JOURNAL OF FORMALIZED MATHEMATICS
Volume 11, Released 1999, Published 2003
Inst. of Computer Science, Univ. 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 [9], 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`.

WWW: `http://mizar.org/JFM/Vol11/polynom1.html`

The articles [33], [17], [43], [36], [44], [45], [46], [14], [20], [37], [32], [3], [35], [16], [15], [12], [13], [19], [2], [11], [39], [38], [42], [8], [18], [4], [24], [1], [5], [41], [27], [40], [28], [7], [22], [6], [23], [31], [10], [34], [9], [30], [29], [26], [25], [21], and [47] provide the notation and terminology for this paper.

1. Basics

One can prove the following propositions:

(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 $a -' b -' c = a -' (b + c)$.

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

© Association of Mizar Users

(4) For every set X and for every binary relation R such that 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 $\operatorname{dom} p_1 = \operatorname{dom} p_2$, then $\operatorname{dom}(p_1 + p_2) = \operatorname{dom} p_1$.

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

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.

We now state the proposition

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

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 p_i is an element of D.

Let X be a set and let S be a 1-sorted structure. A function from X into S is a function from X into the carrier of S.

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

We now state two propositions:

(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 $(\operatorname{SgmX}(R,A))_1 = x$.

(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 $(\operatorname{SgmX}(R,A))_{\operatorname{len}\operatorname{SgmX}(R,A)} = x$.

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. Note that $\operatorname{SgmX}(R,A)$ is non empty and one-to-one.

One can check that $\emptyset$ is finite sequence yielding.

Let us note 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 i be a natural number and let f be a finite sequence. Note that $i \mapsto f$ is finite sequence 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 $y \in \operatorname{rng} f$ holds y is a cardinal number.

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

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

One can check 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.
The following propositions are true:

(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. One can verify that $\langle f \rangle$ is finite sequence yielding.
We now state the 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. Observe that $F \frown G$ is finite sequence yielding.
We now 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 p be a finite sequence of elements of the carrier of L, and let a be an element of L. Then $a \cdot p$ is a finite sequence of elements of the carrier of L and it can be characterized by the condition:

(Def. 2)[1] $\operatorname{dom}(a \cdot p) = \operatorname{dom} p$ and for every set i such that $i \in \operatorname{dom} p$ holds $(a \cdot p)_i = a \cdot p_i$.

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

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

Next we state several propositions:

(19) For every non empty groupoid L and for every element a of L holds $a \cdot \varepsilon_{(\text{the carrier of } L)} = \varepsilon_{(\text{the carrier of } L)}$.

(20) For every non empty groupoid L and for every element a of L holds $\varepsilon_{(\text{the carrier of } L)} \cdot a = \varepsilon_{(\text{the carrier of } L)}$.

(21) For every non empty groupoid L and for all elements a, b of 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 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 L, and p, q be finite sequences of elements of the carrier of L. Then $a \cdot (p \frown q) = (a \cdot p) \frown (a \cdot q)$.

[1] The definition (Def. 1) has been removed.

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

Let us note that every non empty multiplicative loop with zero structure which is non degenerated is also non trivial.

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

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

The following three propositions are true:

(27)[2] 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 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 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.

We now state several 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 $k \in \mathrm{dom}\,\mathrm{Flat}(F)$. Then there exist natural numbers i, j such that $i \in \mathrm{dom}\,F$ and $j \in \mathrm{dom}\,F(i)$ and $k = \sum \overline{\overline{F \restriction (i -' 1)}} + j$ and $F(i)(j) = \mathrm{Flat}(F)(k)$.

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

(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 $\sum \mathrm{Flat}(F) = \sum \sum F$.

(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 $(\mathrm{dom}\,f \longmapsto v) \circ f$ 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 $F = (\mathrm{dom}\,f \longmapsto v) \circ f$ and $v \cdot \mathrm{Flat}(f) = \mathrm{Flat}(F)$.

[2] The propositions (25) and (26) have been removed.

3. Functions Yielding Natural Numbers

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

Let us note 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. One can verify that $f +\cdot (x,n)$ is natural-yielding.

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

Let X be a set. One can verify 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 $b_1 + b_2$ yielding a many sorted set indexed by X is defined as follows:

(Def. 5)[3] For every set x holds $(b_1 + b_2)(x) = b_1(x) + b_2(x)$.

