JOURNAL OF FORMALIZED MATHEMATICS
Volume 15, Released 2003, Published 2003
Inst. of Computer Science, Univ. of Białystok

# Little Bezout Theorem (Factor Theorem)[1]

Piotr Rudnicki
University of Alberta, Edmonton, Canada

**Summary.** We present a formalization of the factor theorem for univariate polynomials, also called the (little) Bezout theorem: Let $r$ belong to a commutative ring $L$ and $p(x)$ be a polynomial over $L$. Then $x-r$ divides $p(x)$ iff $p(r)=0$. We also prove some consequences of this theorem like that any non zero polynomial of degree $n$ over an algebraically closed integral domain has $n$ (non necessarily distinct) roots.

MML Identifier: UPROOTS.

WWW: http://mizar.org/JFM/Vol15/uproots.html

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

## 1. Preliminaries

One can prove the following propositions:

(1) For every natural number $n$ holds $n$ is non empty iff $n=1$ or $n>1$.

(2) Let $f$ be a finite sequence of elements of $\mathbb{N}$. Suppose that for every natural number $i$ such that $i \in \operatorname{dom} f$ holds $f(i) \neq 0$. Then $\sum f = \operatorname{len} f$ if and only if $f = \operatorname{len} f \mapsto 1$.

The scheme *IndFinSeq0* deals with a finite sequence $\mathcal{A}$ and a binary predicate $\mathcal{P}$, and states that:

For every natural number $i$ such that $1 \leq i$ and $i \leq \operatorname{len} \mathcal{A}$ holds $\mathcal{P}[i, \mathcal{A}(i)]$

provided the following conditions are met:

- $\mathcal{P}[1, \mathcal{A}(1)]$, and
- For every natural number $i$ such that $1 \leq i$ and $i < \operatorname{len} \mathcal{A}$ holds if $\mathcal{P}[i, \mathcal{A}(i)]$, then $\mathcal{P}[i+1, \mathcal{A}(i+1)]$.

The following proposition is true

(3) Let $L$ be an add-associative right zeroed right complementable non empty loop structure and $r$ be a finite sequence of elements of $L$. Suppose $\operatorname{len} r \geq 2$ and for every natural number $k$ such that $2 < k$ and $k \in \operatorname{dom} r$ holds $r(k) = 0_L$. Then $\sum r = r_1 + r_2$.

## 2. Canonical Ordering of a Finite Set

Let $A$ be a finite set. The functor $\operatorname{canFS}(A)$ yields a finite sequence of elements of $A$ and is defined by the conditions (Def. 1).

[1]This work has been supported by NSERC Grant OGP9207.

(Def. 1)(i) $\operatorname{len}\operatorname{canFS}(A) = \operatorname{card}A$, and

(ii) there exists a finite sequence $f$ such that $\operatorname{len} f = \operatorname{card}A$ and $f(1) = \langle \operatorname{choose}(A), A \setminus \{\operatorname{choose}(A)\}\rangle$ or $\operatorname{card}A = 0$ and for every natural number $i$ such that $1 \leq i$ and $i < \operatorname{card}A$ and for every set $x$ such that $f(i) = x$ holds $f(i+1) = \langle \operatorname{choose}(x_{\mathbf{2}}), x_{\mathbf{2}} \setminus \{\operatorname{choose}(x_{\mathbf{2}})\}\rangle$ and for every natural number $i$ such that $i \in \operatorname{dom}\operatorname{canFS}(A)$ holds $(\operatorname{canFS}(A))(i) = f(i)_{\mathbf{1}}$.

Next we state four propositions:

(4) For every finite set $A$ holds $\operatorname{canFS}(A)$ is one-to-one.

(5) For every finite set $A$ holds $\operatorname{rng}\operatorname{canFS}(A) = A$.

(6) For every set $a$ holds $\operatorname{canFS}(\{a\}) = \langle a \rangle$.

(7) For every finite set $A$ holds $(\operatorname{canFS}(A))^{-1}$ is a function from $A$ into $\operatorname{Seg}\operatorname{card}A$.

