Contents

Formaliz. Math. 24 (**4**)

FORMALIZED MATHEMATICS
Vol. 24, No. 4, Pages 239–251, 2016
DOI: 10.1515/forma-2016-0020

DE GRUYTER OPEN
degruyter.com/view/j/forma

Homography in $\mathbb{RP}^2$

Roland Coghetto
Rue de la Brasserie 5
7100 La Louvière, Belgium

Summary. The real projective plane has been formalized in Isabelle/HOL by Timothy Makarios [13] and in Coq by Nicolas Magaud, Julien Narboux and Pascal Schreck [12].

Some definitions on the real projective spaces were introduced early in the Mizar Mathematical Library by Wojciech Leonczuk [9], Krzysztof Prazmowski [10] and by Wojciech Skaba [18].

In this article, we check with the Mizar system [4], some properties on the determinants and the Grassmann-Plücker relation in rank 3 [2], [1], [7], [16], [17].

Then we show that the projective space induced (in the sense defined in [9]) by $\mathbb{R}^3$ is a projective plane (in the sense defined in [10]).

Finally, in the real projective plane, we define the homography induced by a 3-by-3 invertible matrix and we show that the images of 3 collinear points are themselves collinear.

MSC: 51N15 03B35

Keywords: projectivity; projective transformation; projective collineation; real projective plane; Grassmann-Plücker relation

MML identifier: ANPROJ_8, version: 8.1.05 5.39.1282

1. Preliminaries

From now on a, b, c, d, e, f denote real numbers, k, m denote natural numbers, D denotes a non empty set, V denotes a non trivial real linear space, u, v, w denote elements of V, and p, q, r denote elements of the projective space over V.

Now we state the propositions:

(1) $\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle, \langle 3, 2\rangle, \langle 3, 3\rangle \in \mathrm{Seg}\, 3 \times \mathrm{Seg}\, 3$.

ISSN 1426–2630(Print), 1898-9934(Online)

(2) $\langle 1, 1\rangle$, $\langle 2, 1\rangle$, $\langle 3, 1\rangle \in \operatorname{Seg} 3 \times \operatorname{Seg} 1$.

(3) $\langle 1, 1\rangle$, $\langle 1, 2\rangle$, $\langle 1, 3\rangle \in \operatorname{Seg} 1 \times \operatorname{Seg} 3$.

(4) $\langle\langle a\rangle, \langle b\rangle, \langle c\rangle\rangle$ is a matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3×1.

(5) Let us consider a matrix N over $\mathbb{R}_{\mathrm{F}}$ of dimension 3×1. Suppose $N = \langle\langle a\rangle, \langle b\rangle, \langle c\rangle\rangle$. Then $N_{\square,1} = \langle a, b, c\rangle$. The theorem is a consequence of (2).

(6) Let us consider a non empty multiplicative magma K, and elements a_1, a_2, a_3, b_1, b_2, b_3 of K. Then $\langle a_1, a_2, a_3\rangle \bullet \langle b_1, b_2, b_3\rangle = \langle a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3\rangle$.

(7) Let us consider a commutative, associative, left unital, Abelian, add-associative, right zeroed, right complementable, non empty double loop structure K, and elements a_1, a_2, a_3, b_1, b_2, b_3 of K. Then $\langle a_1, a_2, a_3\rangle \cdot \langle b_1, b_2, b_3\rangle = a_1 \cdot b_1 + a_2 \cdot b_2 + a_3 \cdot b_3$. The theorem is a consequence of (6).

(8) Let us consider a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension 3, and a matrix N over $\mathbb{R}_{\mathrm{F}}$ of dimension 3×1. Suppose $N = \langle\langle 0\rangle, \langle 0\rangle, \langle 0\rangle\rangle$. Then $M \cdot N = \langle\langle 0\rangle, \langle 0\rangle, \langle 0\rangle\rangle$. The theorem is a consequence of (7), (5), and (2).

(9) u, v and w are lineary dependent if and only if $u = v$ or $u = w$ or $v = w$ or $\{u, v, w\}$ is linearly dependent.

(10) p, q and r are collinear if and only if there exists u and there exists v and there exists w such that $p =$ the direction of u and $q =$ the direction of v and $r =$ the direction of w and u is not zero and v is not zero and w is not zero and ($u = v$ or $u = w$ or $v = w$ or $\{u, v, w\}$ is linearly dependent). The theorem is a consequence of (9).

(11) p, q and r are collinear if and only if there exists u and there exists v and there exists w such that $p =$ the direction of u and $q =$ the direction of v and $r =$ the direction of w and u is not zero and v is not zero and w is not zero and there exists a and there exists b and there exists c such that $a \cdot u + b \cdot v + c \cdot w = 0_V$ and ($a \neq 0$ or $b \neq 0$ or $c \neq 0$).

(12) Let us consider elements u, v, w of V. Suppose $a \neq 0$ and $a\cdot u+b\cdot v+c\cdot w = 0_V$. Then $u = (\frac{-b}{a}) \cdot v + (\frac{-c}{a}) \cdot w$.

(13) If $a \neq 0$ and $a \cdot b + c \cdot d + e \cdot f = 0$, then $b = -(\frac{c}{a}) \cdot d - (\frac{e}{a}) \cdot f$.

(14) Let us consider points u, v, w of $\mathcal{E}^3_{\mathrm{T}}$. Suppose there exists a and there exists b and there exists c such that $a \cdot u + b \cdot v + c \cdot w = 0_{\mathcal{E}^3_{\mathrm{T}}}$ and $a \neq 0$. Then $\langle |u, v, w|\rangle = 0$. The theorem is a consequence of (12).

(15) Let us consider a natural number n. Then $\operatorname{dom} 1_{\mathbb{R}} \operatorname{matrix}(n) = \operatorname{Seg} n$.

(16) Let us consider a matrix A over $\mathbb{R}_{\mathrm{F}}$. Then $(\mathbb{R} \to \mathbb{R}_{\mathrm{F}})(\mathbb{R}_{\mathrm{F}} \to \mathbb{R})A = A$.

(17) Let us consider matrices A, B over $\mathbb{R}_{\mathrm{F}}$, and matrices R_1, R_2 over $\mathbb{R}$. If $A = R_1$ and $B = R_2$, then $A \cdot B = R_1 \cdot R_2$. The theorem is a consequence of (16).

(18) Let us consider a natural number n, a square matrix M over $\mathbb{R}$ of dimension n, and a square matrix N over $\mathbb{R}_{\mathrm{F}}$ of dimension n. If $M = N$, then M is invertible iff N is invertible. The theorem is a consequence of (17).

From now on o, p, q, r, s, t denote points of $\mathcal{E}^3_{\mathrm{T}}$ and M denotes a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3.

Let us consider real numbers p_1, p_2, p_3, q_1, q_2, q_3, r_1, r_2, r_3. Now we state the propositions:

(19) $\langle\langle p_1, p_2, p_3\rangle, \langle q_1, q_2, q_3\rangle, \langle r_1, r_2, r_3\rangle\rangle$ is a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3.

(20) Suppose $M = \langle\langle p_1, q_1, r_1\rangle, \langle p_2, q_2, r_2\rangle, \langle p_3, q_3, r_3\rangle\rangle$. Then

(i) $M_{1,1} = p_1$, and

(ii) $M_{1,2} = q_1$, and

(iii) $M_{1,3} = r_1$, and

(iv) $M_{2,1} = p_2$, and

(v) $M_{2,2} = q_2$, and

(vi) $M_{2,3} = r_2$, and

(vii) $M_{3,1} = p_3$, and

(viii) $M_{3,2} = q_3$, and

(ix) $M_{3,3} = r_3$.

The theorem is a consequence of (1).

(21) Suppose $M = \langle p, q, r\rangle$. Then

(i) $M_{1,1} = (p)_{\mathbf{1}}$, and

(ii) $M_{1,2} = (p)_{\mathbf{2}}$, and

(iii) $M_{1,3} = (p)_{\mathbf{3}}$, and

(iv) $M_{2,1} = (q)_{\mathbf{1}}$, and

(v) $M_{2,2} = (q)_{\mathbf{2}}$, and

(vi) $M_{2,3} = (q)_{\mathbf{3}}$, and

(vii) $M_{3,1} = (r)_{\mathbf{1}}$, and

(viii) $M_{3,2} = (r)_{\mathbf{2}}$, and

(ix) $M_{3,3} = (r)_{\mathbf{3}}$.

The theorem is a consequence of (1).

(22) Let us consider real numbers p_1, p_2, p_3, q_1, q_2, q_3, r_1, r_2, r_3. Suppose $M = \langle\langle p_1, q_1, r_1\rangle, \langle p_2, q_2, r_2\rangle, \langle p_3, q_3, r_3\rangle\rangle$. Then $M^{\mathrm{T}} = \langle\langle p_1, p_2, p_3\rangle, \langle q_1, q_2, q_3\rangle, \langle r_1, r_2, r_3\rangle\rangle$. The theorem is a consequence of (1) and (20).

(23) Suppose $M = \langle p, q, r \rangle$. Then $M^{\mathrm{T}} = \langle \langle (p)_{\mathbf{1}}, (q)_{\mathbf{1}}, (r)_{\mathbf{1}} \rangle, \langle (p)_{\mathbf{2}}, (q)_{\mathbf{2}}, (r)_{\mathbf{2}} \rangle, \langle (p)_{\mathbf{3}}, (q)_{\mathbf{3}}, (r)_{\mathbf{3}} \rangle \rangle$. The theorem is a consequence of (1) and (21).

(24) $\mathrm{lines}(M) = \{\mathrm{Line}(M, 1), \mathrm{Line}(M, 2), \mathrm{Line}(M, 3)\}$.
Proof: $\mathrm{lines}(M) \subseteq \{\mathrm{Line}(M, 1), \mathrm{Line}(M, 2), \mathrm{Line}(M, 3)\}$ by [14, (103)], [19, (1)]. $\{\mathrm{Line}(M, 1), \mathrm{Line}(M, 2), \mathrm{Line}(M, 3)\} \subseteq \mathrm{lines}(M)$ by [3, (1)], [14, (103)]. □

(25) Suppose $M = \langle \langle (p)_{\mathbf{1}}, (p)_{\mathbf{2}}, (p)_{\mathbf{3}} \rangle, \langle (q)_{\mathbf{1}}, (q)_{\mathbf{2}}, (q)_{\mathbf{3}} \rangle, \langle (r)_{\mathbf{1}}, (r)_{\mathbf{2}}, (r)_{\mathbf{3}} \rangle \rangle$. Then

- (i) $\mathrm{Line}(M, 1) = p$, and
- (ii) $\mathrm{Line}(M, 2) = q$, and
- (iii) $\mathrm{Line}(M, 3) = r$.

(26) Let us consider an object x. Then $x \in \mathrm{lines}(M^{\mathrm{T}})$ if and only if there exists a natural number i such that $i \in \mathrm{Seg}\, 3$ and $x = M_{\square, i}$.

2. Grassmann-Plücker Relation

Now we state the propositions:

(27) $\langle |p, q, r| \rangle = (p)_{\mathbf{1}} \cdot (q)_{\mathbf{2}} \cdot (r)_{\mathbf{3}} - (p)_{\mathbf{3}} \cdot (q)_{\mathbf{2}} \cdot (r)_{\mathbf{1}} - (p)_{\mathbf{1}} \cdot (q)_{\mathbf{3}} \cdot (r)_{\mathbf{2}} + (p)_{\mathbf{2}} \cdot (q)_{\mathbf{3}} \cdot (r)_{\mathbf{1}} - (p)_{\mathbf{2}} \cdot (q)_{\mathbf{1}} \cdot (r)_{\mathbf{3}} + (p)_{\mathbf{3}} \cdot (q)_{\mathbf{1}} \cdot (r)_{\mathbf{2}}$.

(28) Grassmannn-Plücker-Relation in rank 3:
$\langle |p, q, r| \rangle \cdot \langle |p, s, t| \rangle - \langle |p, q, s| \rangle \cdot \langle |p, r, t| \rangle + \langle |p, q, t| \rangle \cdot \langle |p, r, s| \rangle = 0$. The theorem is a consequence of (27).

(29) $\langle |p, q, r| \rangle = -\langle |p, r, q| \rangle$. The theorem is a consequence of (27).

(30) $\langle |p, q, r| \rangle = -\langle |q, p, r| \rangle$. The theorem is a consequence of (27).

(31) $\langle |a \cdot p, q, r| \rangle = a \cdot \langle |p, q, r| \rangle$. The theorem is a consequence of (27).

(32) $\langle |p, a \cdot q, r| \rangle = a \cdot \langle |p, q, r| \rangle$. The theorem is a consequence of (30) and (31).

(33) $\langle |p, q, a \cdot r| \rangle = a \cdot \langle |p, q, r| \rangle$. The theorem is a consequence of (29) and (32).

(34) Suppose $M = \langle \langle (p)_{\mathbf{1}}, (q)_{\mathbf{1}}, (r)_{\mathbf{1}} \rangle, \langle (p)_{\mathbf{2}}, (q)_{\mathbf{2}}, (r)_{\mathbf{2}} \rangle, \langle (p)_{\mathbf{3}}, (q)_{\mathbf{3}}, (r)_{\mathbf{3}} \rangle \rangle$. Then $\langle |p, q, r| \rangle = \mathrm{Det}\, M$. The theorem is a consequence of (22).

(35) Suppose $M = \langle \langle (p)_{\mathbf{1}}, (p)_{\mathbf{2}}, (p)_{\mathbf{3}} \rangle, \langle (q)_{\mathbf{1}}, (q)_{\mathbf{2}}, (q)_{\mathbf{3}} \rangle, \langle (r)_{\mathbf{1}}, (r)_{\mathbf{2}}, (r)_{\mathbf{3}} \rangle \rangle$. Then $\langle |p, q, r| \rangle = \mathrm{Det}\, M$.

Let us consider a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension k. Now we state the propositions:

(36) $\mathrm{Det}\, M = 0_{\mathbb{R}_{\mathrm{F}}}$ if and only if $\mathrm{rk}(M) < k$.

