

Little Bezout Theorem (Factor Theorem)¹

Piotr Rudnicki
University of Alberta
Edmonton

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.

The articles [28], [37], [26], [10], [2], [27], [36], [15], [20], [38], [7], [8], [3], [6], [35], [32], [24], [23], [11], [21], [16], [19], [17], [18], [1], [12], [33], [29], [22], [9], [34], [4], [25], [39], [13], [30], [14], [31], 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 $i \in \text{dom } f$ holds $f(i) \neq 0$. Then $\sum f = \text{len } f$ if and only if $f = \text{len } f \mapsto 1$.

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 $i \leq \text{len } \mathcal{A}$ holds
 $\mathcal{P}[i, \mathcal{A}(i)]$

¹This work has been supported by NSERC Grant OGP9207.

provided the parameters meet the following requirements:

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

We now state the proposition

- (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 $\text{len } r \geq 2$ and for every natural number k such that $2 < k$ and $k \in \text{dom } r$ 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 $\text{CFS}(A)$ yielding a finite sequence of elements of A is defined by the conditions (Def. 1).

- (Def. 1)(i) $\text{len } \text{CFS}(A) = \text{card } A$, and
- (ii) there exists a finite sequence f such that $\text{len } f = \text{card } A$ and $f(1) = \langle \text{choose}(A), A \setminus \{\text{choose}(A)\} \rangle$ or $\text{card } A = 0$ and for every natural number i such that $1 \leq i$ and $i < \text{card } A$ and for every set x such that $f(i) = x$ holds $f(i+1) = \langle \text{choose}(x_2), x_2 \setminus \{\text{choose}(x_2)\} \rangle$ and for every natural number i such that $i \in \text{dom } \text{CFS}(A)$ holds $(\text{CFS}(A))(i) = f(i)_1$.

The following four propositions are true:

- (4) For every finite set A holds $\text{CFS}(A)$ is one-to-one.
- (5) For every finite set A holds $\text{rng } \text{CFS}(A) = A$.
- (6) For every set a holds $\text{CFS}(\{a\}) = \langle a \rangle$.
- (7) For every finite set A holds $(\text{CFS}(A))^{-1}$ is a function from A into $\text{Seg } \text{card } A$.

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) -bag yields an element of $\text{Bags } X$ and is defined by:

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

We now state several propositions:

- (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 $((S, n)\text{-bag})(i) = 0$.
- (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 $((S, n)\text{-bag})(i) = n$.
- (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 $\text{support}((S, n)\text{-bag}) = S$.

(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) -bag = 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 $(S \cup T, n)$ -bag = (S, n) -bag + (T, n) -bag.

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

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

We now state several propositions:

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

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

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

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

(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 $\text{dom } f$. 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) $p \neq \mathbf{0}_L$.

One can prove the following proposition

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

Let L be a non trivial non empty zero structure. Note 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 . Note that $\langle x, \mathbf{1}_L \rangle$ is non-zero.

Next we state three propositions:

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

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

- (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 $p * \mathbf{0}.L = \mathbf{0}.L$.

Let us mention 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.

We now 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. Observe that Polynom-Ring L is integral domain-like.

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

We now state a number of propositions:

- (23) For every non degenerated commutative ring L and for all polynomials p, q of L holds $\text{Roots } p \cup \text{Roots } q \subseteq \text{Roots}(p * q)$.
- (24) For every integral domain L and for all polynomials p, q of L holds $\text{Roots}(p * q) = \text{Roots } p \cup \text{Roots } q$.
- (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 $\mathbf{1} \cdot L = \langle \mathbf{1}_L \rangle$.
- (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 $p * \langle \mathbf{1}_L \rangle = p$.
- (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 $\text{len } p = 0$ or $\text{len } q = 0$, then $\text{len}(p * q) = 0$.
- (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 $p(\text{len } p -' 1) \cdot q(\text{len } q -' 1) \neq 0_L$, then $0 < \text{len}(p * q)$.
- (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 $1 < \text{len } p$ and $1 < \text{len } q$, then $\text{len } p < \text{len}(p * q)$.
- (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 $(\langle a, b \rangle * p)(0) = a \cdot p(0)$ and for every natural number i holds $(\langle a, b \rangle * p)(i + 1) = a \cdot p(i + 1) + b \cdot p(i)$.
- (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 $\text{len}(\langle r, \mathbf{1}_L \rangle * q) = \text{len } q + 1$.
- (40) Let L be a non degenerated commutative ring, x be an element of L , and i be a natural number. Then $\text{len}(\langle x, \mathbf{1}_L \rangle^i) = i + 1$.