## 3. More about Bags

Let $X$ be a set, let $S$ be a finite subset of $X$, and let $n$ be a natural number. The functor $(S,n) - \operatorname{bag}$ yielding an element of $\operatorname{Bags}X$ is defined by:

(Def. 2) $(S,n) - \operatorname{bag} = \operatorname{EmptyBag}X {+\cdot} (S \longmapsto n)$.

The following propositions are true:

(8) Let $X$ be a set, $S$ be a finite subset of $X$, $n$ be a natural number, and $i$ be a set. If $i \notin S$, then $((S,n) - \operatorname{bag})(i) = 0$.

(9) Let $X$ be a set, $S$ be a finite subset of $X$, $n$ be a natural number, and $i$ be a set. If $i \in S$, then $((S,n) - \operatorname{bag})(i) = n$.

(10) For every set $X$ and for every finite subset $S$ of $X$ and for every natural number $n$ such that $n \neq 0$ holds $\operatorname{support}(S,n) - \operatorname{bag} = S$.

(11) Let $X$ be a set, $S$ be a finite subset of $X$, and $n$ be a natural number. If $S$ is empty or $n = 0$, then $(S,n) - \operatorname{bag} = \operatorname{EmptyBag}X$.

(12) Let $X$ be a set, $S$, $T$ be finite subsets of $X$, and $n$ be a natural number. If $S$ misses $T$, then $(S \cup T, n) - \operatorname{bag} = (S,n) - \operatorname{bag} + (T,n) - \operatorname{bag}$.

Let $A$ be a set and let $b$ be a bag of $A$. The functor $\operatorname{degree}(b)$ yielding a natural number is defined as follows:

(Def. 3) There exists a finite sequence $f$ of elements of $\mathbb{N}$ such that $\operatorname{degree}(b) = \sum f$ and $f = b \cdot \operatorname{canFS}(\operatorname{support} b)$.

Next we state several propositions:

(13) For every set $A$ and for every bag $b$ of $A$ holds $b = \operatorname{EmptyBag}A$ iff $\operatorname{degree}(b) = 0$.

(14) Let $A$ be a set, $S$ be a finite subset of $A$, and $b$ be a bag of $A$. Then $S = \operatorname{support} b$ and $\operatorname{degree}(b) = \operatorname{card}S$ if and only if $b = (S,1) - \operatorname{bag}$.

(15) Let $A$ be a set, $S$ be a finite subset of $A$, and $b$ be a bag of $A$. Suppose $\operatorname{support} b \subseteq S$. Then there exists a finite sequence $f$ of elements of $\mathbb{N}$ such that $f = b \cdot \operatorname{canFS}(S)$ and $\operatorname{degree}(b) = \sum f$.

(16) For every set $A$ and for all bags $b$, $b_1$, $b_2$ of $A$ such that $b = b_1 + b_2$ holds $\operatorname{degree}(b) = \operatorname{degree}(b_1) + \operatorname{degree}(b_2)$.

(17) Let $L$ be an associative commutative unital non empty groupoid, $f$, $g$ be finite sequences of elements of $L$, and $p$ be a permutation of $\operatorname{dom} f$. If $g = f \cdot p$, then $\prod g = \prod f$.

## 4. More on Polynomials

Let $L$ be a non empty zero structure and let $p$ be a polynomial of $L$. We say that $p$ is non-zero if and only if:

(Def. 4) $p \neq \mathbf{0}.L$.

The following proposition is true

(18) For every non empty zero structure $L$ and for every polynomial $p$ of $L$ holds $p$ is non-zero iff $\mathrm{len}\, p > 0$.

Let $L$ be a non trivial non empty zero structure. One can verify that there exists a polynomial of $L$ which is non-zero.

Let $L$ be a non degenerated non empty multiplicative loop with zero structure and let $x$ be an element of $L$. Observe that $\langle {}_0 x, \mathbf{1}_L \rangle$ is non-zero.

We now state three propositions:

(19) For every non empty zero structure $L$ and for every polynomial $p$ of $L$ such that $\mathrm{len}\, p > 0$ holds $p(\mathrm{len}\, p -' 1) \neq 0_L$.

