FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

# Primitive Roots of Unity and Cyclotomic Polynomials[1]

Broderick Arneson
University of Alberta
Edmonton

Piotr Rudnicki
University of Alberta
Edmonton

**Summary.** We present a formalization of roots of unity, define cyclotomic polynomials and demonstrate the relationship between cyclotomic polynomials and unital polynomials.

MML Identifier: `UNIROOTS`.

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

## 1. Preliminaries

One can prove the following proposition

(1) For every natural number $n$ holds $n = 0$ or $n = 1$ or $n \geqslant 2$.

The scheme *Comp Ind NE* concerns a unary predicate $\mathcal{P}$, and states that:

For every non empty natural number $k$ holds $\mathcal{P}[k]$

provided the parameters satisfy the following condition:

- For every non empty natural number $k$ such that for every non empty natural number $n$ such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$.

Next we state the proposition

(2) For every finite sequence $f$ such that $1 \leqslant \operatorname{len} f$ holds $f \restriction \operatorname{Seg} 1 = \langle f(1) \rangle$.

The following propositions are true:

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




ISSN 1426–2630

(3) Let $f$ be a finite sequence of elements of $\mathbb{C}_{\rm F}$ and $g$ be a finite sequence of elements of $\mathbb{R}$. Suppose $\operatorname{len} f = \operatorname{len} g$ and for every natural number $i$ such that $i \in \operatorname{dom} f$ holds $|f_i| = g(i)$. Then $|\prod f| = \prod g$.

(4) Let $s$ be a non empty finite subset of $\mathbb{C}_{\rm F}$, $x$ be an element of $\mathbb{C}_{\rm F}$, and $r$ be a finite sequence of elements of $\mathbb{R}$. Suppose $\operatorname{len} r = \operatorname{card} s$ and for every natural number $i$ and for every element $c$ of $\mathbb{C}_{\rm F}$ such that $i \in \operatorname{dom} r$ and $c = (\mathrm{CFS}(s))(i)$ holds $r(i) = |x - c|$. Then $|\operatorname{eval}(\text{poly\_with\_roots}((s,1)\text{-bag}), x)| = \prod r$.

(5) Let $f$ be a finite sequence of elements of $\mathbb{C}_{\rm F}$. Suppose that for every natural number $i$ such that $i \in \operatorname{dom} f$ holds $f(i)$ is integer. Then $\sum f$ is integer.

(6) For every real number $r$ there exists an element $z$ of $\mathbb{C}$ such that $z = r$ and $z = r + 0i$.

(7) For all elements $x$, $y$ of $\mathbb{C}_{\rm F}$ and for all real numbers $r_1$, $r_2$ such that $r_1 = x$ and $r_2 = y$ holds $r_1 \cdot r_2 = x \cdot y$ and $r_1 + r_2 = x + y$.

(8) Let $q$ be a real number. Suppose $q$ is an integer and $q > 0$. Let $r$ be an element of $\mathbb{C}_{\rm F}$. If $|r| = 1$ and $r \neq 1 + 0i_{\mathbb{C}_{\rm F}}$, then $|(q + 0i_{\mathbb{C}_{\rm F}}) - r| > q - 1$.

(9) Let $p_1$ be a non empty finite sequence of elements of $\mathbb{R}$ and $x$ be a real number. Suppose $x \geqslant 1$ and for every natural number $i$ such that $i \in \operatorname{dom} p_1$ holds $p_1(i) > x$. Then $\prod p_1 > x$.

(10) For every natural number $n$ holds $\mathbf{1}_{\mathbb{C}_{\rm F}} = \operatorname{power}_{\mathbb{C}_{\rm F}}(\mathbf{1}_{\mathbb{C}_{\rm F}}, n)$.

(11) Let $n$ be a non empty natural number and $i$ be a natural number. Then $\cos(\frac{2\cdot\pi\cdot i}{n}) = \cos(\frac{2\cdot\pi\cdot(i \bmod n)}{n})$ and $\sin(\frac{2\cdot\pi\cdot i}{n}) = \sin(\frac{2\cdot\pi\cdot(i \bmod n)}{n})$.