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

Next we 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 $\text{len}(\langle x, \mathbf{1}_L \rangle^i * q) = i + \text{len } q$.
- (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 $p = \langle r, \mathbf{1}_L \rangle * q$ and $p(\text{len } p -' 1) = \mathbf{1}_L$, then $q(\text{len } q -' 1) = \mathbf{1}_L$.

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 $\text{poly_shift}(p, n)$ yields a polynomial of L and is defined by:

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

We now state several propositions:

- (43) For every non empty zero structure L and for every polynomial p of L holds $\text{poly_shift}(p, 0) = p$.
- (44) Let L be a non empty zero structure, n be a natural number, and p be a polynomial of L . If $n \geq \text{len } p$, then $\text{poly_shift}(p, n) = \mathbf{0} \cdot L$.
- (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 $n \leq \text{len } p$, then $\text{len } \text{poly_shift}(p, n) + n = \text{len } p$.
- (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 $n < \text{len } p$, then $\text{eval}(\text{poly_shift}(p, n), x) = x \cdot \text{eval}(\text{poly_shift}(p, n + 1), x) + p(n)$.
- (47) For every non degenerated commutative ring L and for every polynomial p of L such that $\text{len } p = 1$ holds $\text{Roots } p = \emptyset$.

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 $\text{poly_quotient}(p, r)$ yielding a polynomial of L is defined as follows:

- (Def. 6)(i) $\text{len } \text{poly_quotient}(p, r) + 1 = \text{len } p$ and for every natural number i holds $(\text{poly_quotient}(p, r))(i) = \text{eval}(\text{poly_shift}(p, i + 1), r)$ if $\text{len } p > 0$,
- (ii) $\text{poly_quotient}(p, r) = \mathbf{0} \cdot L$, otherwise.

Next we state several 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 $\text{len } \text{poly_quotient}(p, r) > 0$.
- (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 $\text{Roots} \langle -x, \mathbf{1}_L \rangle = \{x\}$.
- (50) Let L be a non trivial commutative ring, x be an element of L , and p, q be polynomials of L . If $p = \langle -x, \mathbf{1}_L \rangle * q$, 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 $p = \langle -r, \mathbf{1}_L \rangle * \text{poly_quotient}(p, r)$.
- (52) Let L be a non degenerated commutative ring, r be an element of L , and p, q be polynomials of L . If $p = \langle -r, \mathbf{1}_L \rangle * q$, 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 . One can verify that $\text{Roots } p$ 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 $\text{multiplicity}(p, x)$ 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 $F = \{k; k \text{ ranges over natural numbers: } \bigvee_{q: \text{polynomial of } L} p = \langle -x, \mathbf{1}_L \rangle^k * q\}$ and $\text{multiplicity}(p, x) = \max F$.

Next we state 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 $\text{multiplicity}(p, x) \geq 1$.
- (54) For every non degenerated commutative ring L and for every element x of L holds $\text{multiplicity}(\langle -x, \mathbf{1}_L \rangle, x) = 1$.

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

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

Next we state several propositions:

- (55) For every integral domain L and for every element x of L holds $\text{BRoots}(\langle -x, \mathbf{1}_L \rangle) = (\{x\}, 1)$ -bag.
- (56) Let L be an integral domain, x be an element of L , and p, q be non-zero polynomials of L . Then $\text{multiplicity}(p * q, x) = \text{multiplicity}(p, x) + \text{multiplicity}(q, x)$.
- (57) For every integral domain L and for all non-zero polynomials p, q of L holds $\text{BRoots}(p * q) = \text{BRoots}(p) + \text{BRoots}(q)$.
- (58) For every integral domain L and for every non-zero polynomial p of L such that $\text{len } p = 1$ holds $\text{degree}(\text{BRoots}(p)) = 0$.
- (59) For every integral domain L and for every element x of L and for every natural number n holds $\text{degree}(\text{BRoots}(\langle -x, \mathbf{1}_L \rangle^n)) = n$.
- (60) For every algebraic-closed integral domain L and for every non-zero polynomial p of L holds $\text{degree}(\text{BRoots}(p)) = \text{len } p - 1$.

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 $\text{fpoly_mult_root}(c, n)$ yielding a finite sequence of elements of $\text{Polynom-Ring } L$ is defined as follows:

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

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 $\text{poly_with_roots}(b)$ yields a polynomial of L and is defined by the condition (Def. 10).