Let us observe 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 as follows:

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

One can prove the following propositions:

(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 by:

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

The following proposition is true

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

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 observe that $\emptyset$ is finite-support.

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

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

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

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

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

Let f be a finite-support function and let x, y be sets. One can verify that $f +\cdot (x, y)$ is finite-support.

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

We now state two propositions:

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

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

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 $\operatorname{Support} f$ 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) $\operatorname{Support} p$ 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. Note that every many sorted set indexed by X is finite-support.

Let X be a set and let b_1, b_2 be bags of X. One can verify that $b_1 + b_2$ is finite-support and $b_1 -' b_2$ is finite-support.

One can prove the following proposition

(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 bags of n. The predicate $p < q$ is defined by:

(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 bags 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 bags of n. The predicate $p \leq q$ is defined by:

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

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

One can prove the following four propositions:

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

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

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

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

Let X be a set and let d, b be bags of X. The predicate $d \mid b$ is defined by:

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

Let us note that the predicate $d \mid b$ is reflexive.

Next we state several propositions:

(50) For every set n and for all bags d, b of n such that for every set k such that $k \in n$ holds $d(k) \leq b(k)$ holds $d \mid b$.

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

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

(53) For every ordinal number n and for all bags d, b of n such that $d \mid b$ holds $d \leq b$.

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

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

(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 $\mathrm{Bags}\,X$.

The following proposition is true

(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 as follows:

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

We now state several propositions:

(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 bags b_1, b_2 of n such that $b_1 \mid b_2$ 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 $b \mid \mathrm{EmptyBag}\,n$ holds $\mathrm{EmptyBag}\,n = b$.

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

(64) For every ordinal number n and for every bag b of n holds $\mathrm{EmptyBag}\,n \leq b$.

Let n be an ordinal number. The functor $\mathrm{BagOrder}\,n$ yields an order in $\mathrm{Bags}\,n$ and is defined as follows:

(Def. 16) For all bags p, q of n holds $\langle p, q \rangle \in \mathrm{BagOrder}\,n$ iff $p \leq q$.

Let n be an ordinal number. Note that $\mathrm{BagOrder}\,n$ is linear-order.

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

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

The following proposition is true

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

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

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

Next we state the proposition

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

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

One can prove the following proposition

(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 $\mathbb{N}$. Note that $\mathrm{NatMinor}\,f$ is finite.

Let n be an ordinal number and let b be a bag of n. The functor $\mathrm{divisors}\,b$ yielding a finite sequence of elements of $\mathrm{Bags}\,n$ is defined as follows:

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

Let n be an ordinal number and let b be a bag of n. Note that $\mathrm{divisors}\,b$ is non empty and one-to-one.

One can prove the following propositions:

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

(69) For every ordinal number n and for every bag b of n holds $(\mathrm{divisors}\,b)_1 = \mathrm{EmptyBag}\,n$ and $(\mathrm{divisors}\,b)_{\mathrm{len}\,\mathrm{divisors}\,b} = b$.

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

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

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

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

One can prove the following three propositions:

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

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

(74) Let n be an ordinal number, i be a natural number, and b, b_1, b_2 be bags of n. If $i \in \operatorname{dom}\operatorname{decomp} b$ and $(\operatorname{decomp} b)_i = \langle b_1, b_2 \rangle$, then $b_1 = (\operatorname{divisors} b)_i$.

Let n be an ordinal number and let b be a bag of n. Observe that $\operatorname{decomp} b$ is non empty, one-to-one, and finite sequence yielding.

Let n be an ordinal number and let b be an element of $\operatorname{Bags} n$. Observe that $\operatorname{decomp} b$ 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 $(\operatorname{decomp} b)_1 = \langle \operatorname{EmptyBag} n, b \rangle$ and $(\operatorname{decomp} b)_{\operatorname{len}\operatorname{decomp} b} = \langle b, \operatorname{EmptyBag} n \rangle$.