(12) For every non empty natural number $n$ and for every natural number $i$ holds $\cos(\frac{2\cdot\pi\cdot i}{n}) + \sin(\frac{2\cdot\pi\cdot i}{n})i_{\mathbb{C}_{\rm F}} = \cos(\frac{2\cdot\pi\cdot(i \bmod n)}{n}) + \sin(\frac{2\cdot\pi\cdot(i \bmod n)}{n})i_{\mathbb{C}_{\rm F}}$.

(13) Let $n$ be a non empty natural number and $i$, $j$ be natural numbers. Then $(\cos(\frac{2\cdot\pi\cdot i}{n}) + \sin(\frac{2\cdot\pi\cdot i}{n})i_{\mathbb{C}_{\rm F}}) \cdot (\cos(\frac{2\cdot\pi\cdot j}{n}) + \sin(\frac{2\cdot\pi\cdot j}{n})i_{\mathbb{C}_{\rm F}}) = \cos(\frac{2\cdot\pi\cdot((i+j) \bmod n)}{n}) + \sin(\frac{2\cdot\pi\cdot((i+j) \bmod n)}{n})i_{\mathbb{C}_{\rm F}}$.

(14) Let $L$ be a unital associative non empty groupoid, $x$ be an element of $L$, and $n$, $m$ be natural numbers. Then $\operatorname{power}_L(x, n\cdot m) = \operatorname{power}_L(\operatorname{power}_L(x, n), m)$.

(15) For every natural number $n$ and for every element $x$ of $\mathbb{C}_{\rm F}$ such that $x$ is an integer holds $\operatorname{power}_{\mathbb{C}_{\rm F}}(x, n)$ is an integer.

(16) Let $F$ be a finite sequence of elements of $\mathbb{C}_{\rm F}$. Suppose that for every natural number $i$ such that $i \in \operatorname{dom} F$ holds $F(i)$ is an integer. Then $\sum F$ is an integer.

(17) For every real number $a$ such that $0 \leqslant a$ and $a < 2 \cdot \pi$ and $\cos a = 1$ holds $a = 0$.

Let us note that there exists a field which is finite and there exists a skew field which is finite.

## 2. Multiplicative Group of a Skew Field

Let $R$ be a skew field. The functor MultGroup($R$) yields a strict group and is defined by the conditions (Def. 1).

(Def. 1)(i) The carrier of MultGroup($R$) = (the carrier of $R$) $\setminus \{0_R\}$, and

(ii) the multiplication of MultGroup($R$) = (the multiplication of $R$)$\upharpoonright$[: the carrier of MultGroup($R$), the carrier of MultGroup($R$) :].

Next we state three propositions:

(18) For every skew field $R$ holds the carrier of $R$ = (the carrier of MultGroup($R$)) $\cup \{0_R\}$.

(19) Let $R$ be a skew field, $a$, $b$ be elements of $R$, and $c$, $d$ be elements of MultGroup($R$). If $a = c$ and $b = d$, then $c \cdot d = a \cdot b$.

(20) For every skew field $R$ holds $\mathbf{1}_R = 1_{\mathrm{MultGroup}(R)}$.

Let $R$ be a finite skew field. Observe that MultGroup($R$) is finite.

We now state three propositions:

(21) For every finite skew field $R$ holds ord(MultGroup($R$)) = card (the carrier of $R$) $- 1$.

(22) For every skew field $R$ and for every set $s$ such that $s \in$ the carrier of MultGroup($R$) holds $s \in$ the carrier of $R$.

(23) For every skew field $R$ holds the carrier of MultGroup($R$) $\subseteq$ the carrier of $R$.

## 3. Roots of Unity

Let $n$ be a non empty natural number. The functor $n$-roots_of_1 yielding a subset of $\mathbb{C}_{\mathrm{F}}$ is defined by:

(Def. 2) $n$-roots_of_1 = $\{x; x$ ranges over elements of $\mathbb{C}_{\mathrm{F}}$: $x$ is a complex root of $n$, $\mathbf{1}_{\mathbb{C}_{\mathrm{F}}}\}$.