(20) Let $L$ be a non empty zero structure and $p$ be an algebraic sequence of $L$. If $\mathrm{len}\, p = 1$, then $p = \langle {}_0 p(0) \rangle$ and $p(0) \neq 0_L$.

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

One can verify that there exists a well unital non empty double loop structure which is algebraic-closed, add-associative, right zeroed, right complementable, Abelian, commutative, associative, distributive, integral domain-like, and non degenerated.

Next we state the proposition

(22) Let $L$ be an add-associative right zeroed right complementable distributive integral domain-like non empty double loop structure and $p$, $q$ be polynomials of $L$. If $p * q = \mathbf{0}.L$, then $p = \mathbf{0}.L$ or $q = \mathbf{0}.L$.

Let $L$ be an add-associative right zeroed right complementable distributive integral domain-like non empty double loop structure. Note that Polynom-Ring $L$ is integral domain-like.

Let $L$ be an integral domain and let $p$, $q$ be non-zero polynomials of $L$. Observe that $p * q$ is non-zero.

Next we state a number of propositions:

(23) For every non degenerated commutative ring $L$ and for all polynomials $p$, $q$ of $L$ holds $\mathrm{Roots}\, p \cup \mathrm{Roots}\, q \subseteq \mathrm{Roots}(p * q)$.

(24) For every integral domain $L$ and for all polynomials $p$, $q$ of $L$ holds $\mathrm{Roots}(p * q) = \mathrm{Roots}\, p \cup \mathrm{Roots}\, q$.

(25) Let $L$ be an add-associative right zeroed right complementable distributive non empty double loop structure, $p$ be a polynomial of $L$, and $p_1$ be an element of Polynom-Ring $L$. If $p = p_1$, then $-p = -p_1$.

(26) Let $L$ be an add-associative right zeroed right complementable distributive non empty double loop structure, $p$, $q$ be polynomials of $L$, and $p_1$, $q_1$ be elements of Polynom-Ring $L$. If $p = p_1$ and $q = q_1$, then $p - q = p_1 - q_1$.

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

(28) Let $L$ be an add-associative right zeroed right complementable distributive non empty double loop structure and $p$, $q$ be polynomials of $L$. If $p - q = \mathbf{0}.L$, then $p = q$.

(29) Let $L$ be an Abelian add-associative right zeroed right complementable distributive integral domain-like non empty double loop structure and $p$, $q$, $r$ be polynomials of $L$. If $p \neq \mathbf{0}.L$ and $p * q = p * r$, then $q = r$.

(30) Let $L$ be an integral domain, $n$ be a natural number, and $p$ be a polynomial of $L$. If $p \neq \mathbf{0}.L$, then $p^n \neq \mathbf{0}.L$.

(31) For every commutative ring $L$ and for all natural numbers $i$, $j$ and for every polynomial $p$ of $L$ holds $p^i * p^j = p^{i+j}$.

(32) For every non empty multiplicative loop with zero structure $L$ holds $\mathbf{1}.L = \langle_0 \mathbf{1}_L \rangle$.

(33) Let $L$ be an add-associative right zeroed right complementable right unital right distributive non empty double loop structure and $p$ be a polynomial of $L$. Then $p * \langle_0 \mathbf{1}_L \rangle = p$.

(34) Let $L$ be an add-associative right zeroed right complementable distributive non empty double loop structure and $p$, $q$ be polynomials of $L$. If $\operatorname{len} p = 0$ or $\operatorname{len} q = 0$, then $\operatorname{len}(p * q) = 0$.

(35) Let $L$ be an add-associative right zeroed right complementable distributive non empty double loop structure and $p$, $q$ be polynomials of $L$. If $p * q$ is non-zero, then $p$ is non-zero and $q$ is non-zero.

(36) Let $L$ be an add-associative right zeroed right complementable distributive commutative associative left unital non empty double loop structure and $p$, $q$ be polynomials of $L$. If $p(\operatorname{len} p -' 1) \cdot q(\operatorname{len} q -' 1) \neq 0_L$, then $0 < \operatorname{len}(p * q)$.