(37) $\mathrm{rk}(M) < k$ if and only if lines(M) is linearly dependent or M is not without repeated line.

(38) Let us consider a matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $k \times m$. Then Mx2Tran (M) is a function from RLSp2RVSp$(\mathcal{E}^k_{\mathrm{T}})$ into RLSp2RVSp$(\mathcal{E}^m_{\mathrm{T}})$.

(39) Let us consider a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension k. Then Mx2Tran(M) is a linear transformation from RLSp2RVSp$(\mathcal{E}^k_{\mathrm{T}})$ to RLSp2RVSp$(\mathcal{E}^k_{\mathrm{T}})$.
PROOF: Reconsider $M_1 = \mathrm{Mx2Tran}(M)$ as a function from RLSp2RVSp$(\mathcal{E}^k_{\mathrm{T}})$ into RLSp2RVSp$(\mathcal{E}^k_{\mathrm{T}})$. For every elements x, y of RLSp2RVSp$(\mathcal{E}^k_{\mathrm{T}})$, $M_1(x+y) = M_1(x) + M_1(y)$ by [15, (22)]. For every scalar a of $\mathbb{R}_{\mathrm{F}}$ and for every vector x of RLSp2RVSp$(\mathcal{E}^k_{\mathrm{T}})$, $M_1(a \cdot x) = a \cdot M_1(x)$ by [15, (23)]. □

(40) Suppose $M = \langle\langle(p)_{\mathbf{1}}, (p)_{\mathbf{2}}, (p)_{\mathbf{3}}\rangle, \langle(q)_{\mathbf{1}}, (q)_{\mathbf{2}}, (q)_{\mathbf{3}}\rangle, \langle(r)_{\mathbf{1}}, (r)_{\mathbf{2}}, (r)_{\mathbf{3}}\rangle\rangle$ and $\mathrm{rk}(M) < 3$. Then there exists a and there exists b and there exists c such that $a \cdot p + b \cdot q + c \cdot r = 0_{\mathcal{E}^3_{\mathrm{T}}}$ and ($a \neq 0$ or $b \neq 0$ or $c \neq 0$). The theorem is a consequence of (37), (25), (24), (39), and (7).

(41) If $a \cdot p + b \cdot q + c \cdot r = 0_{\mathcal{E}^3_{\mathrm{T}}}$ and ($a \neq 0$ or $b \neq 0$ or $c \neq 0$), then $\langle|p, q, r|\rangle = 0$. The theorem is a consequence of (14) and (30).

(42) Suppose $\langle|p, q, r|\rangle = 0$. Then there exists a and there exists b and there exists c such that $a \cdot p + b \cdot q + c \cdot r = 0_{\mathcal{E}^3_{\mathrm{T}}}$ and ($a \neq 0$ or $b \neq 0$ or $c \neq 0$). The theorem is a consequence of (19), (35), (36), and (40).

(43) p, q and r are lineary dependent if and only if $\langle|p, q, r|\rangle = 0$. The theorem is a consequence of (41) and (42).

3. SOME PROPERTIES ABOUT THE CROSS PRODUCT

Now we state the propositions:

(44) $|(p, p \times q)| = 0$.

(45) $|(p, q \times p)| = 0$.

(46) (i) $\langle|o, p, (o \times p) \times (q \times r)|\rangle = 0$, and

(ii) $\langle|q, r, (o \times p) \times (q \times r)|\rangle = 0$.

The theorem is a consequence of (44) and (45).

(47) (i) o, p and $(o \times p) \times (q \times r)$ are lineary dependent, and

(ii) q, r and $(o \times p) \times (q \times r)$ are lineary dependent.

The theorem is a consequence of (46) and (43).

(48) (i) $0_{\mathcal{E}^3_{\mathrm{T}}} \times p = 0_{\mathcal{E}^3_{\mathrm{T}}}$, and

(ii) $p \times 0_{\mathcal{E}^3_{\mathrm{T}}} = 0_{\mathcal{E}^3_{\mathrm{T}}}$.

(49) $\langle|p, q, 0_{\mathcal{E}^3_{\mathrm{T}}}|\rangle = 0$. The theorem is a consequence of (48).

(50) If $p \times q = 0_{\mathcal{E}^3_{\mathrm{T}}}$ and $r = [1, 1, 1]$, then p, q and r are lineary dependent.

PROOF: Reconsider $r = [1, 1, 1]$ as an element of $\mathcal{E}^3_{\mathrm{T}}$. $\langle|p, q, r|\rangle = 0$ by [8, (2)], (27). □

(51) If p is not zero and q is not zero and $p \times q = 0_{\mathcal{E}^3_{\mathrm{T}}}$, then p and q are proportional.

(52) Let us consider non zero points p, q, r, s of $\mathcal{E}^3_{\mathrm{T}}$. Suppose $(p \times q) \times (r \times s)$ is zero. Then

(i) p and q are proportional, or

(ii) r and s are proportional, or

(iii) $p \times q$ and $r \times s$ are proportional.

The theorem is a consequence of (51).

(53) $\langle|p, q, p \times q|\rangle = |(q, q)| \cdot |(p, p)| - |(q, p)| \cdot |(p, q)|$.

(54) $|(p \times q, p \times q)| = |(q, q)| \cdot |(p, p)| - |(q, p)| \cdot |(p, q)|$.

(55) If p is not zero and $|(p, q)| = 0$ and $|(p, r)| = 0$ and $|(p, s)| = 0$, then $\langle|q, r, s|\rangle = 0$. The theorem is a consequence of (13) and (27).

(56) $\langle|p, q, p \times q|\rangle = |p \times q|^{\mathbf{2}}$. The theorem is a consequence of (53) and (54).

(57) The projective space over $\mathcal{E}^3_{\mathrm{T}}$ is a projective plane defined in terms of collinearity.

PROOF: Set $P =$ the projective space over $\mathcal{E}^3_{\mathrm{T}}$. There exist elements u, v, w_1 of $\mathcal{E}^3_{\mathrm{T}}$ such that for every real numbers a, b, c such that $a \cdot u + b \cdot v + c \cdot w_1 = 0_{\mathcal{E}^3_{\mathrm{T}}}$ holds $a = 0$ and $b = 0$ and $c = 0$ by [6, (22)], [8, (4)], [11, (39)], [8, (2)]. For every elements p, p_1, q, q_1 of P, there exists an element r of P such that p, p_1 and r are collinear and q, q_1 and r are collinear by [9, (26)], (52), [9, (22)], [18, (2)]. □

4. Real Projective Plane and Homography

Let us consider elements u, v, w, x of $\mathcal{E}^3_{\mathrm{T}}$. Now we state the propositions:

(58) Suppose u is not zero and x is not zero and the direction of $u =$ the direction of x. Then $\langle|u, v, w|\rangle = 0$ if and only if $\langle|x, v, w|\rangle = 0$. The theorem is a consequence of (31).

(59) Suppose v is not zero and x is not zero and the direction of $v =$ the direction of x. Then $\langle|u, v, w|\rangle = 0$ if and only if $\langle|u, x, w|\rangle = 0$. The theorem is a consequence of (32).

(60) Suppose w is not zero and x is not zero and the direction of $w =$ the direction of x. Then $\langle|u, v, w|\rangle = 0$ if and only if $\langle|u, v, x|\rangle = 0$. The theorem is a consequence of (33).

(61) (i) $(1_{\mathbb{R}}\,\mathrm{matrix}(3))(1) = e_1$, and

(ii) $(1_{\mathbb{R}}\,\mathrm{matrix}(3))(2) = e_2$, and

(iii) $(1_{\mathbb{R}}\,\mathrm{matrix}(3))(3) = e_3$.

(62) (i) the base finite sequence of 3 and $1 = e_1$, and

(ii) the base finite sequence of 3 and $2 = e_2$, and

(iii) the base finite sequence of 3 and $3 = e_3$.

(63) Let us consider a finite sequence p_2 of elements of D. Suppose $\mathrm{len}\, p_2 = 3$. Then

(i) $\langle p_2\rangle_{\square,1} = \langle p_2(1)\rangle$, and

(ii) $\langle p_2\rangle_{\square,2} = \langle p_2(2)\rangle$, and

(iii) $\langle p_2\rangle_{\square,3} = \langle p_2(3)\rangle$.

The theorem is a consequence of (3).

(64) (i) $\langle e_1\rangle_{\square,1} = \langle 1\rangle$, and

(ii) $\langle e_1\rangle_{\square,2} = \langle 0\rangle$, and

(iii) $\langle e_1\rangle_{\square,3} = \langle 0\rangle$.

The theorem is a consequence of (63).

(65) (i) $\langle e_2\rangle_{\square,1} = \langle 0\rangle$, and

(ii) $\langle e_2\rangle_{\square,2} = \langle 1\rangle$, and

(iii) $\langle e_2\rangle_{\square,3} = \langle 0\rangle$.

The theorem is a consequence of (63).

(66) (i) $\langle e_3\rangle_{\square,1} = \langle 0\rangle$, and

(ii) $\langle e_3\rangle_{\square,2} = \langle 0\rangle$, and

(iii) $\langle e_3\rangle_{\square,3} = \langle 1\rangle$.

The theorem is a consequence of (63).

(67) (i) $(I^{3\times 3}_{\mathbb{R}_{\mathrm{F}}})_{\square,1} = \langle 1, 0, 0\rangle$, and

(ii) $(I^{3\times 3}_{\mathbb{R}_{\mathrm{F}}})_{\square,2} = \langle 0, 1, 0\rangle$, and

(iii) $(I^{3\times 3}_{\mathbb{R}_{\mathrm{F}}})_{\square,3} = \langle 0, 0, 1\rangle$.

The theorem is a consequence of (1) and (15).

(68) (i) $\mathrm{Line}(I^{3\times 3}_{\mathbb{R}_{\mathrm{F}}}, 1) = \langle 1, 0, 0\rangle$, and

(ii) $\mathrm{Line}(I^{3\times 3}_{\mathbb{R}_{\mathrm{F}}}, 2) = \langle 0, 1, 0\rangle$, and

(iii) $\mathrm{Line}(I^{3\times 3}_{\mathbb{R}_{\mathrm{F}}}, 3) = \langle 0, 0, 1\rangle$.

The theorem is a consequence of (1).

(69) (i) $\langle e_1\rangle^{\mathrm{T}} = \langle\langle 1\rangle, \langle 0\rangle, \langle 0\rangle\rangle$, and

(ii) $\langle e_2\rangle^{\mathrm{T}} = \langle\langle 0\rangle, \langle 1\rangle, \langle 0\rangle\rangle$, and

(iii) $\langle e_3\rangle^{\mathrm{T}} = \langle\langle 0\rangle, \langle 0\rangle, \langle 1\rangle\rangle$.

The theorem is a consequence of (64), (65), and (66).

From now on p_1 denotes a finite sequence of elements of D.

Now we state the propositions:

(70) Let us consider a finite sequence p_1 of elements of D. If $k \in \mathrm{dom}\, p_1$, then $\langle p_1\rangle_{1,k} = p_1(k)$.

(71) If $k \in \mathrm{dom}\, p_1$, then $\langle p_1\rangle_{\square,k} = \langle p_1(k)\rangle$. The theorem is a consequence of (70).

(72) Let us consider an element p_2 of $\mathcal{R}^3$. Suppose $p_1 = p_2$. Then $(\mathbb{R} \to \mathbb{R}_{\mathrm{F}})\,\mathrm{ColVec2Mx}(p_2) = \langle p_1\rangle^{\mathrm{T}}$. The theorem is a consequence of (71).

In the sequel P denotes a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3.

Now we state the propositions:

(73) Suppose $P = \langle\langle (p)_{\mathbf{1}}, (p)_{\mathbf{2}}, (p)_{\mathbf{3}}\rangle, \langle (q)_{\mathbf{1}}, (q)_{\mathbf{2}}, (q)_{\mathbf{3}}\rangle, \langle (r)_{\mathbf{1}}, (r)_{\mathbf{2}}, (r)_{\mathbf{3}}\rangle\rangle$. Then

(i) $\mathrm{Line}(P, 1) = p$, and

(ii) $\mathrm{Line}(P, 2) = q$, and

(iii) $\mathrm{Line}(P, 3) = r$.

(74) Suppose $P = \langle\langle (p)_{\mathbf{1}}, (p)_{\mathbf{2}}, (p)_{\mathbf{3}}\rangle, \langle (q)_{\mathbf{1}}, (q)_{\mathbf{2}}, (q)_{\mathbf{3}}\rangle, \langle (r)_{\mathbf{1}}, (r)_{\mathbf{2}}, (r)_{\mathbf{3}}\rangle\rangle$. Then

(i) $P_{\square,1} = \langle (p)_{\mathbf{1}}, (q)_{\mathbf{1}}, (r)_{\mathbf{1}}\rangle$, and

(ii) $P_{\square,2} = \langle (p)_{\mathbf{2}}, (q)_{\mathbf{2}}, (r)_{\mathbf{2}}\rangle$, and

(iii) $P_{\square,3} = \langle (p)_{\mathbf{3}}, (q)_{\mathbf{3}}, (r)_{\mathbf{3}}\rangle$.

(75) $\mathrm{width}\langle p_1\rangle = \mathrm{len}\, p_1$.

(76) Suppose $\mathrm{len}\, p_1 = 3$. Then

(i) $\mathrm{Line}(\langle p_1\rangle^{\mathrm{T}}, 1) = \langle p_1(1)\rangle$, and

(ii) $\mathrm{Line}(\langle p_1\rangle^{\mathrm{T}}, 2) = \langle p_1(2)\rangle$, and

(iii) $\mathrm{Line}(\langle p_1\rangle^{\mathrm{T}}, 3) = \langle p_1(3)\rangle$.

The theorem is a consequence of (75) and (63).

(77) If $\mathrm{len}\, p_1 = 3$, then $\langle p_1\rangle^{\mathrm{T}} = \langle\langle p_1(1)\rangle, \langle p_1(2)\rangle, \langle p_1(3)\rangle\rangle$. The theorem is a consequence of (76).