We now state several propositions:

(24) Let $n$ be a non empty natural number and $x$ be an element of $\mathbb{C}_{\mathrm{F}}$. Then $x \in n$-roots_of_1 if and only if $x$ is a complex root of $n$, $\mathbf{1}_{\mathbb{C}_{\mathrm{F}}}$.

(25) For every non empty natural number $n$ holds $\mathbf{1}_{\mathbb{C}_{\mathrm{F}}} \in n$-roots_of_1 .

(26) For every non empty natural number $n$ and for every element $x$ of $\mathbb{C}_{\mathrm{F}}$ such that $x \in n$-roots_of_1 holds $|x| = 1$.

(27) Let $n$ be a non empty natural number and $x$ be an element of $\mathbb{C}_{\mathrm{F}}$. Then $x \in n$-roots_of_1 if and only if there exists a natural number $k$ such that $x = \cos(\frac{2 \cdot \pi \cdot k}{n}) + \sin(\frac{2 \cdot \pi \cdot k}{n}) i_{\mathbb{C}_{\mathrm{F}}}$.

(28) For every non empty natural number $n$ and for all elements $x$, $y$ of $\mathbb{C}$ such that $x \in n$-roots_of_1 and $y \in n$-roots_of_1 holds $x \cdot y \in n$-roots_of_1 .

(29) For every non empty natural number $n$ holds $n$-roots_of_1 $=$ $\{\cos(\frac{2 \cdot \pi \cdot k}{n}) + \sin(\frac{2 \cdot \pi \cdot k}{n}) i_{\mathbb{C}_{\rm F}}; k$ ranges over natural numbers: $k < n\}$.

(30) For every non empty natural number $n$ holds $\overline{\overline{n\text{-roots\_of\_1}}} = n$.

Let $n$ be a non empty natural number. One can check that $n$-roots_of_1 is non empty and $n$-roots_of_1 is finite.

Next we state several propositions:

(31) For all non empty natural numbers $n$, $n_1$ such that $n_1 \mid n$ holds $n_1$-roots_of_1 $\subseteq n$-roots_of_1 .

(32) Let $R$ be a skew field, $x$ be an element of MultGroup($R$), and $y$ be an element of $R$. If $y = x$, then for every natural number $k$ holds $\text{power}_{\text{MultGroup}(R)}(x, k) = \text{power}_R(y, k)$.

(33) For every non empty natural number $n$ and for every element $x$ of MultGroup($\mathbb{C}_{\rm F}$) such that $x \in n$-roots_of_1 holds $x$ is not of order 0.

(34) Let $n$ be a non empty natural number, $k$ be a natural number, and $x$ be an element of MultGroup($\mathbb{C}_{\rm F}$). If $x = \cos(\frac{2 \cdot \pi \cdot k}{n}) + \sin(\frac{2 \cdot \pi \cdot k}{n}) i_{\mathbb{C}_{\rm F}}$, then $\text{ord}(x) = n \div (k \gcd n)$.

(35) For every non empty natural number $n$ holds $n$-roots_of_1 $\subseteq$ the carrier of MultGroup($\mathbb{C}_{\rm F}$).

(36) For every non empty natural number $n$ there exists an element $x$ of MultGroup($\mathbb{C}_{\rm F}$) such that $\text{ord}(x) = n$.

(37) For every non empty natural number $n$ and for every element $x$ of MultGroup($\mathbb{C}_{\rm F}$) holds $\text{ord}(x) \mid n$ iff $x \in n$-roots_of_1 .

(38) For every non empty natural number $n$ holds $n$-roots_of_1 $= \{x; x$ ranges over elements of MultGroup($\mathbb{C}_{\rm F}$): $\text{ord}(x) \mid n\}$.

(39) Let $n$ be a non empty natural number and $x$ be a set. Then $x \in$ $n$-roots_of_1 if and only if there exists an element $y$ of MultGroup($\mathbb{C}_{\rm F}$) such that $x = y$ and $\text{ord}(y) \mid n$.