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

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

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

(i) $\operatorname{dom} f = \operatorname{dom}\operatorname{decomp} b$,

(ii) $\operatorname{dom} g = \operatorname{dom}\operatorname{decomp} b$,

(iii) for every natural number k such that $k \in \operatorname{dom} f$ holds $f(k) = (\operatorname{decomp}(((\operatorname{decomp} b)_k)_1$ **qua** element of $\operatorname{Bags} n)) ^\frown (\operatorname{len}\operatorname{decomp}(((\operatorname{decomp} b)_k)_1$ **qua** element of $\operatorname{Bags} n) \mapsto \langle ((\operatorname{decomp} b)_k)_2 \rangle)$, and

(iv) for every natural number k such that $k \in \operatorname{dom} g$ holds $g(k) = (\operatorname{len}\operatorname{decomp}(((\operatorname{decomp} b)_k)_2$ **qua** element of $\operatorname{Bags} n) \mapsto \langle ((\operatorname{decomp} b)_k)_1 \rangle) ^\frown \operatorname{decomp}(((\operatorname{decomp} b)_k)_2$ **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. A series of X, S is a function from $\operatorname{Bags} X$ into S.

Let n be a set, let L be a 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)[4] For every bag x of n holds $(p+q)(x) = p(x) + q(x)$.

We now state the 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 observe that the functor $p + q$ is commutative.

One can prove the following 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 as follows:

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

[4] The definition (Def. 20) has been removed.

Let us observe that the functor $-p$ is involutive.

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 $p-q$ yielding a series of n, L is defined as follows:

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

Let n be a set and let S be a non empty zero structure. The functor 0_nS yields a series of n, S and is defined as follows:

(Def. 24) $0_nS=\mathrm{Bags}\,n\longmapsto 0_S$.

We now state two propositions:

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

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

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

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

The following propositions are true:

(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 $p-p=0_nL$.

(84) Let n be a set and L be a unital non empty multiplicative loop with zero structure. Then $(1\_(n,L))(\mathrm{EmptyBag}\,n)=1_L$ and for every bag b of n such that $b\neq\mathrm{EmptyBag}\,n$ 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 $p*q$ yielding a series of n, L 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) $\mathrm{len}\,s=\mathrm{len}\,\mathrm{decomp}\,b$, and

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

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 observe that the functor $p*q$ is commutative.

One can prove the following 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 polynomials of n, L. Note 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. One can verify 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 polynomials of n, L. Observe that $p - q$ is finite-Support.

Let n be an ordinal number and let S be a non empty zero structure. Note 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. One can verify 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 polynomials of n, L. Note 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 polynomials 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 polynomials 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) $\mathbf{1}_{\text{Polynom-Ring}(n,L)} = 1\_(n, L)$.

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. Note 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. Note 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. One can verify 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. One can check 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 verify that Polynom-Ring(n,L) is unital and right 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. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal1.html.

[4] Grzegorz Bancerek. The well ordering relations. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/wellord1.html.

[5] Grzegorz Bancerek. König's theorem. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/card_3.html.

[6] Grzegorz Bancerek. Monoids. *Journal of Formalized Mathematics*, 4, 1992. http://mizar.org/JFM/Vol4/monoid_0.html.

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

[8] 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.

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

[10] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Journal of Formalized Mathematics*, 8, 1996. http://mizar.org/JFM/Vol8/funct_7.html.

[11] Józef Białas. Group and field definitions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/realset1.html.

[12] Czesław Byliński. Basic functions and operations on functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_3.html.

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

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

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

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

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

[18] 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.

[19] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/funct_4.html.

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

[21] 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.

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

[23] Małgorzata Korolkiewicz. Homomorphisms of many sorted algebras. *Journal of Formalized Mathematics*, 6, 1994. http://mizar.org/JFM/Vol6/msualg_3.html.

[24] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/seqm_3.html.

[25] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/rfinseq.html.

[26] Jarosław Kotowicz and Yuji Sakai. Properties of partial functions from a domain to the set of real numbers. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/rfunct_3.html.

[27] 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.

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

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

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

[31] Andrzej Trybulec. Binary operations applied to functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funcop_1.html.

[32] Andrzej Trybulec. Semilattice operations on finite subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/setwiseo.html.

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

[34] Andrzej Trybulec. Function domains and Frænkel operator. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/fraenkel.html.

[35] Andrzej Trybulec. Many-sorted sets. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/pboole.html.

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

[37] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finsub_1.html.

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

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

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

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

[42] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski - Zorn lemma. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/orders_2.html.

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

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

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

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

[47] 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 September 22, 1999

Published January 2, 2004