Let us consider D. Let p be a finite sequence of elements of D. Assume $\mathrm{len}\, p = 3$. The functor $\mathrm{F2M}(p)$ yielding a finite sequence of elements of D^1 is defined by the term

(Def. 1) $\langle\langle p(1)\rangle, \langle p(2)\rangle, \langle p(3)\rangle\rangle$.

Let us consider a finite sequence p of elements of $\mathbb{R}$. Now we state the propositions:

(78) If $\operatorname{len} p = 3$, then $\operatorname{len} \mathrm{F2M}(p) = 3$.

(79) If $\operatorname{len} p = 3$, then p is a 3-element finite sequence of elements of $\mathbb{R}$.

(80) If $p = [0, 0, 0]$, then $\mathrm{F2M}(p) = \langle\langle 0\rangle, \langle 0\rangle, \langle 0\rangle\rangle$.

(81) Suppose $\operatorname{len} p_1 = 3$. Then $\langle\langle p_1\rangle_{\square,1}, \langle p_1\rangle_{\square,2}, \langle p_1\rangle_{\square,3}\rangle = \mathrm{F2M}(p_1)$. The theorem is a consequence of (63).

Let us consider D. Let p be a finite sequence of elements of D^1. Assume $\operatorname{len} p = 3$. The functor $\mathrm{M2F}(p)$ yielding a finite sequence of elements of D is defined by the term

(Def. 2) $\langle p(1)(1), p(2)(1), p(3)(1)\rangle$.

Now we state the proposition:

(82) Let us consider a finite sequence p of elements of $\mathbb{R}^1$. Suppose $\operatorname{len} p = 3$. Then $\mathrm{M2F}(p)$ is a point of $\mathcal{E}^3_{\mathrm{T}}$.

Let p be a finite sequence of elements of $\mathbb{R}^1$ and a be a real number. Assume $\operatorname{len} p = 3$. The functor $a \cdot p$ yielding a finite sequence of elements of $\mathbb{R}^1$ is defined by

(Def. 3) there exist real numbers p_1, p_2, p_3 such that $p_1 = p(1)(1)$ and $p_2 = p(2)(1)$ and $p_3 = p(3)(1)$ and $it = \langle\langle a \cdot p_1\rangle, \langle a \cdot p_2\rangle, \langle a \cdot p_3\rangle\rangle$.

Let us consider a finite sequence p of elements of $\mathbb{R}^1$. Now we state the propositions:

(83) If $\operatorname{len} p = 3$, then $\mathrm{M2F}(a \cdot p) = a \cdot \mathrm{M2F}(p)$.

(84) If $\operatorname{len} p = 3$, then $\langle\langle p(1)(1)\rangle, \langle p(2)(1)\rangle, \langle p(3)(1)\rangle\rangle = p$.

(85) If $\operatorname{len} p = 3$, then $\mathrm{F2M}(\mathrm{M2F}(p)) = p$. The theorem is a consequence of (84).

(86) Let us consider a finite sequence p of elements of $\mathbb{R}$. If $\operatorname{len} p = 3$, then $\mathrm{M2F}(\mathrm{F2M}(p)) = p$.

(87) (i) $\langle e_1\rangle^{\mathrm{T}} = \mathrm{F2M}(e_1)$, and

(ii) $\langle e_2\rangle^{\mathrm{T}} = \mathrm{F2M}(e_2)$, and

(iii) $\langle e_3\rangle^{\mathrm{T}} = \mathrm{F2M}(e_3)$.

The theorem is a consequence of (69).

(88) Let us consider a finite sequence p of elements of D. If $\operatorname{len} p = 3$, then $\langle p\rangle^{\mathrm{T}} = \mathrm{F2M}(p)$. The theorem is a consequence of (77).

(89) $\mathrm{Line}(\langle p_1\rangle, 1) = p_1$.

(90) Let us consider a matrix M over D of dimension 3×1. Then

(i) $\mathrm{Line}(M,1)=\langle M_{1,1}\rangle$, and

(ii) $\mathrm{Line}(M,2)=\langle M_{2,1}\rangle$, and

(iii) $\mathrm{Line}(M,3)=\langle M_{3,1}\rangle$.

From now on R denotes a ring.

Now we state the propositions:

(91) Let us consider a square matrix N over R of dimension 3, and a finite sequence p of elements of R. If $\mathrm{len}\, p = 3$, then $N \cdot \langle p\rangle^{\mathrm{T}}$ is 3,1-size.

(92) Let us consider a finite sequence p_1 of elements of R, and a square matrix N over R of dimension 3. Suppose $\mathrm{len}\, p_1 = 3$. Then

(i) $\mathrm{Line}(N \cdot \langle p_1\rangle^{\mathrm{T}}, 1) = \langle (N \cdot \langle p_1\rangle^{\mathrm{T}})_{1,1}\rangle$, and

(ii) $\mathrm{Line}(N \cdot \langle p_1\rangle^{\mathrm{T}}, 2) = \langle (N \cdot \langle p_1\rangle^{\mathrm{T}})_{2,1}\rangle$, and

(iii) $\mathrm{Line}(N \cdot \langle p_1\rangle^{\mathrm{T}}, 3) = \langle (N \cdot \langle p_1\rangle^{\mathrm{T}})_{3,1}\rangle$.

The theorem is a consequence of (91) and (90).

(93) $(\langle p_1\rangle^{\mathrm{T}})_{\square,1} = p_1$. The theorem is a consequence of (89).

(94) Let us consider finite sequences p_1, q_1, r_1 of elements of $\mathbb{R}_{\mathrm{F}}$. Suppose $p = p_1$ and $q = q_1$ and $r = r_1$ and $\langle|p,q,r|\rangle \neq 0$. Then there exists a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension 3 such that

(i) M is invertible, and

(ii) $M \cdot p_1 = \mathrm{F2M}(e_1)$, and

(iii) $M \cdot q_1 = \mathrm{F2M}(e_2)$, and

(iv) $M \cdot r_1 = \mathrm{F2M}(e_3)$.

PROOF: Reconsider $P = \langle\langle (p)_{\mathbf{1}}, (p)_{\mathbf{2}}, (p)_{\mathbf{3}}\rangle, \langle (q)_{\mathbf{1}}, (q)_{\mathbf{2}}, (q)_{\mathbf{3}}\rangle, \langle (r)_{\mathbf{1}}, (r)_{\mathbf{2}}, (r)_{\mathbf{3}}\rangle\rangle$ as a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3. $\langle|p,q,r|\rangle = \mathrm{Det}\, P$. Consider N being a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3 such that N is inverse of P^{T}. $N \cdot \langle p_1\rangle^{\mathrm{T}}$ is a matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3×1 and $N \cdot \langle q_1\rangle^{\mathrm{T}}$ is a matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3×1 and $N \cdot \langle r_1\rangle^{\mathrm{T}}$ is a matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3×1. $N \cdot \langle p_1\rangle^{\mathrm{T}} = \mathrm{F2M}(e_1)$ by (78), [3, (91), (45), (1)]. $N \cdot \langle q_1\rangle^{\mathrm{T}} = \mathrm{F2M}(e_2)$ by (78), [3, (91), (45), (1)]. $N \cdot \langle r_1\rangle^{\mathrm{T}} = \mathrm{F2M}(e_3)$ by (78), [3, (91), (45), (1)]. □

(95) Let us consider finite sequences p_1, q_1, r_1 of elements of $\mathbb{R}_{\mathrm{F}}$, and finite sequences p_2, q_2, r_2 of elements of $\mathbb{R}^1$. Suppose $P = \langle\langle (p)_{\mathbf{1}}, (q)_{\mathbf{1}}, (r)_{\mathbf{1}}\rangle, \langle (p)_{\mathbf{2}}, (q)_{\mathbf{2}}, (r)_{\mathbf{2}}\rangle, \langle (p)_{\mathbf{3}}, (q)_{\mathbf{3}}, (r)_{\mathbf{3}}\rangle\rangle$ and $p = p_1$ and $q = q_1$ and $r = r_1$ and $p_2 = M \cdot p_1$ and $q_2 = M \cdot q_1$ and $r_2 = M \cdot r_1$. Then $(M \cdot P)^{\mathrm{T}} = \langle \mathrm{M2F}(p_2), \mathrm{M2F}(q_2), \mathrm{M2F}(r_2)\rangle$.

PROOF: $P^{\mathrm{T}} = \langle\langle (p)_{\mathbf{1}}, (p)_{\mathbf{2}}, (p)_{\mathbf{3}}\rangle, \langle (q)_{\mathbf{1}}, (q)_{\mathbf{2}}, (q)_{\mathbf{3}}\rangle, \langle (r)_{\mathbf{1}}, (r)_{\mathbf{2}}, (r)_{\mathbf{3}}\rangle\rangle$. $\mathrm{width}\, M = \mathrm{len}\langle p_1\rangle^{\mathrm{T}}$ and $\mathrm{width}\, M = \mathrm{len}\langle q_1\rangle^{\mathrm{T}}$ and $\mathrm{width}\, M = \mathrm{len}\langle r_1\rangle^{\mathrm{T}}$ by (75), [11, (50)]. $\mathrm{len}\, p_2 = 3$ and $\mathrm{len}\, q_2 = 3$ and $\mathrm{len}\, r_2 = 3$. □

(96) Let us consider finite sequences p_2, q_2, r_2 of elements of $\mathbb{R}^1$. Suppose $M = \langle \text{M2F}(p_2), \text{M2F}(q_2), \text{M2F}(r_2) \rangle$ and $\text{Det}\, M = 0$ and $\text{M2F}(p_2) = p$ and $\text{M2F}(q_2) = q$ and $\text{M2F}(r_2) = r$. Then $\langle |p, q, r| \rangle = 0$. The theorem is a consequence of (35).

(97) Let us consider points p_3, q_3, r_3 of $\mathcal{E}^3_{\mathrm{T}}$, finite sequences p_2, q_2, r_2 of elements of $\mathbb{R}^1$, and finite sequences p_1, q_1, r_1 of elements of $\mathbb{R}_{\mathrm{F}}$. Suppose M is invertible and $p = p_1$ and $q = q_1$ and $r = r_1$ and $p_2 = M \cdot p_1$ and $q_2 = M \cdot q_1$ and $r_2 = M \cdot r_1$ and $\text{M2F}(p_2) = p_3$ and $\text{M2F}(q_2) = q_3$ and $\text{M2F}(r_2) = r_3$. Then $\langle |p, q, r| \rangle = 0$ if and only if $\langle |p_3, q_3, r_3| \rangle = 0$. The theorem is a consequence of (19), (23), (95), and (35).

(98) If $0 < m$, then every matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension $m \times 1$ is a finite sequence of elements of $\mathbb{R}^1$.

Proof: Consider s being a finite sequence such that $s \in \text{rng}\, M$ and $\text{len}\, s = 1$. Consider n being a natural number such that for every object x such that $x \in \text{rng}\, M$ there exists a finite sequence s such that $s = x$ and $\text{len}\, s = n$. Consider s_1 being a finite sequence such that $s_1 = s$ and $\text{len}\, s_1 = n$. $\text{rng}\, M \subseteq \mathbb{R}^1$ by [5, (132)]. $\square$

(99) Let us consider a finite sequence u_1 of elements of $\mathbb{R}_{\mathrm{F}}$. Suppose $\text{len}\, u_1 = 3$. Then $\langle u_1 \rangle^{\mathrm{T}} = I^{3\times 3}_{\mathbb{R}_{\mathrm{F}}} \cdot \langle u_1 \rangle^{\mathrm{T}}$. The theorem is a consequence of (77), (91), (2), (68), (7), and (93).

(100) Let us consider an element u of $\mathcal{E}^3_{\mathrm{T}}$, and a finite sequence u_1 of elements of $\mathbb{R}_{\mathrm{F}}$. Suppose $u = u_1$ and $\langle u_1 \rangle^{\mathrm{T}} = \langle \langle 0 \rangle, \langle 0 \rangle, \langle 0 \rangle \rangle$. Then $u = 0_{\mathcal{E}^3_{\mathrm{T}}}$. The theorem is a consequence of (77).

(101) Let us consider an invertible square matrix N over $\mathbb{R}_{\mathrm{F}}$ of dimension 3, elements u, μ of $\mathcal{E}^3_{\mathrm{T}}$, a finite sequence u_1 of elements of $\mathbb{R}_{\mathrm{F}}$, and a finite sequence u_2 of elements of $\mathbb{R}^1$. Suppose u is not zero and $u = u_1$ and $u_2 = N \cdot u_1$ and $\mu = \text{M2F}(u_2)$. Then μ is not zero. The theorem is a consequence of (75), (85), (80), (8), (99), and (100).

Let N be an invertible square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3. The homography of N yielding a function from the projective space over $\mathcal{E}^3_{\mathrm{T}}$ into the projective space over $\mathcal{E}^3_{\mathrm{T}}$ is defined by

(Def. 4) for every point x of the projective space over $\mathcal{E}^3_{\mathrm{T}}$, there exist elements u, v of $\mathcal{E}^3_{\mathrm{T}}$ and there exists a finite sequence u_1 of elements of $\mathbb{R}_{\mathrm{F}}$ and there exists a finite sequence p of elements of $\mathbb{R}^1$ such that $x =$ the direction of u and u is not zero and $u = u_1$ and $p = N \cdot u_1$ and $v = \text{M2F}(p)$ and v is not zero and $\mathit{it}(x) =$ the direction of v.

Now we state the proposition:

(102) Let us consider an invertible square matrix N over $\mathbb{R}_{\mathrm{F}}$ of dimension 3, and points p, q, r of the projective space over $\mathcal{E}^3_{\mathrm{T}}$. Then p, q and r are

collinear if and only if (the homography of N)(p), (the homography of N)(q) and (the homography of N)(r) are collinear.