(Def. 10) There exists a finite sequence f of elements of (the carrier of $\text{Polynom-Ring } L$)^{*} and there exists a finite sequence s of elements of L such that $\text{len } f = \text{card support } b$ and $s = \text{CFS}(\text{support } b)$ and for every natural number i such that $i \in \text{dom } f$ holds $f(i) = \text{fpoly_mult_root}(s_i, b(s_i))$ and $\text{poly_with_roots}(b) = \prod \text{Flat}(f)$.

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 $\text{poly_with_roots}(\text{EmptyBag}(\text{the carrier of } L)) = \langle \mathbf{1}_L \rangle$.
- (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 $\text{poly_with_roots}(\langle \{c\}, 1 \rangle\text{-bag}) = \langle -c, \mathbf{1}_L \rangle$.
- (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 $\text{Polynom-Ring } L$)^{*}, and s be a finite sequence of elements of L . Suppose $\text{len } f = \text{card support } b$ and $s = \text{CFS}(\text{support } b)$ and for every natural number i such that $i \in \text{dom } f$ holds $f(i) = \text{fpoly_mult_root}(s_i, b(s_i))$. Then $\text{len Flat}(f) = \text{degree}(b)$.
- (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 $\text{Polynom-Ring } L$)^{*}, s be a finite sequence of elements of L , and c be an element of L such that $\text{len } f = \text{card support } b$ and $s = \text{CFS}(\text{support } b)$ and for every natural number i such that $i \in \text{dom } f$ holds $f(i) = \text{fpoly_mult_root}(s_i, b(s_i))$. Then
 - (i) if $c \in \text{support } b$, then $\text{card}(\text{Flat}(f)^{-1}(\langle \{-c, \mathbf{1}_L\} \rangle)) = b(c)$, and
 - (ii) if $c \notin \text{support } b$, then $\text{card}(\text{Flat}(f)^{-1}(\langle \{-c, \mathbf{1}_L\} \rangle)) = 0$.
- (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 $\text{Polynom-Ring } L$. 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 $c = (\text{CFS}(s))(i)$ holds $f(i) = \langle -c, \mathbf{1}_L \rangle$. Then $\text{poly_with_roots}(\langle s, 1 \rangle\text{-bag}) = \prod f$.
- (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 $c = (\text{CFS}(s))(i)$ holds $f(i) = \text{eval}(\langle -c, \mathbf{1}_L \rangle, x)$. Then $\text{eval}(\text{poly_with_roots}((s, 1)\text{-bag}), x) = \prod f$.

REFERENCES

- [1] Grzegorz Bancerek. Cardinal numbers. *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 and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(1):107–114, 1990.
- [4] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on trees. *Formalized Mathematics*, 4(1):91–101, 1993.
- [5] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(3):433–439, 1990.
- [6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(3):529–536, 1990.
- [7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(1):153–164, 1990.
- [9] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(3):521–527, 1990.
- [10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(1):47–53, 1990.
- [11] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(4):661–668, 1990.
- [12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(1):165–167, 1990.
- [13] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(4):573–577, 1997.
- [14] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(3):471–475, 1990.
- [15] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(2):335–342, 1990.
- [16] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(2):265–269, 2001.
- [17] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(2):391–395, 2001.
- [18] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(3):461–470, 2001.
- [19] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(2):339–346, 2001.
- [20] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(1):3–11, 1991.
- [21] Michał Muzalewski and Lesław W. Szczęcha. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(1):97–104, 1991.
- [22] Yatsuka Nakamura, Piotr Rudnicki, Andrzej Trybulec, and Pauline N. Kawamoto. Preliminaries to circuits, I. *Formalized Mathematics*, 5(2):167–172, 1996.
- [23] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(1):83–86, 1993.
- [24] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(1):111–115, 1991.
- [25] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(1):95–110, 2001.
- [26] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
- [27] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(2):369–376, 1990.
- [28] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(1):9–11, 1990.

- [29] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(1):97–105, 1990.
- [30] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(1):15–22, 1993.
- [31] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(4):341–347, 2003.
- [32] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(5):979–981, 1990.
- [33] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(5):821–827, 1990.
- [34] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(3):581–588, 1990.
- [35] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(3):575–579, 1990.
- [36] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(2):291–296, 1990.
- [37] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(1):67–71, 1990.
- [38] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(1):73–83, 1990.
- [39] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(2):205–211, 1992.

Received December 30, 2003