(37) Let $L$ be an add-associative right zeroed right complementable distributive commutative associative left unital integral domain-like non empty double loop structure and $p$, $q$ be polynomials of $L$. If $1 < \operatorname{len} p$ and $1 < \operatorname{len} q$, then $\operatorname{len} p < \operatorname{len}(p * q)$.

(38) Let $L$ be an add-associative right zeroed right complementable left distributive non empty double loop structure, $a$, $b$ be elements of $L$, and $p$ be a polynomial of $L$. Then $(\langle_0 a, b\rangle * p)(0) = a \cdot p(0)$ and for every natural number $i$ holds $(\langle_0 a, b\rangle * p)(i+1) = a \cdot p(i+1) + b \cdot p(i)$.

(39) Let $L$ be an add-associative right zeroed right complementable distributive well unital commutative associative non degenerated non empty double loop structure, $r$ be an element of $L$, and $q$ be a non-zero polynomial of $L$. Then $\operatorname{len}(\langle_0 r, \mathbf{1}_L\rangle * q) = \operatorname{len} q + 1$.

(40) Let $L$ be a non degenerated commutative ring, $x$ be an element of $L$, and $i$ be a natural number. Then $\operatorname{len}(\langle_0 x, \mathbf{1}_L\rangle^i) = i + 1$.

Let $L$ be a non degenerated commutative ring, let $x$ be an element of $L$, and let $n$ be a natural number. One can verify that $\langle_0 x, \mathbf{1}_L\rangle^n$ is non-zero.

We now state two propositions:

(41) Let $L$ be a non degenerated commutative ring, $x$ be an element of $L$, $q$ be a non-zero polynomial of $L$, and $i$ be a natural number. Then $\operatorname{len}(\langle_0 x, \mathbf{1}_L\rangle^i * q) = i + \operatorname{len} q$.

(42) Let $L$ be an add-associative right zeroed right complementable distributive well unital commutative associative non degenerated non empty double loop structure, $r$ be an element of $L$, and $p$, $q$ be polynomials of $L$. If $p = \langle_0 r, \mathbf{1}_L\rangle * q$ and $p(\operatorname{len} p -' 1) = \mathbf{1}_L$, then $q(\operatorname{len} q -' 1) = \mathbf{1}_L$.

## 5. Little Bezout Theorem

Let $L$ be a non empty zero structure, let $p$ be a polynomial of $L$, and let $n$ be a natural number. The functor $\operatorname{poly\_shift}(p, n)$ yielding a polynomial of $L$ is defined as follows:

(Def. 5) For every natural number $i$ holds $(\operatorname{poly\_shift}(p, n))(i) = p(n + i)$.

One can prove the following propositions:

(43) For every non empty zero structure $L$ and for every polynomial $p$ of $L$ holds $\mathrm{poly\_shift}(p,0) = p$.

(44) Let $L$ be a non empty zero structure, $n$ be a natural number, and $p$ be a polynomial of $L$. If $n \geq \mathrm{len}\, p$, then $\mathrm{poly\_shift}(p,n) = \mathbf{0}.L$.

(45) Let $L$ be a non degenerated non empty multiplicative loop with zero structure, $n$ be a natural number, and $p$ be a polynomial of $L$. If $n \leq \mathrm{len}\, p$, then $\mathrm{len}\,\mathrm{poly\_shift}(p,n) + n = \mathrm{len}\, p$.

(46) Let $L$ be a non degenerated commutative ring, $x$ be an element of $L$, $n$ be a natural number, and $p$ be a polynomial of $L$. If $n < \mathrm{len}\, p$, then $\mathrm{eval}(\mathrm{poly\_shift}(p,n),x) = x \cdot \mathrm{eval}(\mathrm{poly\_shift}(p,n+1),x) + p(n)$.

(47) For every non degenerated commutative ring $L$ and for every polynomial $p$ of $L$ such that $\mathrm{len}\, p = 1$ holds $\mathrm{Roots}\, p = \emptyset$.