PROOF: If p, q and r are collinear, then (the homography of N)(p), (the homography of N)(q) and (the homography of N)(r) are collinear by [10, (23)], (43), [9, (22), (1)]. If (the homography of N)(p), (the homography of N)(q) and (the homography of N)(r) are collinear, then p, q and r are collinear. □

References

[1] Susanne Apel. *The geometry of brackets and the area principle.* Phd thesis, Technische Universität München, Fakultät für Mathematik, 2014.

[2] Susanne Apel and Jürgen Richter-Gebert. Cancellation patterns in automatic geometric theorem proving. In *Automated Deduction in Geometry*, pages 1–33. Springer, 2010.

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

[4] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

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

[6] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.

[7] Laurent Fuchs and Laurent Thery. A formalization of Grassmann-Cayley algebra in Coq and its application to theorem proving in projective geometry. In *Automated Deduction in Geometry*, pages 51–67. Springer, 2010.

[8] Kanchun, Hiroshi Yamazaki, and Yatsuka Nakamura. Cross products and tripple vector products in 3-dimensional Euclidean space. *Formalized Mathematics*, 11(**4**):381–383, 2003.

[9] Wojciech Leończuk and Krzysztof Prażmowski. A construction of analytical projective space. *Formalized Mathematics*, 1(**4**):761–766, 1990.

[10] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces – part I. *Formalized Mathematics*, 1(**4**):767–776, 1990.

[11] Xiquan Liang, Piqing Zhao, and Ou Bai. Vector functions and their differentiation formulas in 3-dimensional Euclidean spaces. *Formalized Mathematics*, 18(**1**):1–10, 2010. doi:10.2478/v10037-010-0001-2.

[12] Nicolas Magaud, Julien Narboux, and Pascal Schreck. Formalizing projective plane geometry in Coq. In *Automated Deduction in Geometry*, pages 141–162. Springer, 2008.

[13] Timothy James McKenzie Makarios. A mechanical verification of the independence of Tarski's Euclidean Axiom. Victoria University of Wellington, New Zealand, 2012. Master's thesis.

[14] Karol Pąk. Basic properties of the rank of matrices over a field. *Formalized Mathematics*, 15(**4**):199–211, 2007. doi:10.2478/v10037-007-0024-5.

[15] Karol Pąk. Linear transformations of Euclidean topological spaces. *Formalized Mathematics*, 19(**2**):103–108, 2011. doi:10.2478/v10037-011-0016-3.

[16] Jürgen Richter-Gebert. Mechanical theorem proving in projective geometry. *Annals of Mathematics and Artificial Intelligence*, 13(1-2):139–172, 1995.

[17] Jürgen Richter-Gebert. *Perspectives on projective geometry: a guided tour through real and complex geometry.* Springer Science & Business Media, 2011.

[18] Wojciech Skaba. The collinearity structure. *Formalized Mathematics*, 1(**4**):657–659, 1990.
[19] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

Received October 18, 2016

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 24, No. 4, Pages 253–259, 2016
DOI: 10.1515/forma-2016-0021

DE GRUYTER OPEN
degruyter.com/view/j/forma

The Basic Existence Theorem of Riemann-Stieltjes Integral

Kazuhisa Nakasho
Akita Prefectural University
Akita, Japan

Keiko Narita
Hirosaki-city
Aomori, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, the basic existence theorem of Riemann-Stieltjes integral is formalized. This theorem states that if f is a continuous function and ρ is a function of bounded variation in a closed interval of real line, f is Riemann-Stieltjes integrable with respect to ρ. In the first section, basic properties of real finite sequences are formalized as preliminaries. In the second section, we formalized the existence theorem of the Riemann-Stieltjes integral. These formalizations are based on [15], [12], [10], and [11].

MSC: 26A42 26A45 03B35

Keywords: Riemann-Stieltjes integral; bounded variation; continuous function

MML identifier: INTEGR23, version: 8.1.05 5.39.1282

1. Preliminaries

Now we state the propositions:

(1) Let us consider a real number E, a finite sequence q of elements of $\mathbb{R}$, and a finite sequence S of elements of $\mathbb{R}$. Suppose $\operatorname{len} S = \operatorname{len} q$ and for every natural number i such that $i \in \operatorname{dom} S$ there exists a real number r such that $r = q(i)$ and $S(i) = r \cdot E$. Then $\sum S = \sum q \cdot E$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence q of elements of $\mathbb{R}$ for every finite sequence S of elements of $\mathbb{R}$ such that $\$_1 = \operatorname{len} S$

ISSN 1426–2630(Print), 1898-9934(Online)

and $\operatorname{len} S = \operatorname{len} q$ and for every natural number i such that $i \in \operatorname{dom} S$ there exists a real number r such that $r = q(i)$ and $S(i) = r \cdot E$ holds $\sum S = \sum q \cdot E$. $\mathcal{P}[0]$ by [7, (72)]. For every natural number i, $\mathcal{P}[i]$ from [1, Sch. 2]. □

(2) Let us consider finite sequences x, y of elements of $\mathbb{R}$. Suppose $\operatorname{len} x = \operatorname{len} y$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} x$ there exists a real number v such that $v = x(i)$ and $y(i) = |v|$. Then $|\sum x| \leqslant \sum y$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequences x, y of elements of $\mathbb{R}$ such that $\$_1 = \operatorname{len} x$ and $\operatorname{len} x = \operatorname{len} y$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} x$ there exists a real number v such that $v = x(i)$ and $y(i) = |v|$ holds $|\sum x| \leqslant \sum y$. $\mathcal{P}[0]$ by [7, (72)], [3, (44)]. For every natural number i, $\mathcal{P}[i]$ from [1, Sch. 2]. □

(3) Let us consider finite sequences p, q of elements of $\mathbb{R}$. Suppose $\operatorname{len} p = \operatorname{len} q$ and for every natural number j such that $j \in \operatorname{dom} p$ holds $|p(j)| \leqslant q(j)$. Then $|\sum p| \leqslant \sum q$.

PROOF: Define $\mathcal{P}[\text{natural number}, \text{set}] \equiv$ there exists a real number v such that $v = p(\$_1)$ and $\$_2 = |v|$. For every natural number i such that $i \in \operatorname{Seg} \operatorname{len} p$ there exists an element x of $\mathbb{R}$ such that $\mathcal{P}[i, x]$. Consider u being a finite sequence of elements of $\mathbb{R}$ such that $\operatorname{dom} u = \operatorname{Seg} \operatorname{len} p$ and for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} p$ holds $\mathcal{P}[i, u(i)]$ from [2, Sch. 5]. For every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} p$ there exists a real number v such that $v = p(i)$ and $u(i) = |v|$. $|\sum p| \leqslant \sum u$. □

(4) Let us consider a natural number n, and an object a. Then $\operatorname{len}(n \mapsto a) = n$.

(5) Let us consider a finite sequence p, and an object a. Then $p = \operatorname{len} p \mapsto a$ if and only if for every object k such that $k \in \operatorname{dom} p$ holds $p(k) = a$.

PROOF: If $p = \operatorname{len} p \mapsto a$, then for every object k such that $k \in \operatorname{dom} p$ holds $p(k) = a$ by [4, (57)]. □

(6) Let us consider a finite sequence p of elements of $\mathbb{R}$, a natural number i, and a real number r. Suppose $i \in \operatorname{dom} p$ and $p(i) = r$ and for every natural number k such that $k \in \operatorname{dom} p$ and $k \neq i$ holds $p(k) = 0$. Then $\sum p = r$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence p of elements of $\mathbb{R}$ for every natural number i for every real number r such that $\operatorname{len} p = \$_1$ and $i \in \operatorname{dom} p$ and $p(i) = r$ and for every natural number k such that $k \in \operatorname{dom} p$ and $k \neq i$ holds $p(k) = 0$ holds $\sum p = r$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [4, (19), (16)], [18, (25)], [17, (7)]. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 2]. □

(7) Let us consider finite sequences p, q of elements of $\mathbb{R}$. Suppose $\operatorname{len} p \leqslant$

$\operatorname{len} q$ and for every natural number i such that $i \in \operatorname{dom} q$ holds if $i \leqslant \operatorname{len} p$, then $q(i) = p(i)$ and if $\operatorname{len} p < i$, then $q(i) = 0$. Then $\sum q = \sum p$.

PROOF: Consider i_1 being a natural number such that $i_1 = \operatorname{len} q - \operatorname{len} p$. Set $x = i_1 \mapsto (0$ **qua** real number). $q = p \frown x$ by (4), [18, (25)], [16, (13)], [4, (57)]. □

(8) Let us consider real numbers a, b, c, d. If $b \leqslant c$, then $[a, b] \cap [c, d] \subseteq [b, b]$.

(9) Let us consider a real number a, a subset A of $\mathbb{R}$, and a real-valued function ϱ. If $A \subseteq [a, a]$, then $\operatorname{vol}(A, \varrho) = 0$.

(10) Let us consider a non empty, increasing finite sequence s of elements of $\mathbb{R}$, and a natural number m. Suppose $m \in \operatorname{dom} s$. Then $s \restriction m$ is a non empty, increasing finite sequence of elements of $\mathbb{R}$.

PROOF: Set $H = s \restriction m$. For every extended reals e_1, e_2 such that e_1, $e_2 \in \operatorname{dom} H$ and $e_1 < e_2$ holds $H(e_1) < H(e_2)$ by [19, (57)], [5, (47)]. □

(11) Let us consider non empty, increasing finite sequences s, t of elements of $\mathbb{R}$. Suppose $s(\operatorname{len} s) < t(1)$. Then $s \frown t$ is a non empty, increasing finite sequence of elements of $\mathbb{R}$.

PROOF: Set $H = s \frown t$. For every extended reals e_1, e_2 such that e_1, $e_2 \in \operatorname{dom} H$ and $e_1 < e_2$ holds $H(e_1) < H(e_2)$ by [18, (25)], [2, (25), (3)]. □

(12) Let us consider a non empty, increasing finite sequence s of elements of $\mathbb{R}$, and a real number a. Suppose $s(\operatorname{len} s) < a$. Then $s \frown \langle a \rangle$ is a non empty, increasing finite sequence of elements of $\mathbb{R}$. The theorem is a consequence of (11).

(13) Let us consider a finite sequence T of elements of $\mathbb{R}$, and natural numbers n, m. Suppose $n + 1 < m \leqslant \operatorname{len} T$. Then there exists a finite sequence T_1 of elements of $\mathbb{R}$ such that

(i) $\operatorname{len} T_1 = m - (n + 1)$, and

(ii) $\operatorname{rng} T_1 \subseteq \operatorname{rng} T$, and

(iii) for every natural number i such that $i \in \operatorname{dom} T_1$ holds $T_1(i) = T(i + n)$.

PROOF: Define $\mathcal{F}(\text{natural number}) = T(\$_1 + n)$. Reconsider $m_1 = m - (n + 1)$ as a natural number. Consider p being a finite sequence such that $\operatorname{len} p = m_1$ and for every natural number k such that $k \in \operatorname{dom} p$ holds $p(k) = \mathcal{F}(k)$ from [2, Sch. 2]. $\operatorname{rng} p \subseteq \operatorname{rng} T$ by [18, (25)], [5, (3)]. □

(14) Let us consider a non empty, increasing finite sequence T of elements of $\mathbb{R}$, and natural numbers n, m. Suppose $n + 1 < m \leqslant \operatorname{len} T$. Then there exists a non empty, increasing finite sequence T_1 of elements of $\mathbb{R}$ such that

(i) $\operatorname{len} T_1 = m - (n+1)$, and

(ii) $\operatorname{rng} T_1 \subseteq \operatorname{rng} T$, and

(iii) for every natural number i such that $i \in \operatorname{dom} T_1$ holds $T_1(i) = T(i+n)$.

PROOF: Consider p being a finite sequence of elements of $\mathbb{R}$ such that $\operatorname{len} p = m-(n+1)$ and $\operatorname{rng} p \subseteq \operatorname{rng} T$ and for every natural number i such that $i \in \operatorname{dom} p$ holds $p(i) = T(i+n)$. For every extended reals e_1, e_2 such that e_1, $e_2 \in \operatorname{dom} p$ and $e_1 < e_2$ holds $p(e_1) < p(e_2)$ by [18, (25)]. □

(15) Let us consider a finite sequence p of elements of $\mathbb{R}$, and natural numbers n, m. Suppose $n+1 < m \leqslant \operatorname{len} p$. Then there exists a finite sequence p_1 of elements of $\mathbb{R}$ such that

(i) $\operatorname{len} p_1 = m - (n+1) - 1$, and

(ii) $\operatorname{rng} p_1 \subseteq \operatorname{rng} p$, and

(iii) for every natural number i such that $i \in \operatorname{dom} p_1$ holds $p_1(i) = p(i+n+1)$.

The theorem is a consequence of (13).

