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

Primitive Roots of Unity and Cyclotomic Polynomials[1]

Broderic Arneson
University of Alberta, Edmonton, Canada

Piotr Rudnicki
University of Alberta, Edmonton, Canada

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.

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

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

1. PRELIMINARIES

The following proposition is true

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

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 following condition is satisfied:

- 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 $\mathcal{P}[k]$.

We now state the proposition

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

One can prove the following propositions:

(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 $c = (\operatorname{canFS}(s))(i)$ holds $r(i) = |x - c|$. Then $|\operatorname{eval}(\text{poly\_with\_roots}((s, 1) - \text{bag}), x)| = \prod r$.

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

(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 $x \geq 1$ 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 $0 \leq a$ 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)$\restriction$[:the carrier of MultGroup(R), the carrier of MultGroup(R):].

One can prove the following 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. Note that MultGroup(R) is finite.

Next we 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 $n-\text{roots\_of\_1}$ yields a subset of $\mathbb{C}_{\rm F}$ and is defined by:

(Def. 2) $n-\text{roots\_of\_1} = \{x; x$ ranges over elements of $\mathbb{C}_{\rm F}$: x is a complex root of n, $\mathbf{1}_{\mathbb{C}_{\rm F}}\}$.

Next we state several propositions:

(24) Let n be a non empty natural number and x be an element of $\mathbb{C}_{\rm F}$. Then $x \in n-\text{roots\_of\_1}$ if and only if x is a complex root of n, $\mathbf{1}_{\mathbb{C}_{\rm F}}$.

(25) For every non empty natural number n holds $\mathbf{1}_{\mathbb{C}_{\rm F}} \in n-\text{roots\_of\_1}$.

(26) For every non empty natural number n and for every element x of $\mathbb{C}_{\rm F}$ such that $x \in n-\text{roots\_of\_1}$ holds $|x| = 1$.

(27) Let n be a non empty natural number and x be an element of $\mathbb{C}_{\rm F}$. Then $x \in n-\text{roots\_of\_1}$ if and only if there exists a natural number k such that $x = \cos(\frac{2\cdot\pi\cdot k}{n}) + \sin(\frac{2\cdot\pi\cdot k}{n}) i_{\mathbb{C}_{\rm F}}$.

(28) For every non empty natural number n and for all elements x, y of $\mathbb{C}$ such that $x \in n-\text{roots\_of\_1}$ and $y \in n-\text{roots\_of\_1}$ holds $x \cdot y \in n-\text{roots\_of\_1}$.

(29) For every non empty natural number n holds $n-\text{roots\_of\_1} = \{\cos(\frac{2\cdot\pi\cdot k}{n}) + \sin(\frac{2\cdot\pi\cdot k}{n}) i_{\mathbb{C}_{\rm F}}; k$ 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. Observe that $n-\text{roots\_of\_1}$ is non empty and $n-\text{roots\_of\_1}$ is finite.

One can prove the following propositions:

(31) For all non empty natural numbers n, n_1 such that $n_1 \mid n$ holds $n_1-\text{roots\_of\_1} \subseteq n-\text{roots\_of\_1}$.

(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 $x \in n-\text{roots\_of\_1}$ 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 $n-\text{roots\_of\_1} \subseteq$ 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 $x \in n-\text{roots\_of\_1}$.

(38) For every non empty natural number n holds $n-\text{roots\_of\_1} = \{x; x$ 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 $x \in n-\text{roots\_of\_1}$ 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 $n-\text{th\_roots\_of\_1}$ yields a strict group and is defined by:

(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 $\mathbb{C}_{\mathrm{F}}$) $\restriction [: n-$ roots_of_1, $n-$ roots_of_1 $:]$.

The following proposition is true

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

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) yielding a polynomial of L is defined as follows:

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

We now state four propositions:

(41) unital_poly$(\mathbb{C}_{\mathrm{F}}, 1) = \langle_0 - \mathbf{1}_{\mathbb{C}_{\mathrm{F}}}, \mathbf{1}_{\mathbb{C}_{\mathrm{F}}} \rangle$.

(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.

We now state several propositions:

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

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

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

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

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

(50) For every non empty natural number n holds unital_poly$(\mathbb{C}_{\mathrm{F}},n) =$ 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.

Next we state the proposition

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

(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$)$.

Next we state a number of propositions:

(52) cyclotomic_poly$(1) = \langle_0 -\mathbf{1}_{\mathbb{C}_{\rm F}}, \mathbf{1}_{\mathbb{C}_{\rm F}}\rangle$.