Let $L$ be a non degenerated commutative ring, let $r$ be an element of $L$, and let $p$ be a polynomial of $L$. Let us assume that $r$ is a root of $p$. The functor $\mathrm{poly\_quotient}(p,r)$ yielding a polynomial of $L$ is defined as follows:

(Def. 6)(i) $\mathrm{len}\,\mathrm{poly\_quotient}(p,r) + 1 = \mathrm{len}\, p$ and for every natural number $i$ holds $(\mathrm{poly\_quotient}(p,r))(i) = \mathrm{eval}(\mathrm{poly\_shift}(p,i+1),r)$ if $\mathrm{len}\, p > 0$,

(ii) $\mathrm{poly\_quotient}(p,r) = \mathbf{0}.L$, otherwise.

One can prove the following propositions:

(48) Let $L$ be a non degenerated commutative ring, $r$ be an element of $L$, and $p$ be a non-zero polynomial of $L$. If $r$ is a root of $p$, then $\mathrm{len}\,\mathrm{poly\_quotient}(p,r) > 0$.

(49) Let $L$ be an add-associative right zeroed right complementable left distributive well unital non empty double loop structure and $x$ be an element of $L$. Then $\mathrm{Roots}\langle_0 -x, \mathbf{1}_L\rangle = \{x\}$.

(50) Let $L$ be a non trivial commutative ring, $x$ be an element of $L$, and $p$, $q$ be polynomials of $L$. If $p = \langle_0 -x, \mathbf{1}_L\rangle * q$, then $x$ is a root of $p$.

(51) Let $L$ be a non degenerated commutative ring, $r$ be an element of $L$, and $p$ be a polynomial of $L$. If $r$ is a root of $p$, then $p = \langle_0 -r, \mathbf{1}_L\rangle * \mathrm{poly\_quotient}(p,r)$.

(52) Let $L$ be a non degenerated commutative ring, $r$ be an element of $L$, and $p$, $q$ be polynomials of $L$. If $p = \langle_0 -r, \mathbf{1}_L\rangle * q$, then $r$ is a root of $p$.

## 6. POLYNOMIALS DEFINED BY ROOTS

Let $L$ be an integral domain and let $p$ be a non-zero polynomial of $L$. Note that $\mathrm{Roots}\, p$ is finite.

Let $L$ be a non degenerated commutative ring, let $x$ be an element of $L$, and let $p$ be a non-zero polynomial of $L$. The functor $\mathrm{multiplicity}(p,x)$ yields a natural number and is defined by the condition (Def. 7).

(Def. 7) There exists a finite non empty subset $F$ of $\mathbb{N}$ such that $F = \{k; k$ ranges over natural numbers: $\bigvee_{q:\text{polynomial of } L}\ p = \langle_0 -x, \mathbf{1}_L\rangle^k * q\}$ and $\mathrm{multiplicity}(p,x) = \max F$.

One can prove the following two propositions:

(53) Let $L$ be a non degenerated commutative ring, $p$ be a non-zero polynomial of $L$, and $x$ be an element of $L$. Then $x$ is a root of $p$ if and only if $\mathrm{multiplicity}(p,x) \geq 1$.

(54) For every non degenerated commutative ring $L$ and for every element $x$ of $L$ holds $\mathrm{multiplicity}(\langle_0 -x, \mathbf{1}_L\rangle, x) = 1$.

Let $L$ be an integral domain and let $p$ be a non-zero polynomial of $L$. The functor $\mathrm{BRoots}(p)$ yielding a bag of the carrier of $L$ is defined as follows:

(Def. 8) support BRoots$(p)$ = Roots $p$ and for every element $x$ of $L$ holds $(\mathrm{BRoots}(p))(x) = \mathrm{multiplicity}(p,x)$.

One can prove the following propositions:

(55) For every integral domain $L$ and for every element $x$ of $L$ holds $\mathrm{BRoots}(\langle_0 -x, \mathbf{1}_L\rangle) = (\{x\},1) - \mathrm{bag}$.