2. Existence of Riemann-Stieltjes Integral for Continuous Functions

Now we state the propositions:

(16) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, a partition T of A, a real-valued function ϱ, a non empty, closed interval subset B of $\mathbb{R}$, a non empty, increasing finite sequence S_0 of elements of $\mathbb{R}$, and a finite sequence S_1 of elements of $\mathbb{R}$.
Suppose $B \subseteq A$ and $\inf B = \inf A$ and there exists a partition S of B such that $S = S_0$ and $\operatorname{len} S_1 = \operatorname{len} S$ and for every natural number j such that $j \in \operatorname{dom} S$ there exists a finite sequence p of elements of $\mathbb{R}$ such that $S_1(j) = \sum p$ and $\operatorname{len} p = \operatorname{len} T$ and for every natural number i such that $i \in \operatorname{dom} T$ holds $p(i) = |\operatorname{vol}(\operatorname{divset}(T,i) \cap \operatorname{divset}(S,j), \varrho)|$.
Then there exists a partition H of B and there exists a var-volume F of ϱ and H such that $\sum S_1 = \sum F$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non empty, closed interval subset B of $\mathbb{R}$ for every non empty, increasing finite sequence S_0 of elements of $\mathbb{R}$ for every finite sequence S_1 of elements of $\mathbb{R}$ such that $B \subseteq A$ and $\inf B = \inf A$ and $\operatorname{len} S_0 = \$_1$ and there exists a partition S of B such that $S = S_0$ and $\operatorname{len} S_1 = \operatorname{len} S$ and for every natural number j such

that $j \in \operatorname{dom} S$ there exists a finite sequence p of elements of $\mathbb{R}$ such that $S_1(j) = \sum p$ and $\operatorname{len} p = \operatorname{len} T$ and for every natural number i such that $i \in \operatorname{dom} T$ holds $p(i) = |\operatorname{vol}(\operatorname{divset}(T,i) \cap \operatorname{divset}(S,j), \varrho)|$ there exists a partition H of B and there exists a var-volume F of ϱ and H such that $\sum S_1 = \sum F$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [18, (29)], [1, (14)], [18, (25)], [2, (40)]. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 2]. □

(17) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, a function ϱ from A into $\mathbb{R}$, and partitions T, S of A. Suppose ϱ is bounded-variation. Then there exists a finite sequence S_1 of elements of $\mathbb{R}$ such that

(i) $\operatorname{len} S_1 = \operatorname{len} S$, and

(ii) $\sum S_1 \leqslant \operatorname{TotalVD}(\varrho)$, and

(iii) for every natural number j such that $j \in \operatorname{dom} S$ there exists a finite sequence p of elements of $\mathbb{R}$ such that $S_1(j) = \sum p$ and $\operatorname{len} p = \operatorname{len} T$ and for every natural number i such that $i \in \operatorname{dom} T$ holds $p(i) = |\operatorname{vol}(\operatorname{divset}(T,i) \cap \operatorname{divset}(S,j), \varrho)|$.

PROOF: Define $\mathcal{P}[\text{natural number}, \text{object}] \equiv$ there exists a finite sequence p of elements of $\mathbb{R}$ such that $\$_2 = \sum p$ and $\operatorname{len} p = \operatorname{len} T$ and for every natural number i such that $i \in \operatorname{dom} T$ holds $p(i) = |\operatorname{vol}(\operatorname{divset}(T,i) \cap \operatorname{divset}(S, \$_1), \varrho)|$. For every natural number j such that $j \in \operatorname{Seg} \operatorname{len} S$ there exists an element x of $\mathbb{R}$ such that $\mathcal{P}[j,x]$. Consider S_1 being a finite sequence of elements of $\mathbb{R}$ such that $\operatorname{dom} S_1 = \operatorname{Seg} \operatorname{len} S$ and for every natural number j such that $j \in \operatorname{Seg} \operatorname{len} S$ holds $\mathcal{P}[j, S_1(j)]$ from [2, Sch. 5]. Consider H being a partition of A, F being a var-volume of ϱ and H such that $\sum S_1 = \sum F$. □

(18) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, a function ϱ from A into $\mathbb{R}$, and a partial function u from $\mathbb{R}$ to $\mathbb{R}$.
Suppose ϱ is bounded-variation and $\operatorname{dom} u = A$ and $u{\restriction}A$ is uniformly continuous. Let us consider a division sequence T of A, and a middle volume sequence S of ϱ, u and T. Suppose δ_T is convergent and $\lim \delta_T = 0$. Then middle-sum(S) is convergent.

PROOF: For every division sequence T of A and for every middle volume sequence S of ϱ, u and T such that δ_T is convergent and $\lim \delta_T = 0$ holds middle-sum(S) is convergent by [14, (6)], [9, (9)], [8, (87)], [6, (5)]. □

(19) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, a function ϱ from A into $\mathbb{R}$, a partial function u from $\mathbb{R}$ to $\mathbb{R}$, division sequences T_0, T, T_1 of A, a middle volume sequence S_0 of ϱ, u and T_0, and a middle volume sequence S of ϱ, u and T.

Suppose for every natural number i, $T_1(2 \cdot i) = T_0(i)$ and $T_1(2 \cdot i+1) = T(i)$. Then there exists a middle volume sequence S_1 of ϱ, u and T_1 such that for every natural number i, $S_1(2 \cdot i) = S_0(i)$ and $S_1(2 \cdot i + 1) = S(i)$.

PROOF: Reconsider $S_3 = S_0$, $S_2 = S$ as a sequence of $\mathbb{R}^*$. Define $\mathcal{F}$(natural number) $= S_3(\$_1)(\in \mathbb{R}^*)$. Define $\mathcal{G}$(natural number) $= S_2(\$_1)(\in \mathbb{R}^*)$. Consider S_1 being a sequence of $\mathbb{R}^*$ such that for every natural number n, $S_1(2 \cdot n) = \mathcal{F}(n)$ and $S_1(2 \cdot n + 1) = \mathcal{G}(n)$ from [13, Sch. 1]. For every element i of $\mathbb{N}$, $S_1(i)$ is a middle volume of ϱ, u and $T_1(i)$ by [13, (14)], [6, (5)]. □

(20) Let us consider sequences S_1, S_2, S_3 of real numbers. Suppose S_3 is convergent and for every natural number i, $S_3(2 \cdot i) = S_1(i)$ and $S_3(2 \cdot i + 1) = S_2(i)$. Then

(i) S_1 is convergent, and

(ii) $\lim S_1 = \lim S_3$, and

(iii) S_2 is convergent, and

(iv) $\lim S_2 = \lim S_3$.

PROOF: For every real number r such that $0 < r$ there exists a natural number m_1 such that for every natural number i such that $m_1 \leqslant i$ holds $|S_1(i) - \lim S_3| < r$ by [13, (14)], [1, (11)]. For every real number r such that $0 < r$ there exists a natural number m_1 such that for every natural number i such that $m_1 \leqslant i$ holds $|S_2(i) - \lim S_3| < r$ by [13, (14)], [1, (11)]. □

(21) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, a function ϱ from A into $\mathbb{R}$, and a continuous partial function u from $\mathbb{R}$ to $\mathbb{R}$. Suppose ϱ is bounded-variation and $\operatorname{dom} u = A$. Then u is Riemann-Stieltjes integrable with ϱ.

PROOF: Consider T_0 being a division sequence of A such that δ_{T_0} is convergent and $\lim \delta_{T_0} = 0$. Set $S_0 =$ the middle volume sequence of ϱ, u and T_0. Set $I = \lim$ middle-sum(S_0). For every division sequence T of A and for every middle volume sequence S of ϱ, u and T such that δ_T is convergent and $\lim \delta_T = 0$ holds middle-sum(S) is convergent and $\lim$ middle-sum$(S) = I$ by (18), [13, (15)], (19), [13, (16)]. □

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

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

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

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

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

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

[7] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[9] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Darboux's theorem. *Formalized Mathematics*, 9(**1**):197–200, 2001.

[10] S.L. Gupta and Nisha Rani. *Fundamental Real Analysis*. Vikas Pub., 1986.

[11] Einar Hille. *Methods in classical and functional analysis*. Addison-Wesley Publishing Co., Halsted Press, 1974.

[12] H. Kestelman. *Modern theories of integration*. Dover Publications, 2nd edition, 1960.

[13] Keiko Narita, Noboru Endou, and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into real Banach space. *Formalized Mathematics*, 21(**2**):145–152, 2013. doi:10.2478/forma-2013-0016.

[14] Keiko Narita, Kazuhisa Nakasho, and Yasunari Shidama. Riemann-Stieltjes integral. *Formalized Mathematics*, 24(**3**):199–204, 2016. doi:10.1515/forma-2016-0016.

[15] Daniel W. Stroock. *A Concise Introduction to the Theory of Integration*. Springer Science & Business Media, 1999.

[16] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

[17] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[18] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[19] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received October 18, 2016

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 24, No. 4, Pages 261–273, 2016
DOI: 10.1515/forma-2016-0022

DE GRUYTER OPEN
degruyter.com/view/j/forma

On Subnomials

Rafał Ziobro
Department of Carbohydrate Technology
University of Agriculture
Krakow, Poland

Summary. While discussing the sum of consecutive powers as a result of division of two binomials W.W. Sawyer [12] observes

> "It is a curious fact that most algebra textbooks give our ast result twice. It appears in two different chapters and usually there is no mention in either of these that it also occurs in the other. The first chapter, of course, is that on factors. The second is that on geometrical progressions. Geometrical progressions are involved in nearly all financial questions involving compound interest – mortgages, annuities, etc."

It's worth noticing that the first issue involves a simple arithmetical division of 99...9 by 9. While the above notion seems not have changed over the last 50 years, it reflects only a special case of a broader class of problems involving two variables. It seems strange, that while binomial formula is discussed and studied widely [7], [8], little research is done on its counterpart with all coefficients equal to one, which we will call here the subnomial. The study focuses on its basic properties and applies it to some simple problems usually proven by induction [6].

MSC: 40-04 03B35

Keywords: binomial formula; geometrical progression; polynomials

MML identifier: NEWTON04, version: 8.1.05 5.39.1282

From now on a, b, i, j, k, l, m, n denote natural numbers.

Let a be a positive real number and n be a natural number. Let us note that a^n is positive.

Let a be a non negative real number. One can check that a^n is non negative.

Let us observe that $\sqrt{a^2}$ reduces to a.

Observe that there exists a complex which is real and there exists a complex which is non real.

ISSN 1426–2630(Print), 1898-9934(Online)

Let a be a non real complex. One can verify that $\Im(a)$ is non zero.

Let a be a real number. One can check that $\Re(a)$ reduces to a.

Now we state the proposition:

(1) Let us consider a non zero real number a, and a complex a_1. If $a \cdot a_1$ is a real number, then a_1 is a real number.

Note that every binary relation which is $\mathbb{R}$-valued is also $\mathbb{C}$-valued and every binary relation which is $\mathbb{Q}$-valued is also $\mathbb{R}$-valued and every binary relation which is $\mathbb{Q}$-valued is also $\mathbb{C}$-valued and every binary relation which is $\mathbb{Z}$-valued is also $\mathbb{Q}$-valued and every binary relation which is $\mathbb{Z}$-valued is also $\mathbb{R}$-valued and every binary relation which is $\mathbb{Z}$-valued is also $\mathbb{C}$-valued.

Every binary relation which is $\mathbb{N}$-valued is also $\mathbb{Z}$-valued and every binary relation which is $\mathbb{N}$-valued is also $\mathbb{Q}$-valued and every binary relation which is $\mathbb{N}$-valued is also $\mathbb{R}$-valued and every binary relation which is $\mathbb{N}$-valued is also $\mathbb{C}$-valued and every binary relation which is real-valued is also $\mathbb{R}$-valued and every binary relation which is complex-valued is also $\mathbb{C}$-valued.

Let a be an object. Observe that $1 \cdot \operatorname{len}\langle a \rangle$ reduces to 1.

Let f be a finite sequence. Let us note that $(\langle a \rangle \frown f)(1)$ reduces to a and $(f \frown \langle a \rangle)(1 + \operatorname{len} f)$ reduces to a.

Let x be a complex. Observe that $\sum \langle x \rangle$ reduces to x.

Let f, g be finite sequences. Let us note that $(f \frown g) \restriction \operatorname{dom} f$ reduces to f and $(f \frown g) \restriction \operatorname{len} f$ reduces to f.

Now we state the proposition:

(2) Let us consider a finite sequence f. Then there exists a non empty set D such that f is a finite sequence of elements of D.

Let f be a finite sequence. One can check that $f(0)$ reduces to 0 and $f \restriction \operatorname{len} f$ reduces to f. Note that $f_{\lfloor \operatorname{len} f}$ is empty.

Let n be a natural number. One can verify that $\overline{\overline{\operatorname{Seg} n}}$ reduces to n and $\overline{\overline{\mathbb{Z}_n}}$ reduces to n.

Note that $\operatorname{len} \operatorname{id}_{\operatorname{Seg} n}$ reduces to n and $\operatorname{len} \operatorname{idseq}(n)$ reduces to n.

Let m, n be natural numbers. One can check that $(\operatorname{idseq}(m+n))(m)$ reduces to m and $(\operatorname{Rev}(\operatorname{idseq}(m + (n + 1))))(m + 1)$ reduces to $n + 1$.

Let a, b be natural numbers. The functors: $\min(a, b)$ and $\max(a, b)$ yield natural numbers. Let f be a finite sequence and n be a natural number. One can check that $f \restriction (\operatorname{len} f + n)$ reduces to f and $f \restriction \operatorname{Seg} \max(\operatorname{len} f, n)$ reduces to f. One can verify that $f_{\lfloor \operatorname{len} f + n}$ is empty and $f_{\lfloor \operatorname{len} f}(n)$ is zero.

Let us consider an element n of $\mathbb{N}$, a set D, and a finite sequence f of elements of D. Now we state the propositions:

(3) If $n \in \operatorname{dom} f$, then $\operatorname{len}(f \restriction n) = n$.

(4) If $n \geqslant \operatorname{len} f$, then $\operatorname{len}(f \restriction n) = \operatorname{len} f$.

Let f be a finite sequence and n be a non zero natural number. One can verify that $f(\operatorname{len} f + n)$ is zero.

Let f be a finite sequence of elements of $\mathbb{R}$ and i, j be natural numbers. One can verify that $(f \restriction i) \restriction (i + j)$ reduces to $f \restriction i$.

Let a be a natural number. Note that $\sum (a \mapsto 0)$ reduces to 0. Note that $\sum (a \mapsto 0)$ is zero.

Let b be an object. One can verify that $\operatorname{len}(a \mapsto b)$ reduces to a.

Let a be a non zero natural number. Observe that $a \mapsto b$ is non empty and $a \mapsto b$ is constant.

Let us observe that the value of $a \mapsto b$ reduces to b.

Let f be a constant finite sequence. Let us observe that $\operatorname{Rev}(f)$ reduces to f.

Let a be a natural number, b be a non zero natural number, and x be an object. One can check that $((a+b) \mapsto x)(b)$ reduces to x. Let us observe that $(a \mapsto x)(a + b)$ is zero.

Let a be an object and n be a natural number. Observe that $\operatorname{Rev}(n \mapsto a)$ reduces to $n \mapsto a$.