Let $n$ be a non empty natural number. The functor $n$-th_roots_of_1 yielding a strict group is defined as follows:

(Def. 3) The carrier of $n$-th_roots_of_1 $=$ $n$-roots_of_1 and the multiplication of $n$-th_roots_of_1 $=$ (the multiplication of $\mathbb{C}_{\rm F}$)$\restriction$[: $n$-roots_of_1, $n$-roots_of_1 :].

One can prove the following proposition

(40) For every non empty natural number $n$ holds $n$-th_roots_of_1 is a subgroup of MultGroup($\mathbb{C}_{\rm F}$).

## 4. The Unital Polynomial $x^n - 1$

Let $n$ be a non empty natural number and let $L$ be a left unital non empty double loop structure. The functor unital_poly$(L, n)$ yields a polynomial of $L$ and is defined as follows:

(Def. 4) unital_poly$(L, n) = \mathbf{0}.\, L +\cdot (0, -\mathbf{1}_L) +\cdot (n, \mathbf{1}_L)$.

Next we state four propositions:

(41) unital_poly$(\mathbb{C}_{\rm F}, 1) = \langle -\mathbf{1}_{\mathbb{C}_{\rm F}}, \mathbf{1}_{\mathbb{C}_{\rm F}} \rangle$.

(42) Let $L$ be a left unital non empty double loop structure and $n$ be a non empty natural number. Then (unital_poly$(L, n))(0) = -\mathbf{1}_L$ and (unital_poly$(L, n))(n) = \mathbf{1}_L$.

(43) Let $L$ be a left unital non empty double loop structure, $n$ be a non empty natural number, and $i$ be a natural number. If $i \neq 0$ and $i \neq n$, then (unital_poly$(L, n))(i) = 0_L$.

(44) Let $L$ be a non degenerated left unital non empty double loop structure and $n$ be a non empty natural number. Then len unital_poly$(L, n) = n+1$.

Let $L$ be a non degenerated left unital non empty double loop structure and let $n$ be a non empty natural number. Observe that unital_poly$(L, n)$ is non-zero.

The following propositions are true:

(45) For every non empty natural number $n$ and for every element $x$ of $\mathbb{C}_{\rm F}$ holds eval(unital_poly$(\mathbb{C}_{\rm F}, n), x) = \text{power}_{\mathbb{C}_{\rm F}}(x, n) - 1$.

(46) For every non empty natural number $n$ holds Roots unital_poly$(\mathbb{C}_{\rm F}, n) =$ $n$-roots_of_1 .

(47) Let $n$ be a natural number and $z$ be an element of $\mathbb{C}_{\rm F}$. Suppose $z$ is a real number. Then there exists a real number $x$ such that $x = z$ and $\text{power}_{\mathbb{C}_{\rm F}}(z, n) = x^n$.

(48) Let $n$ be a non empty natural number and $x$ be a real number. Then there exists an element $y$ of $\mathbb{C}_{\rm F}$ such that $y = x$ and eval(unital_poly$(\mathbb{C}_{\rm F}, n), y) =$ $x^n - 1$.

(49) For every non empty natural number $n$ holds BRoots(unital_poly$(\mathbb{C}_{\rm F}, n)) =$ ($n$-roots_of_1, 1)-bag .

(50) For every non empty natural number $n$ holds unital_poly$(\mathbb{C}_{\rm F}, n) =$ poly_with_roots(($n$-roots_of_1, 1)-bag).

Let $i$ be an integer and let $n$ be a natural number. Then $i^n$ is an integer.

The following proposition is true

(51) For every non empty natural number $n$ and for every element $i$ of $\mathbb{C}_{\rm F}$ such that $i$ is an integer holds eval(unital_poly$(\mathbb{C}_{\rm F}, n), i)$ is an integer.

## 5. Cyclotomic Polynomials

Let $d$ be a non empty natural number. The functor cyclotomic_poly($d$) yields a polynomial of $\mathbb{C}_{\rm F}$ and is defined by:

(Def. 5) There exists a non empty finite subset $s$ of $\mathbb{C}_{\rm F}$ such that $s = \{y; y$ ranges over elements of MultGroup($\mathbb{C}_{\rm F}$): ord($y$) $= d\}$ and cyclotomic_poly($d$) $=$ poly_with_roots($(s, 1)$-bag).