(56) Let $L$ be an integral domain, $x$ be an element of $L$, and $p$, $q$ be non-zero polynomials of $L$. Then $\mathrm{multiplicity}(p*q,x) = \mathrm{multiplicity}(p,x) + \mathrm{multiplicity}(q,x)$.

(57) For every integral domain $L$ and for all non-zero polynomials $p$, $q$ of $L$ holds $\mathrm{BRoots}(p*q) = \mathrm{BRoots}(p) + \mathrm{BRoots}(q)$.

(58) For every integral domain $L$ and for every non-zero polynomial $p$ of $L$ such that $\mathrm{len}\, p = 1$ holds $\mathrm{degree}(\mathrm{BRoots}(p)) = 0$.

(59) For every integral domain $L$ and for every element $x$ of $L$ and for every natural number $n$ holds $\mathrm{degree}(\mathrm{BRoots}(\langle_0 -x, \mathbf{1}_L\rangle^n)) = n$.

(60) For every algebraic-closed integral domain $L$ and for every non-zero polynomial $p$ of $L$ holds $\mathrm{degree}(\mathrm{BRoots}(p)) = \mathrm{len}\, p -' 1$.

Let $L$ be an add-associative right zeroed right complementable distributive non empty double loop structure, let $c$ be an element of $L$, and let $n$ be a natural number. The functor fpoly_mult_root$(c,n)$ yields a finite sequence of elements of Polynom-Ring $L$ and is defined by:

(Def. 9) len fpoly_mult_root$(c,n) = n$ and for every natural number $i$ such that $i \in$ dom fpoly_mult_root$(c,n)$ holds $(\mathrm{fpoly\_mult\_root}(c,n))(i) = \langle_0 -c, \mathbf{1}_L\rangle$.

Let $L$ be an add-associative right zeroed right complementable distributive non empty double loop structure and let $b$ be a bag of the carrier of $L$. The functor poly_with_roots$(b)$ yielding a polynomial of $L$ is defined by the condition (Def. 10).

(Def. 10) There exists a finite sequence $f$ of elements of (the carrier of Polynom-Ring $L)^*$ and there exists a finite sequence $s$ of elements of $L$ such that $\mathrm{len}\, f = \mathrm{card\,support}\, b$ and $s = \mathrm{canFS}(\mathrm{support}\, b)$ and for every natural number $i$ such that $i \in \mathrm{dom}\, f$ holds $f(i) = \mathrm{fpoly\_mult\_root}(s_i, b(s_i))$ and $\mathrm{poly\_with\_roots}(b) = \prod \mathrm{Flat}(f)$.

The following propositions are true:

(61) Let $L$ be an Abelian add-associative right zeroed right complementable commutative distributive right unital non empty double loop structure. Then poly_with_roots(EmptyBag (the carrier of $L$)) $= \langle_0 \mathbf{1}_L\rangle$.

(62) Let $L$ be an add-associative right zeroed right complementable distributive non empty double loop structure and $c$ be an element of $L$. Then $\mathrm{poly\_with\_roots}((\{c\},1) - \mathrm{bag}) = \langle_0 -c, \mathbf{1}_L\rangle$.

(63) Let $L$ be an add-associative right zeroed right complementable distributive non empty double loop structure, $b$ be a bag of the carrier of $L$, $f$ be a finite sequence of elements of (the carrier of Polynom-Ring $L)^*$, and $s$ be a finite sequence of elements of $L$. Suppose $\mathrm{len}\, f = \mathrm{card\,support}\, b$ and $s = \mathrm{canFS}(\mathrm{support}\, b)$ and for every natural number $i$ such that $i \in \mathrm{dom}\, f$ holds $f(i) = \mathrm{fpoly\_mult\_root}(s_i, b(s_i))$. Then $\mathrm{len\,Flat}(f) = \mathrm{degree}(b)$.