Note that $\binom{n}{0 \cdot 1}$ reduces to 1 and $\binom{n}{n \cdot 1}$ reduces to 1.

Let f be a non-negative yielding finite sequence of elements of $\mathbb{R}$ and i be a natural number. One can check that $f(i)$ is non negative and every finite sequence which is empty is also non-positive yielding.

Let f be a non-positive yielding finite sequence of elements of $\mathbb{R}$ and i be a natural number. Note that $f(i)$ is non positive.

Let f be a non-negative yielding finite sequence of elements of $\mathbb{R}$ and i, j be natural numbers. One can check that $(f \restriction j)(i)$ is non negative and $f_{\lfloor j}(i)$ is non negative.

Let f be an empty, real-valued finite sequence. One can verify that $\prod f$ is non negative.

Let f be a non-negative yielding finite sequence of elements of $\mathbb{R}$. One can verify that $\sum f$ is non negative and $\prod f$ is non negative.

Let f be a non-positive yielding finite sequence of elements of $\mathbb{R}$. Let us note that $\sum f$ is non positive.

Let a be an object and f be a non-negative yielding finite sequence of elements of $\mathbb{R}$. One can check that $f(a)$ is non negative.

Let f be a non-positive yielding finite sequence of elements of $\mathbb{R}$. One can verify that $f(a)$ is non positive.

Let D be a set and f, g be D-valued finite sequences. Let us note that $f \frown g$ is D-valued.

Let f be a finite sequence of elements of $\mathbb{R}$ and n be a natural number. One can verify that $(f \restriction n)_{\lfloor n}$ is empty and $f_{\lfloor \max(\operatorname{len} f, n)}$ is empty.

Let D be a set. One can verify that there exists a finite sequence of elements of D which is empty and every finite sequence of elements of D which is empty is also non-negative yielding and every finite sequence which is non-negative yielding and $\mathbb{Z}$-valued is also $\mathbb{N}$-valued and every finite sequence of elements of $\mathbb{Z}$ which is non-negative yielding is also $\mathbb{N}$-valued.

Let f be a $\mathbb{C}$-valued finite sequence. Note that $f + 0$ reduces to f and $f - 0$ reduces to f.

Let x be an object. One can check that $\langle x \rangle(1)$ reduces to x.

Now we state the propositions:

(5) Let us consider a finite sequence f. Then every permutation of $\operatorname{dom} f$ is a permutation of $\operatorname{dom} \operatorname{Rev}(f)$.

(6) $\operatorname{Rev}(\operatorname{idseq}(n))$ is a permutation of $\operatorname{Seg} n$.

Let us consider a finite sequence f. Now we state the propositions:

(7) $\operatorname{idseq}(\operatorname{len} f)$ is a permutation of $\operatorname{dom} f$.

(8) $\operatorname{Rev}(\operatorname{idseq}(\operatorname{len} f))$ is a permutation of $\operatorname{dom} \operatorname{Rev}(f)$. The theorem is a consequence of (6).

(9) Let us consider a function f, and a permutation h of $\operatorname{dom} f$. Then $\operatorname{dom}(f \cdot h) = \operatorname{dom} f$.

Let f be a finite sequence and h be a permutation of $\operatorname{dom} f$. Observe that $f \cdot h$ is finite sequence-like and $f \cdot h$ is $(\operatorname{dom} f)$-defined.

Let us consider a finite sequence f. Now we state the propositions:

(10) $f = \operatorname{Rev}(f) \cdot \operatorname{Rev}(\operatorname{idseq}(\operatorname{len} f))$.

Proof: Reconsider $P = \operatorname{Rev}(\operatorname{idseq}(\operatorname{len} f))$ as a permutation of $\operatorname{dom} \operatorname{Rev}(f)$. Reconsider $g = \operatorname{Rev}(f) \cdot P$ as a finite sequence. For every object x such that $x \in \operatorname{dom} f$ holds $f(x) = g(x)$ by [13, (25)], [1, (21)], [3, (57)], [4, (12)]. □

(11) f and $\operatorname{Rev}(f)$ are fiberwise equipotent. The theorem is a consequence of (10) and (8).

(12) Let us consider a non empty set D, and a D-valued finite sequence r. Suppose $\operatorname{len} r = i + j$. Then there exist D-valued finite sequences p, q such that

  (i) $\operatorname{len} p = i$, and

  (ii) $\operatorname{len} q = j$, and

  (iii) $r = p \frown q$.

(13) Let us consider a non-negative yielding finite sequence f of elements of $\mathbb{R}$. Then $\sum f \geqslant \sum (f \restriction j)$.

(14) Let us consider a $\mathbb{C}$-valued finite sequence f, and complexes x_1, x_2. Then $(f + x_1) + x_2 = f + (x_1 + x_2)$.

Let f be a $\mathbb{C}$-valued finite sequence and x be a complex. One can check that $f + x - x$ reduces to f and $f - x + x$ reduces to f.

Let x, y be real numbers. One can check that $\max(\min(x, y), \max(x, y))$ reduces to $\max(x, y)$ and $\min(\min(x, y), \max(x, y))$ reduces to $\min(x, y)$.

Let z be a non negative real number. Let us observe that $\min(\min(x, y), y+z)$ reduces to $\min(x, y)$ and $\max(\max(x, y), y - z)$ reduces to $\max(x, y)$.

Let f be a finite sequence and i, j be natural numbers. Observe that $(f{\restriction}i){\restriction}(i+j)$ reduces to $f{\restriction}i$.

Let f be a non-negative yielding finite sequence of elements of $\mathbb{R}$ and n be a natural number. One can check that $f{\restriction}n$ is non-negative yielding and $f_{\lfloor n}$ is non-negative yielding.

Let f be a finite sequence of elements of $\mathbb{R}$. Note that $f - \min f$ is non-negative yielding and $f - \max f$ is non-positive yielding.

Let f be a finite sequence. Let us note that $\mathrm{Rev}(f)$ is $(\mathrm{len}\, f)$-element.

Let D be a non empty set and f be a D-valued finite sequence. Note that $\mathrm{Rev}(f)$ is D-valued.

Let a be a complex and f be a complex-valued finite sequence. Let us note that $a \cdot f$ is $(\mathrm{len}\, f)$-element.

Let a, b be real numbers and n be a natural number.

Note that $\mathrm{len}\langle \binom{n+1-1}{0} a^0 b^{n+1-1}, \ldots, \binom{n+1-1}{n+1-1} a^{n+1-1} b^0 \rangle$ reduces to $n+1$.

Let us note that $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle$ is $(n+1)$-element.

Let us note that $\mathrm{len}\langle \binom{n+1-1}{0}, \ldots, \binom{n+1-1}{n+1-1} \rangle$ reduces to $n+1$. One can verify that $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$ is non-negative yielding and $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$ is $(n+1)$-element.

Let n be a non zero natural number. Let us note that $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle(2)$ reduces to n and $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle(n)$ reduces to n.

Now we state the propositions:

(15) Let us consider complex-valued functions f_1, f_2, f_3. Then $(f_1 \cdot f_2) \cdot f_3 = f_1 \cdot (f_2 \cdot f_3)$.

(16) Let us consider finite sequences f, g of elements of $\mathbb{C}$, and an object i. Then $(f \cdot g)(i) = f(i) \cdot g(i)$.

Let us consider real numbers x, y. Now we state the propositions:

(17) $\max(x, y) - \min(x, y) = |x - y|$.

(18) (i) $\min(x, y) \cdot \max(x, y) = x \cdot y$, and

(ii) $\min(x, y) + \max(x, y) = x + y$.

Let us consider a non-negative yielding finite sequence f of elements of $\mathbb{R}$. Now we state the propositions:

(19) $\sum f \geqslant \sum (f{\restriction}j)$.

(20) If $i \geqslant j$, then $\sum (f{\restriction}i) \geqslant \sum (f{\restriction}j)$. The theorem is a consequence of (19).

(21) $\sum f \geqslant f(n)$.

(22) Let us consider finite sequences f, g, h of elements of $\mathbb{C}$. Suppose $\operatorname{dom} h = \operatorname{dom} f \cap \operatorname{dom} g$. Then $\operatorname{len} h = \min(\operatorname{len} f, \operatorname{len} g)$.

Let us consider finite sequences f, g of elements of $\mathbb{C}$. Now we state the propositions:

(23) $\operatorname{len}(f + g) = \min(\operatorname{len} f, \operatorname{len} g)$. The theorem is a consequence of (22).

(24) $\operatorname{len}(f \cdot g) = \min(\operatorname{len} f, \operatorname{len} g)$. The theorem is a consequence of (22).

(25) $\operatorname{len}(f - g) = \min(\operatorname{len} f, \operatorname{len} g)$. The theorem is a consequence of (23).

(26) Let us consider non-negative yielding finite sequences f, g of elements of $\mathbb{R}$. Then $(f \cdot g)(n) \leqslant \sum f \cdot g(n)$. The theorem is a consequence of (21).

(27) Let us consider a real number r, and a non zero natural number n. Then there exists a finite sequence f of elements of $\mathbb{R}$ such that

(i) $\operatorname{len} f = n$, and

(ii) $\sum f = r$.

Let us consider a finite sequence f of elements of $\mathbb{C}$ and a complex x. Now we state the propositions:

(28) $f + x = f + \operatorname{len} f \mapsto x$.

PROOF: Reconsider $g = \operatorname{len} f \mapsto x$ as a finite sequence of elements of $\mathbb{C}$. $\operatorname{len}(f + g) = \min(\operatorname{len} f, \operatorname{len}(\operatorname{len} f \mapsto x))$. For every natural number i such that $i \in \operatorname{dom}(f + x)$ holds $(f + x)(i) = (f + g)(i)$ by [13, (25)], [1, (21)], [13, (29)]. $\square$

(29) $\sum(f + x) = \sum f + x \cdot \operatorname{len} f$. The theorem is a consequence of (28).

(30) Let us consider a complex-valued finite sequence f, and a complex x. Then $\sum(f - x) = \sum f - x \cdot \operatorname{len} f$. The theorem is a consequence of (29).

(31) Let us consider a finite sequence f of elements of $\mathbb{R}$, and a non-negative yielding finite sequence g of elements of $\mathbb{R}$. If for every natural number x, $f(x) \geqslant g(x)$, then f is non-negative yielding.

(32) Let us consider finite sequences f, g of elements of $\mathbb{R}$. If for every natural number x, $f(x) \geqslant g(x)$, then $\sum f \geqslant \sum g$.

(33) Let us consider a finite sequence f of elements of $\mathbb{C}$.
Then $\sum(f \restriction (1 \textbf{ qua } \text{natural number})) = f((1 \textbf{ qua } \text{natural number}))$.

(34) Let us consider a finite sequence f of elements of $\mathbb{C}$, and a natural number n. Then $\sum(f_{\lfloor n} \restriction 1) = f(n + 1)$. The theorem is a consequence of (33).

(35) Let us consider a finite sequence f, and natural numbers a, b. Then $(f_{\lfloor a})_{\lfloor b} = f_{\lfloor a+b}$. The theorem is a consequence of (2).

Let us consider a finite sequence f of elements of $\mathbb{C}$. Now we state the propositions:

(36) $f = ((f \restriction i) ^\frown (f_{\lfloor i} \restriction (1 \textbf{ qua } \text{natural number}))) ^\frown f_{\lfloor i+1}$. The theorem is a consequence of (35).

(37) $\sum f = \sum (f \restriction i) + f(i+1) + \sum f_{\lfloor i+1}$. The theorem is a consequence of (35) and (34).

(38) Let us consider a finite sequence f, and a non zero natural number i. Then $f(n+i) = f_{\lfloor n}(i)$. The theorem is a consequence of (2).

(39) Let us consider finite sequences f, g of elements of $\mathbb{R}$. Suppose for every natural number x, $f(x) \geqslant g(x)$ and there exists i such that $f(i+1) > g(i+1)$. Then $\sum f > \sum g$.

Proof: Consider i being a natural number such that $f(i+1) > g(i+1)$. $\sum f = \sum (f \restriction i) + f(i+1) + \sum f_{\lfloor i+1}$. $\sum g = \sum (g \restriction i) + g(i+1) + \sum g_{\lfloor i+1}$. For every natural number x, $(f \restriction i)(x) \geqslant (g \restriction i)(x)$ and $f_{\lfloor i+1}(x) \geqslant g_{\lfloor i+1}(x)$ by [13, (112)], [3, (17)], [13, (25)], (38). $\sum (f \restriction i) \geqslant \sum (g \restriction i)$ and $\sum f_{\lfloor i+1} \geqslant \sum g_{\lfloor i+1}$. □

(40) Let us consider non-negative yielding finite sequences f, g of elements of $\mathbb{R}$. Then $\sum f \cdot \sum g \geqslant \sum (f \cdot g)$. The theorem is a consequence of (26) and (32).

(41) Let us consider a complex a, and a complex-valued finite sequence f. Then $\operatorname{len} f \mapsto a \cdot f = a \cdot f$.

Proof: For every object x such that $x \in \operatorname{dom}(\operatorname{len} f \mapsto a \cdot f)$ holds $(\operatorname{len} f \mapsto a \cdot f)(x) = (a \cdot f)(x)$ by [13, (25)], [1, (10)]. □

(42) Let us consider complexes a, b. Then $a \cdot \langle b \rangle = \langle a \cdot b \rangle$.

Proof: For every object x such that $x \in \operatorname{Seg} 1$ holds $\langle a \cdot b \rangle(x) = a \cdot \langle b \rangle(x)$ by [2, (2)]. □

Let us consider a complex a and complex-valued finite sequences f, g. Now we state the propositions:

(43) $a \cdot (f ^\frown g) = (a \cdot f) ^\frown (a \cdot g)$.

Proof: For every object x such that $x \in \operatorname{dom}(a \cdot (f ^\frown g))$ holds $(a \cdot (f ^\frown g))(x) = ((a \cdot f) ^\frown (a \cdot g))(x)$ by [2, (25)]. □

(44) If $g = \operatorname{Rev}(f)$, then $\operatorname{Rev}(a \cdot f) = a \cdot g$.