The following propositions are true:

(52) cyclotomic_poly(1) $= \langle -\mathbf{1}_{\mathbb{C}_{\rm F}}, \mathbf{1}_{\mathbb{C}_{\rm F}} \rangle$.

(53) Let $n$ be a non empty natural number and $f$ be a finite sequence of elements of the carrier of Polynom-Ring($\mathbb{C}_{\rm F}$). Suppose len $f = n$ and for every non empty natural number $i$ such that $i \in \operatorname{dom} f$ holds if $i \nmid n$, then $f(i) = \langle \mathbf{1}_{\mathbb{C}_{\rm F}} \rangle$ and if $i \mid n$, then $f(i) =$ cyclotomic_poly($i$). Then unital_poly($\mathbb{C}_{\rm F}, n$) $= \prod f$.

(54) Let $n$ be a non empty natural number. Then there exists a finite sequence $f$ of elements of the carrier of Polynom-Ring($\mathbb{C}_{\rm F}$) and there exists a polynomial $p$ of $\mathbb{C}_{\rm F}$ such that

(i) $p = \prod f$,

(ii) $\operatorname{dom} f = \operatorname{Seg} n$,

(iii) for every non empty natural number $i$ such that $i \in \operatorname{Seg} n$ holds if $i \nmid n$ or $i = n$, then $f(i) = \langle \mathbf{1}_{\mathbb{C}_{\rm F}} \rangle$ and if $i \mid n$ and $i \neq n$, then $f(i) =$ cyclotomic_poly($i$), and

(iv) unital_poly($\mathbb{C}_{\rm F}, n$) $=$ cyclotomic_poly($n$) $* p$.

(55) For every non empty natural number $d$ and for every natural number $i$ holds (cyclotomic_poly($d$))(0) $= 1$ or (cyclotomic_poly($d$))(0) $= -1$ but (cyclotomic_poly($d$))($i$) is integer.

(56) For every non empty natural number $d$ and for every element $z$ of $\mathbb{C}_{\rm F}$ such that $z$ is an integer holds eval(cyclotomic_poly($d$), $z$) is an integer.

(57) Let $n$, $n_1$ be non empty natural numbers, $f$ be a finite sequence of elements of the carrier of Polynom-Ring($\mathbb{C}_{\rm F}$), and $s$ be a finite subset of $\mathbb{C}_{\rm F}$. Suppose that

(i) $s = \{y; y$ ranges over elements of MultGroup($\mathbb{C}_{\rm F}$): ord($y$) $\mid n \wedge$ ord($y$) $\nmid n_1 \wedge$ ord($y$) $\neq n\}$,

(ii) $\operatorname{dom} f = \operatorname{Seg} n$, and

(iii) for every non empty natural number $i$ such that $i \in \operatorname{dom} f$ holds if $i \nmid n$ or $i \mid n_1$ or $i = n$, then $f(i) = \langle \mathbf{1}_{\mathbb{C}_{\rm F}} \rangle$ and if $i \mid n$ and $i \nmid n_1$ and $i \neq n$, then $f(i) =$ cyclotomic_poly($i$).

Then $\prod f =$ poly_with_roots($(s, 1)$-bag).

(58) Let $n$, $n_1$ be non empty natural numbers. Suppose $n_1 < n$ and $n_1 \mid n$. Then there exists a finite sequence $f$ of elements of the carrier of Polynom-Ring($\mathbb{C}_{\rm F}$) and there exists a polynomial $p$ of $\mathbb{C}_{\rm F}$ such that

(i) $p = \prod f$,

(ii) $\operatorname{dom} f = \operatorname{Seg} n$,

(iii) for every non empty natural number $i$ such that $i \in \operatorname{Seg} n$ holds if $i \nmid n$ or $i \mid n_1$ or $i = n$, then $f(i) = \langle \mathbf{1}_{\mathbb{C}_\mathrm{F}} \rangle$ and if $i \mid n$ and $i \nmid n_1$ and $i \neq n$, then $f(i) = \text{cyclotomic\_poly}(i)$, and

(iv) $\text{unital\_poly}(\mathbb{C}_\mathrm{F}, n) = \text{unital\_poly}(\mathbb{C}_\mathrm{F}, n_1) * \text{cyclotomic\_poly}(n) * p$.