(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 $i \in$ dom f holds if $i \nmid n$, then $f(i) = \langle_0 \mathbf{1}_{\mathbb{C}_{\rm F}}\rangle$ 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) dom f = Seg n,

(iii) for every non empty natural number i such that $i \in$ Seg n holds if $i \nmid n$ or $i = n$, then $f(i) = \langle_0 \mathbf{1}_{\mathbb{C}_{\rm F}}\rangle$ 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) dom f = Seg n, and

(iii) for every non empty natural number i such that $i \in$ dom f holds if $i \nmid n$ or $i \mid n_1$ or $i = n$, then $f(i) = \langle_0 \mathbf{1}_{\mathbb{C}_{\rm F}}\rangle$ 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) dom f = Seg n,

(iii) for every non empty natural number i such that $i \in$ Seg n holds if $i \nmid n$ or $i \mid n_1$ or $i = n$, then $f(i) = \langle_0 \mathbf{1}_{\mathbb{C}_{\rm F}}\rangle$ and if $i \mid n$ and $i \nmid n_1$ and $i \neq n$, then $f(i)$ = cyclotomic_poly(i), and

(iv) unital_poly$(\mathbb{C}_{\rm F}, n)$ = unital_poly$(\mathbb{C}_{\rm F}, n_1) *$ cyclotomic_poly$(n) * p$.

(59) Let i be an integer, c be an element of $\mathbb{C}_{\rm F}$, f be a finite sequence of elements of the carrier of Polynom-Ring($\mathbb{C}_{\rm F}$), and p be a polynomial of $\mathbb{C}_{\rm F}$. Suppose $p = \prod f$ and $c = i$ and for every non empty natural number i such that $i \in$ dom f holds $f(i) = \langle_0 \mathbf{1}_{\mathbb{C}_{\rm F}}\rangle$ or $f(i)$ = cyclotomic_poly(i). Then 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 $\mathbb{C}_{\rm F}$. If $q_1 = q$ and j = eval(cyclotomic_poly$(n), q_1)$ and k = eval(unital_poly$(\mathbb{C}_{\rm F}, n), q_1)$, 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 $j = \mathrm{eval}(\mathrm{cyclotomic\_poly}(n), q_1)$ and $k = \mathrm{eval}(\mathrm{unital\_poly}(\mathbb{C}_\mathrm{F}, n), q_1)$ and $l = \mathrm{eval}(\mathrm{unital\_poly}(\mathbb{C}_\mathrm{F}, n_1), q_1)$, 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 $j = \mathrm{eval}(\mathrm{cyclotomic\_poly}(n), q_1)$ 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 $j = \mathrm{eval}(\mathrm{cyclotomic\_poly}(n), q_1)$ 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 $i = \mathrm{eval}(\mathrm{cyclotomic\_poly}(n), q_1)$ holds $|i| > q - 1$.

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

[5] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/binop_1.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. Partial functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/partfun1.html.

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

[10] Czesław Byliński. The complex numbers. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/complex1.html.

[11] 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.

[12] 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.

[13] Library Committee. Introduction to arithmetic. *Journal of Formalized Mathematics*, Addenda, 2003. http://mizar.org/JFM/Addenda/arytm_0.html.

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

[15] Krzysztof Hryniewiecki. Basic properties of real numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/real_1.html.

[16] Andrzej Kondracki. Basic properties of rational numbers. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/rat_1.html.

[17] 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.

[18] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/int_2.html.

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

[20] Anna Justyna Milewska. The Hahn Banach theorem in the vector space over the field of complex numbers. *Journal of Formalized Mathematics*, 12, 2000. http://mizar.org/JFM/Vol12/hahnban1.html.

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

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

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

[24] Robert Milewski. Trigonometric form of complex numbers. *Journal of Formalized Mathematics*, 12, 2000. `http://mizar.org/JFM/Vol12/comptrig.html`.

[25] 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`.

[26] 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`.

[27] Jan Popiołek. Some properties of functions modul and signum. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/absvalue.html`.

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

[29] Konrad Raczkowski. Integer and rational exponents. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/prepower.html`.

[30] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Journal of Formalized Mathematics*, 15, 2003. `http://mizar.org/JFM/Vol15/uproots.html`.

[31] 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`.

[32] Andrzej Trybulec. Enumerated sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/enumset1.html`.

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

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

[35] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/int_1.html`.

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

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

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

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

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

[41] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/group_2.html`.

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

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

[44] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Journal of Formalized Mathematics*, 10, 1998. `http://mizar.org/JFM/Vol10/sin_cos.html`.

[45] 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