Proof: Set $h = a \cdot f$. Set $h_1 = a \cdot g$. Set $h_2 = \operatorname{Rev}(h)$. For every object x such that $x \in \operatorname{dom} h_1$ holds $h_1(x) = h_2(x)$ by [13, (25)], [1, (21)], [13, (29)]. □

Let a, b be real numbers and n be a natural number.

The functor $(a, b) \operatorname{Subnomial} n$ yielding a finite sequence of elements of $\mathbb{R}$ is defined by the term

(Def. 1) $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle / \langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$.

Now we state the proposition:

(45) Let us consider real numbers a, b, and a natural number n. Then

(i) $\mathrm{len}\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle = \mathrm{len}\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$, and

(ii) $\mathrm{len}((a,b)\,\mathrm{Subnomial}\, n) = \mathrm{len}\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$, and

(iii) $\mathrm{len}\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle = \mathrm{len}((a,b)\,\mathrm{Subnomial}\, n)$, and

(iv) $\mathrm{dom}\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle = \mathrm{dom}\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$, and

(v) $\mathrm{dom}((a,b)\,\mathrm{Subnomial}\, n) = \mathrm{dom}\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$, and

(vi) $\mathrm{dom}\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle = \mathrm{dom}((a,b)\,\mathrm{Subnomial}\, n)$.

Let a, b be real numbers and n be a natural number.

Note that $\mathrm{len}((a,b)\,\mathrm{Subnomial}(n+1-1))$ reduces to $n+1$. Observe that $(a,b)\,\mathrm{Subnomial}\, n$ is $(n+1)$-element.

Let a, b be integers and n, m be natural numbers.

Observe that $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle(m)$ is integer.

Let n be a natural number. One can check that $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle$ is $\mathbb{Z}$-valued. Now we state the proposition:

(46) Let us consider integers a, b, and a natural number k. Suppose $k \in \mathrm{dom}\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$. Then $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle(k) \mid \langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle(k)$.

Let l, k be natural numbers. Note that $\binom{l+k}{k}$ is positive.

Let l be a natural number and k be a non zero natural number. One can check that $\binom{l}{l+k}$ is zero and $\langle \binom{l}{0}, \ldots, \binom{l}{l} \rangle(l+k+1)$ is zero.

Let k be a natural number. Observe that $\langle \binom{l+k}{0}, \ldots, \binom{l+k}{l+k} \rangle(k+1)$ is positive.

Now we state the proposition:

(47) Let us consider natural numbers k, l. Suppose $k \in \mathrm{dom}\langle \binom{l}{0}, \ldots, \binom{l}{l} \rangle$. Then $\langle \binom{l}{0}, \ldots, \binom{l}{l} \rangle(k)$ is not zero.

Let a, b be integers and m, n be natural numbers. One can check that $((a,b)\,\mathrm{Subnomial}\, n)(m)$ is integer.

Let n be a natural number. Note that $(a,b)\,\mathrm{Subnomial}\, n$ is $\mathbb{Z}$-valued.

Let a, b be real numbers. One can verify that the functor $(a,b)\,\mathrm{Subnomial}\, n$ yields a finite sequence of elements of $\mathbb{R}$ and is defined by

(Def. 2) $\mathrm{len}\, it = n+1$ and for every natural numbers i, l, m such that $i \in \mathrm{dom}\, it$ and $m = i-1$ and $l = n-m$ holds $it(i) = a^l \cdot b^m$.

Let a, b be positive real numbers and k, l be natural numbers. Note that $((a,b)\,\mathrm{Subnomial}(k+l))(k+1)$ is positive.

Let n be a natural number. Let us note that $\sum((a,b)\,\mathrm{Subnomial}\, n)$ is positive.

Let k be a natural number and n be a non zero natural number. One can verify that $\langle \binom{n}{0} 0^0 0^n, \ldots, \binom{n}{n} 0^n 0^0 \rangle(k)$ is zero and $((0,0)\,\mathrm{Subnomial}\, n)(k)$ is zero and $\langle \binom{n}{0} 0^0 0^n, \ldots, \binom{n}{n} 0^n 0^0 \rangle$ is empty yielding and $(0,0)\,\mathrm{Subnomial}\, n$ is empty yielding.

Let f be an empty yielding finite sequence of elements of $\mathbb{C}$. Let us observe that $\sum f$ is zero.

Let n be a natural number. One can check that $\langle\binom{n}{0},\ldots,\binom{n}{n}\rangle(1)$ reduces to 1 and $\langle\binom{n}{0},\ldots,\binom{n}{n}\rangle(n+1)$ reduces to 1.

Now we state the proposition:

(48) Let us consider real numbers a, b, and a natural number n. Then

(i) $\langle\binom{n}{0}a^0b^n,\ldots,\binom{n}{n}a^nb^0\rangle(1)=((a,b)\,\mathrm{Subnomial}\,n)(1)$, and

(ii) $\langle\binom{n}{0}a^0b^n,\ldots,\binom{n}{n}a^nb^0\rangle(n+1)=((a,b)\,\mathrm{Subnomial}\,n)(n+1)$.

Let us consider real numbers a, b. Now we state the propositions:

(49) $(a,b)\,\mathrm{Subnomial}(n+1)=a\cdot((a,b)\,\mathrm{Subnomial}\,n)\frown\langle b^{n+1}\rangle$.

Proof: For every natural number k such that $1\leqslant k\leqslant\mathrm{len}((a,b)\,\mathrm{Subnomial}\,(n+1))$ holds $((a,b)\,\mathrm{Subnomial}(n+1))(k)=(a\cdot((a,b)\,\mathrm{Subnomial}\,n)\frown\langle b^{n+1}\rangle)(k)$ by [13, (25)], [1, (21)], [10, (6)], [5, (16)]. □

(50) $(a,b)\,\mathrm{Subnomial}(n+1)=\langle a^{n+1}\rangle\frown(b\cdot((a,b)\,\mathrm{Subnomial}\,n))$.

Proof: For every natural number k such that $1\leqslant k\leqslant\mathrm{len}((a,b)\,\mathrm{Subnomial}\,(n+1))$ holds $((a,b)\,\mathrm{Subnomial}(n+1))(k)=(\langle a^{n+1}\rangle\frown(b\cdot((a,b)\,\mathrm{Subnomial}\,n)))(k)$ by [1, (13), (21)], [13, (25)], [10, (2), (6)]. □

(51) Let us consider real numbers a, b, and a natural number n. Then $a^{n+1}-b^{n+1}=(a-b)\cdot\sum((a,b)\,\mathrm{Subnomial}\,n)$. The theorem is a consequence of (49) and (50).

(52) Let us consider a real number a, and a non zero natural number n. Then $a^n=\sum((a,0)\,\mathrm{Subnomial}\,n)$. The theorem is a consequence of (51).

(53) Let us consider a real number a, and a natural number n. Then $a^{n+1}=\sum((a,1)\,\mathrm{Subnomial}\,n)\cdot(a-1)+1$. The theorem is a consequence of (51).

(54) Let us consider real numbers a, b, c, d, a natural number n, and an object x. Suppose $x\in\mathrm{dom}((a\cdot b,c\cdot d)\,\mathrm{Subnomial}\,n)$. Then $((a\cdot b,c\cdot d)\,\mathrm{Subnomial}\,n)(x)=((a,d)\,\mathrm{Subnomial}\,n)(x)\cdot((b,c)\,\mathrm{Subnomial}\,n)(x)$.

(55) Let us consider real numbers a, b, c, d, and a natural number n. Then $(a\cdot b,c\cdot d)\,\mathrm{Subnomial}\,n=((a,d)\,\mathrm{Subnomial}\,n)\cdot((b,c)\,\mathrm{Subnomial}\,n)$. The theorem is a consequence of (54).

Let us consider real numbers a, b and a natural number n. Now we state the propositions:

(56) $(a,b)\,\mathrm{Subnomial}\,n=((a,1)\,\mathrm{Subnomial}\,n)\cdot((1,b)\,\mathrm{Subnomial}\,n)$. The theorem is a consequence of (55).

(57) $\langle\binom{n}{0}a^0b^n,\ldots,\binom{n}{n}a^nb^0\rangle=\langle\binom{n}{0},\ldots,\binom{n}{n}\rangle\cdot((a,b)\,\mathrm{Subnomial}\,n)$.

Proof: $\mathrm{dom}\langle\binom{n}{0}a^0b^n,\ldots,\binom{n}{n}a^nb^0\rangle=\mathrm{dom}\langle\binom{n}{0},\ldots,\binom{n}{n}\rangle$. For every object c such that $c\in\mathrm{dom}\langle\binom{n}{0}a^0b^n,\ldots,\binom{n}{n}a^nb^0\rangle$ holds $\langle\binom{n}{0}a^0b^n,\ldots,\binom{n}{n}a^nb^0\rangle(c)=\langle\binom{n}{0},\ldots,\binom{n}{n}\rangle(c)\cdot((a,b)\,\mathrm{Subnomial}\,n)(c)$ by [13, (25)], [1, (10)]. □

(58) (i) $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle = \langle \binom{n}{0} a^0 1^n, \ldots, \binom{n}{n} a^n 1^0 \rangle \cdot ((1, b) \operatorname{Subnomial} n)$, and

(ii) $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle = ((a, 1) \operatorname{Subnomial} n) \cdot \langle \binom{n}{0} 1^0 b^n, \ldots, \binom{n}{n} 1^n b^0 \rangle$.

The theorem is a consequence of (57), (56), and (15).

(59) Let us consider real numbers a, b, c, d, and a natural number n. Then $\langle \binom{n}{0} a \cdot b^0 c \cdot d^n, \ldots, \binom{n}{n} a \cdot b^n c \cdot d^0 \rangle = (\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle \cdot ((a, c) \operatorname{Subnomial} n)) \cdot ((b, d) \operatorname{Subnomial} n)$. The theorem is a consequence of (57) and (55).

(60) Let us consider a real number a, and natural numbers n, i. Suppose $i \in \operatorname{dom}((a, a) \operatorname{Subnomial} n)$. Then $((a, a) \operatorname{Subnomial} n)(i) = a^n$.

Let us consider a natural number n and a real number a. Now we state the propositions:

(61) $(a, a) \operatorname{Subnomial} n = (n + 1) \mapsto a^n$.

PROOF: For every natural number j, $((a, a) \operatorname{Subnomial} n)(j) = ((n + 1) \mapsto a^n)(j)$ by [13, (25)], (60), [1, (10)]. □

(62) $\prod((a, a) \operatorname{Subnomial} n) = a^{n \cdot (n+1)}$. The theorem is a consequence of (61).

(63) Let us consider a natural number n, and n-element, complex-valued finite sequences f, g. Then $\prod(f \cdot g) = \prod f \cdot \prod g$.

(64) Let us consider real numbers a, b, and a natural number n.
Then $(a, b) \operatorname{Subnomial} n = \operatorname{Rev}((b, a) \operatorname{Subnomial} n)$.
PROOF: $\operatorname{dom}((a, b) \operatorname{Subnomial} n) = \operatorname{dom}\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$ and $\operatorname{dom}((b, a) \operatorname{Subnomial} n) = \operatorname{dom}\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$. For every object i such that $i \in \operatorname{dom}((a, b) \operatorname{Subnomial} n)$ holds $((a, b) \operatorname{Subnomial} n)(i) = (\operatorname{Rev}((b, a) \operatorname{Subnomial} n))(i)$ by [13, (26)], [3, (57), (59), (58)]. □

Let n be a natural number and i be a natural number. One can check that $((1, 1) \operatorname{Subnomial}(n + i))(i + 1)$ reduces to 1.

Let i be a non zero natural number. Observe that $((1, -1) \operatorname{Subnomial}(2 \cdot i + n))(2 \cdot i)$ reduces to -1.

Let i be an odd natural number. Let us observe that $((1, -1) \operatorname{Subnomial}(n + i))(i)$ reduces to 1.

Let a be a real number.

One can check that $n \mapsto a$ is constant and $(a, a) \operatorname{Subnomial} n$ is constant.

Let a, b be non negative real numbers and n, k be natural numbers. One can check that $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle(k)$ is non negative and $((a, b) \operatorname{Subnomial} n)(k)$ is non negative.

Now we state the propositions:

(65) Let us consider a real number a, and a natural number n.
Then $\sum((a, a) \operatorname{Subnomial} n) = (n + 1) \cdot a^n$. The theorem is a consequence of (60).

(66) Let us consider a real number a, and an even natural number n. Then $\sum((a,-a)\,\mathrm{Subnomial}\,n) = a^n$. The theorem is a consequence of (65) and (51).

Let n be an even natural number. Note that $\sum((1,-1)\,\mathrm{Subnomial}\,n)$ reduces to 1.

Let a be a real number and n be an odd natural number. One can verify that $\sum((a,-a)\,\mathrm{Subnomial}\,n)$ is zero.

Let n be a natural number. Let us observe that $\sum((1,1)\,\mathrm{Subnomial}(n+1-1))$ reduces to $n+1$.

One can verify that $\sum\langle\binom{n}{0},\ldots,\binom{n}{n}\rangle$ is non zero.

Let a, b be non negative real numbers. Observe that $(a,b)\,\mathrm{Subnomial}\,n$ is non-negative yielding and $\langle\binom{n}{0}a^0b^n,\ldots,\binom{n}{n}a^nb^0\rangle$ is non-negative yielding and $\sum((a,b)\,\mathrm{Subnomial}\,n)$ is non negative and $\sum\langle\binom{n}{0}a^0b^n,\ldots,\binom{n}{n}a^nb^0\rangle$ is non negative.

Let us consider real numbers a, b. Now we state the propositions:

(67) $(a,b)\,\mathrm{Subnomial}\,n$ and $(b,a)\,\mathrm{Subnomial}\,n$ are fiberwise equipotent. The theorem is a consequence of (11) and (64).

(68) $\prod((a,b)\,\mathrm{Subnomial}\,n) = \prod((b,a)\,\mathrm{Subnomial}\,n)$.