(64) Let $L$ be an add-associative right zeroed right complementable distributive non empty double loop structure, $b$ be a bag of the carrier of $L$, $f$ be a finite sequence of elements of (the carrier of Polynom-Ring $L)^*$, $s$ be a finite sequence of elements of $L$, and $c$ be an element of $L$ such that $\mathrm{len}\, f = \mathrm{card\,support}\, b$ and $s = \mathrm{canFS}(\mathrm{support}\, b)$ and for every natural number $i$ such that $i \in \mathrm{dom}\, f$ holds $f(i) = \mathrm{fpoly\_mult\_root}(s_i, b(s_i))$. Then

(i) if $c \in \mathrm{support}\, b$, then $\mathrm{card}(\mathrm{Flat}(f)^{-1}(\{\langle_0 -c, \mathbf{1}_L\rangle\})) = b(c)$, and

(ii) if $c \notin \mathrm{support}\, b$, then $\mathrm{card}(\mathrm{Flat}(f)^{-1}(\{\langle_0 -c, \mathbf{1}_L\rangle\})) = 0$.

(65) For every commutative ring $L$ and for all bags $b_1$, $b_2$ of the carrier of $L$ holds $\text{poly\_with\_roots}(b_1 + b_2) = \text{poly\_with\_roots}(b_1) * \text{poly\_with\_roots}(b_2)$.

(66) Let $L$ be an algebraic-closed integral domain and $p$ be a non-zero polynomial of $L$. If $p(\text{len}\, p -' 1) = \mathbf{1}_L$, then $p = \text{poly\_with\_roots}(\text{BRoots}(p))$.

(67) Let $L$ be a commutative ring, $s$ be a non empty finite subset of $L$, and $f$ be a finite sequence of elements of Polynom-Ring$L$. Suppose $\text{len}\, f = \overline{\overline{s}}$ and for every natural number $i$ and for every element $c$ of $L$ such that $i \in \text{dom}\, f$ and $c = (\text{canFS}(s))(i)$ holds $f(i) = \langle_0 -c, \mathbf{1}_L \rangle$. Then $\text{poly\_with\_roots}((s, 1) - \text{bag}) = \prod f$.

(68) Let $L$ be a non trivial commutative ring, $s$ be a non empty finite subset of $L$, $x$ be an element of $L$, and $f$ be a finite sequence of elements of $L$. Suppose $\text{len}\, f = \text{card}\, s$ and for every natural number $i$ and for every element $c$ of $L$ such that $i \in \text{dom}\, f$ and $c = (\text{canFS}(s))(i)$ holds $f(i) = \text{eval}(\langle_0 -c, \mathbf{1}_L \rangle, x)$. Then $\text{eval}(\text{poly\_with\_roots}((s, 1) - \text{bag}), x) = \prod f$.

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

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

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

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

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

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

[9] 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.

[10] 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.

[11] 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.

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

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

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

[15] 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.

[16] Anna Justyna Milewska. The field of complex numbers. *Journal of Formalized Mathematics*, 12, 2000. http://mizar.org/JFM/Vol12/complfld.html.

[17] Robert Milewski. The evaluation of polynomials. *Journal of Formalized Mathematics*, 12, 2000. http://mizar.org/JFM/Vol12/polynom4.html.

[18] Robert Milewski. Fundamental theorem of algebra. *Journal of Formalized Mathematics*, 12, 2000. http://mizar.org/JFM/Vol12/polynom5.html.

[19] Robert Milewski. The ring of polynomials. *Journal of Formalized Mathematics*, 12, 2000. http://mizar.org/JFM/Vol12/polynom3.html.

[20] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/vectsp_2.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] Yatsuka Nakamura, Piotr Rudnicki, Andrzej Trybulec, and Pauline N. Kawamoto. Preliminaries to circuits, I. *Journal of Formalized Mathematics*, 6, 1994. http://mizar.org/JFM/Vol6/pre_circ.html.

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

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

[25] 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.

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

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

[28] Andrzej Trybulec. Tuples, projections and Cartesian products. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/mcart_1.html.

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

[30] Andrzej Trybulec. On the sets inhabited by numbers. *Journal of Formalized Mathematics*, 15, 2003. http://mizar.org/JFM/Vol16/membered.html.

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

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

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

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

[35] Wojciech A. Trybulec. Linear combinations in real linear space. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/rlvect_2.html.

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

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

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

[39] 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 December 30, 2003*

*Published January 6, 2004*