(59) Let $i$ be an integer, $c$ be an element of $\mathbb{C}_\mathrm{F}$, $f$ be a finite sequence of elements of the carrier of Polynom-Ring($\mathbb{C}_\mathrm{F}$), and $p$ be a polynomial of $\mathbb{C}_\mathrm{F}$. Suppose $p = \prod f$ and $c = i$ and for every non empty natural number $i$ such that $i \in \operatorname{dom} f$ holds $f(i) = \langle \mathbf{1}_{\mathbb{C}_\mathrm{F}} \rangle$ or $f(i) = \text{cyclotomic\_poly}(i)$. Then $\text{eval}(p, c)$ is integer.

(60) Let $n$ be a non empty natural number, $j$, $k$, $q$ be integers, and $q_1$ be an element of $\mathbb{C}_\mathrm{F}$. If $q_1 = q$ and $j = \text{eval}(\text{cyclotomic\_poly}(n), q_1)$ and $k = \text{eval}(\text{unital\_poly}(\mathbb{C}_\mathrm{F}, n), q_1)$, then $j \mid k$.

(61) Let $n$, $n_1$ be non empty natural numbers and $q$ be an integer. Suppose $n_1 < n$ and $n_1 \mid n$. Let $q_1$ be an element of $c_1$. Suppose $q_1 = q$. Let $j$, $k$, $l$ be integers. If $j = \text{eval}(\text{cyclotomic\_poly}(n), q_1)$ and $k = \text{eval}(\text{unital\_poly}(\mathbb{C}_\mathrm{F}, n), q_1)$ and $l = \text{eval}(\text{unital\_poly}(\mathbb{C}_\mathrm{F}, n_1), q_1)$, then $j \mid k \div l$, where $c_1 =$ the carrier of $\mathbb{C}_\mathrm{F}$.

(62) Let $n$, $q$ be non empty natural numbers and $q_1$ be an element of $\mathbb{C}_\mathrm{F}$. If $q_1 = q$, then for every integer $j$ such that $j = \text{eval}(\text{cyclotomic\_poly}(n), q_1)$ holds $j \mid q^n - 1$.

(63) Let $n$, $n_1$, $q$ be non empty natural numbers. Suppose $n_1 < n$ and $n_1 \mid n$. Let $q_1$ be an element of $\mathbb{C}_\mathrm{F}$. If $q_1 = q$, then for every integer $j$ such that $j = \text{eval}(\text{cyclotomic\_poly}(n), q_1)$ holds $j \mid (q^n - 1) \div (q^{n_1} - 1)$.

(64) Let $n$ be a non empty natural number. Suppose $1 < n$. Let $q$ be a natural number. Suppose $1 < q$. Let $q_1$ be an element of $\mathbb{C}_\mathrm{F}$. If $q_1 = q$, then for every integer $i$ such that $i = \text{eval}(\text{cyclotomic\_poly}(n), q_1)$ holds $|i| > q - 1$.

## 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. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

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

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

[6] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

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

[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[10] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[11] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[12] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[13] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[14] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[15] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**):841–845, 1990.
[16] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[17] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[18] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**):265–269, 2001.
[19] Anna Justyna Milewska. The Hahn Banach theorem in the vector space over the field of complex numbers. *Formalized Mathematics*, 9(**2**):363–371, 2001.
[20] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.
[21] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.
[22] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.
[23] Robert Milewski. Trigonometric form of complex numbers. *Formalized Mathematics*, 9(**3**):455–460, 2001.
[24] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[25] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.
[26] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.
[27] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[28] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.
[29] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2004.
[30] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[31] Andrzej Trybulec. Introduction to arithmetics. *To appear in Formalized Mathematics.*
[32] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*
[33] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[34] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[35] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[36] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.
[37] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[38] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(**3**):581–588, 1990.
[39] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[40] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.
[41] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[42] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[43] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[44] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

[45] 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*