One can check that Polynom-Ring(n, L) is unital and right-distributive.

References

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

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

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

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

[5] Grzegorz Bancerek. Monoids. *Formalized Mathematics*, 3(**2**):213–225, 1992.

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

[7] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on trees. *Formalized Mathematics*, 4(**1**):91–101, 1993.

[8] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

[9] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

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

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

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

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

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

[17] Andrzej Kondracki. The chinese remainder theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[18] Małgorzata Korolkiewicz. Homomorphisms of many sorted algebras. *Formalized Mathematics*, 5(**1**):61–65, 1996.

[19] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.
[20] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[21] Beata Madras. On the concept of the triangulation. *Formalized Mathematics*, 5(**3**):457–462, 1996.
[22] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(**3**):339–345, 1996.
[23] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[24] Wojciech Skaba and Michał Muzalewski. From double loops to fields. *Formalized Mathematics*, 2(**1**):185–191, 1991.
[25] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[26] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.
[27] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[28] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[29] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[30] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[31] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[32] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[33] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski - Zorn lemma. *Formalized Mathematics*, 1(**2**):387–393, 1990.
[34] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[35] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[36] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[37] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[38] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.

Received September 22, 1999