(69) Let us consider a non negative real number a.

Then $\prod((a,1)\,\mathrm{Subnomial}\,n) = a^{\binom{n+1}{2}}$. The theorem is a consequence of (62), (55), (63), and (67).

(70) $n!\cdot k! \leqslant (n+k)!$.

(71) $\binom{n+k}{k} = 1$ if and only if $n=0$ or $k=0$.

Proof: If $n \neq 0$ and $k \neq 0$, then $\binom{n+k}{k} \neq 1$ by [1, (14)], [10, (22)]. □

(72) $n!\cdot k! = (n+k)!$ if and only if $n=0$ or $k=0$. The theorem is a consequence of (71).

Let n, k be non zero natural numbers. One can check that $(n+k)! - n!\cdot k!$ is positive. Now we state the propositions:

(73) Let us consider a real number a. Then $\sum((a,a)\,\mathrm{Subnomial}\,n) = \sum((1,1)\,\mathrm{Subnomial}\,n)\cdot\sum\langle\binom{n}{0}a^0 0^n,\ldots,\binom{n}{n}a^n 0^0\rangle$. The theorem is a consequence of (65).

(74) Let us consider real numbers a, b, c. Then $\sum\langle\binom{n}{0}a+b^0c^n,\ldots,\binom{n}{n}a+b^nc^0\rangle = \sum\langle\binom{n}{0}a^0b+c^n,\ldots,\binom{n}{n}a^nb+c^0\rangle$.

(75) $\langle\binom{n}{0},\ldots,\binom{n}{n}\rangle(i+1) = \binom{n}{i}$.

(76) $\binom{2\cdot n}{n} = \frac{(2\cdot n)!}{n!^2}$.

(77) $\langle\binom{2\cdot n+1}{0},\ldots,\binom{2\cdot n+1}{2\cdot n+1}\rangle(n+1) = \langle\binom{2\cdot n+1}{0},\ldots,\binom{2\cdot n+1}{2\cdot n+1}\rangle(n+2)$. The theorem is a consequence of (75).

(78) Let us consider a non zero integer a.
If $1 \leqslant k \leqslant n$, then $a \mid ((a,b)\,\mathrm{Subnomial}\,n)(k)$.

(79) Let us consider integers a, b. Then $a \cdot b \mid \langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle(i) - ((a,b)\,\mathrm{Subnomial}\,n)(i)$. The theorem is a consequence of (45).

(80) Let us consider a $\mathbb{Z}$-valued finite sequence f, and an integer a. Suppose for every natural number n such that $n \in \mathrm{dom}\, f$ holds $a \mid f(n)$. Then $a \mid \sum f$.
PROOF: Reconsider $f_1 = f$ as a finite sequence of elements of $\mathbb{R}$. Reconsider $k = \min f_1$ as an integer. Reconsider $f_2 = f$ as a finite sequence of elements of $\mathbb{C}$. Reconsider $g = f_2 - k$ as a finite sequence of elements of $\mathbb{Z}$. Reconsider $l = |a|$ as a natural number. $a \mid k$ by [11, (12)]. If $m \in \mathrm{dom}\, g$, then $l \mid g(m)$ by [11, (10)], [9, (4), (13)]. $\sum(g+k) = \sum g + k \cdot \mathrm{len}\, g$. $\square$

(81) Let us consider integers a, b. Then $a \cdot b \cdot (a-b) \mid (a-b) \cdot (a+b)^n - (a^{n+1} - b^{n+1})$. The theorem is a consequence of (79), (80), and (51).

Let us consider non negative real numbers a, b.

(82) $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle(i) \geqslant ((a,b)\,\mathrm{Subnomial}\,n)(i)$. The theorem is a consequence of (47) and (57).

(83) $(a+b)^n \geqslant \sum((a,b)\,\mathrm{Subnomial}\,n)$. The theorem is a consequence of (82) and (32).

Let us consider non negative real numbers a, b and a non zero natural number n. Now we state the propositions:

(84) $a^n + b^n \leqslant \sum((a,b)\,\mathrm{Subnomial}\,n)$. The theorem is a consequence of (48).

(85) $a \cdot (a + 2 \cdot b)^n + b^{n+1} \geqslant (a+b)^{n+1}$.

(86) $a \cdot (a+b)^n + (a+b) \cdot b^n \leqslant (a+b)^{n+1}$.

Let us consider positive real numbers a, b and a non zero natural number n. Now we state the propositions:

(87) $\sum((a,b)\,\mathrm{Subnomial}(n+1)) < \sum\langle \binom{n+1}{0} a^0 b^{n+1}, \ldots, \binom{n+1}{n+1} a^{n+1} b^0 \rangle$. The theorem is a consequence of (82), (57), and (39).

(88) $\sum((a+b,0)\,\mathrm{Subnomial}(n+1)) > \sum((a,b)\,\mathrm{Subnomial}(n+1))$. The theorem is a consequence of (51) and (87).

(89) Let us consider real numbers a, b, and natural numbers n, i. Then $((a,b)\,\mathrm{Subnomial}\,n)(i) \leqslant ((|a|,|b|)\,\mathrm{Subnomial}\,n)(i)$. The theorem is a consequence of (45).

(90) Let us consider a real number a, a natural number n, and an odd natural number i. Then $((a,-a)\,\mathrm{Subnomial}(n+i))(i) = a^{n+i}$. The theorem is a consequence of (54) and (60).

(91) Let us consider a real number a, a natural number n, and a non zero natural number i. Then $((a,-a)\,\mathrm{Subnomial}(n+2 \cdot i))(2 \cdot i) = -a^{n+2 \cdot i}$. The

theorem is a consequence of (54) and (60).

Let us consider real numbers a, b and a natural number n. Now we state the propositions:

(92) $(a,b)\,\mathrm{Subnomial}(n+1) = \langle a^{n+1}\rangle \frown (b \cdot ((a,b)\,\mathrm{Subnomial}\,n))$.

Proof: $\mathrm{dom}((a,b)\,\mathrm{Subnomial}(n+1)) = \mathrm{dom}(\langle a^{n+1}\rangle \frown (b\cdot((a,b)\,\mathrm{Subnomial}\,n)))$ by [13, (29)], [2, (22)]. For every object i such that $i \in \mathrm{dom}((a,b)\,\mathrm{Subnomial}(n+1))$ holds $((a,b)\,\mathrm{Subnomial}(n+1))(i) = (\langle a^{n+1}\rangle \frown (b\cdot((a,b)\,\mathrm{Subnomial}\,n)))(i)$ by [13, (25)], [1, (10), (13)], [2, (65)]. □

(93) $(a,b)\,\mathrm{Subnomial}(n+2) = (\langle a^{n+2}\rangle \frown (a \cdot b \cdot ((a,b)\,\mathrm{Subnomial}\,n))) \frown \langle b^{n+2}\rangle$.

The theorem is a consequence of (92), (44), (64), (43), and (42).

Acknowledgement: Ad Maiorem Dei Gloriam

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

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

[3] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(**2**):241–245, 1996.

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

[5] Wenpai Chang, Hiroshi Yamazaki, and Yatsuka Nakamura. The inner product and conjugate of finite sequences of complex numbers. *Formalized Mathematics*, 13(**3**):367–373, 2005.

[6] Jacek Gancarzewicz. *Arytmetyka*. Wydawnictwo UJ, Kraków, 2000. In Polish.

[7] Cao Hui-Qin and Pan Hao. Factors of alternating binomial sums. *Advances in Applied Mathematics*, 45(1):96–107, 2010. doi:http://dx.doi.org/10.1016/j.aam.2009.09.004.

[8] Sudesh K. Khanduja, Ramneek Khassa, and Shanta Laishram. Some irreducibility results for truncated binomial expansions. *Journal of Number Theory*, 131(2):300–308, 2011. doi:http://dx.doi.org/10.1016/j.jnt.2010.08.004.

[9] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**): 573–577, 1997.

[10] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[11] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[12] W.W. Sawyer. *The Search for Pattern*. Penguin Books Ltd, Harmondsworth, Middlessex, England, 1970.

[13] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

Received October 18, 2016

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 24, No. 4, Pages 275–280, 2016
DOI: 10.1515/forma-2016-0023

DE GRUYTER OPEN
degruyter.com/view/j/forma

Leibniz Series for π[1]

Karol Pąk
Institute of Informatics
University of Białystok
Ciołkowskiego 1M, 15-245 Białystok
Poland

Summary. In this article we prove the Leibniz series for π which states that

$$\frac{\pi}{4} = \sum_{n=0}^{\infty} \frac{(-1)^n}{2 \cdot n + 1}.$$

The formalization follows K. Knopp [8], [1] and [6]. *Leibniz's Series for Pi* is item `#26` from the "Formalizing 100 Theorems" list maintained by Freek Wiedijk at `http://www.cs.ru.nl/F.Wiedijk/100/` .

MSC: 40G99 03B35

Keywords: π approximation; Leibniz theorem; Leibniz series

MML identifier: `LEIBNIZ1`, version: `8.1.05 5.39.1282`

1. Preliminaries

From now on i, n, m denote natural numbers, r, s denote real numbers, and A denotes a non empty, closed interval subset of $\mathbb{R}$.

Now we state the proposition:

(1) $\operatorname{rng}((\text{the function tan}){\restriction}]-\frac{\pi}{2}, \frac{\pi}{2}[) = \mathbb{R}$.

Proof: Set $P = \frac{\pi}{2}$. Set $I =]-P, P[$. $\mathbb{R} \subseteq \operatorname{rng}((\text{the function tan}){\restriction}I)$ by [4, (50)], [20, (30)], [14, (15)], [16, (1)]. □

[1]This work has been financed by the resources of the Polish National Science Centre granted by decision no. DEC-2012/07/N/ST6/02147.

One can verify that the function arctan is total and the function arctan is differentiable.

Now we state the propositions:

(2) (The function arctan)$'(r) = \frac{1}{1+r^{\mathbf{2}}}$.

(3) Let us consider an open subset Z of $\mathbb{R}$. Then

(i) the function arctan is differentiable on Z, and

(ii) for every r such that $r \in Z$ holds (the function arctan)$'_{\restriction Z}(r) = \frac{1}{1+r^{\mathbf{2}}}$.

The theorem is a consequence of (2).

Let us consider n. One can verify that $\square^n$ is continuous.

Now we state the propositions:

(4) (i) $\mathrm{dom}(\frac{\square^n}{\square^0+\square^2}) = \mathbb{R}$, and

(ii) $\frac{\square^n}{\square^0+\square^2}$ is continuous, and

(iii) $(\frac{\square^n}{\square^0+\square^2})(r) = \frac{r^n}{1+r^{\mathbf{2}}}$.

(5) $\int\limits_A (\frac{\square^0}{\square^0+\square^2})(x)dx =$
(the function arctan)(sup A) − (the function arctan)(inf A).

Proof: Set $Z_0 = \square^0$. Set $Z_2 = \square^2$. Set $f = \frac{Z_0}{Z_0+Z_2}$. $\mathrm{dom}\, f = \mathbb{R}$. f is continuous. If $r \in \mathbb{R}$, then $f(r) = \frac{1}{1+r^{\mathbf{2}}}$ by [13, (4)], (4). For every element x of $\mathbb{R}$ such that $x \in \mathrm{dom}$(the function arctan)$'_{\restriction\mathbb{R}}$ holds (the function arctan)$'_{\restriction\mathbb{R}}(x) = f(x)$. $\square$

(6) $\int\limits_A ((-1)^i \cdot (\frac{\square^{2\cdot n}}{\square^0+\square^2}))(x)dx = (-1)^i \cdot ((\frac{1}{2\cdot n+1})\cdot(\sup A)^{2\cdot n+1} - (\frac{1}{2\cdot n+1})\cdot (\inf A)^{2\cdot n+1}) + \int\limits_A ((-1)^{i+1} \cdot (\frac{\square^{2\cdot(n+1)}}{\square^0+\square^2}))(x)dx.$

Proof: Set $I_1 = (-1)^i$. Set $i_1 = i+1$. Set $n_1 = n+1$. Set $I_2 = (-1)^{i_1}$. Set $Z_0 = \square^0$. Set $Z_2 = \square^2$. Set $Z_{2n} = \square^{2\cdot n}$. Set $f = I_1 \cdot Z_{2n}$. Set $g = I_2 \cdot (\frac{\square^{2\cdot n_1}}{Z_0+Z_2})$. $\mathrm{dom}\, g = \mathbb{R}$. For every element x of $\mathbb{R}$, $(I_1 \cdot (\frac{Z_{2n}}{Z_0+Z_2}))(x) = (f+g)(x)$ by [13, (6)], [17, (36)], (4). $f + g = I_1 \cdot (\frac{Z_{2n}}{Z_0+Z_2})$. $\frac{\square^{2\cdot n_1}}{Z_0+Z_2}$ is continuous. $\square$

(7) Suppose $A = [0, r]$ and $r \geqslant 0$. Then $|\int\limits_A (\frac{\square^{2\cdot n}}{\square^0+\square^2})(x)dx| \leqslant (\frac{1}{2\cdot n+1}) \cdot r^{2\cdot n+1}$.

Proof: Set $Z_0 = \square^0$. Set $Z_2 = \square^2$. Set $N = 2 \cdot n$. Set $Z_n = \square^N$. Set $f = \frac{Z_n}{Z_0+Z_2}$. f is continuous and $\mathrm{dom}\, f = \mathbb{R}$. Reconsider $f_1 = f \restriction A$ as a function from A into $\mathbb{R}$. Reconsider $Z_1 = Z_n \restriction A$ as a function from A into $\mathbb{R}$. For every r such that $r \in A$ holds $f_1(r) \leqslant Z_1(r)$ by [4, (49)], [17, (36)], [18, (3)], (4). For every object x such that $x \in \mathbb{R}$ holds $f(x) = |f|(x)$ by [13, (8)], (4). □

2. Euler Transformation

Let a be a sequence of real numbers. The alternating series of a yielding a sequence of real numbers is defined by

(Def. 1) $it(i) = (-1)^i \cdot a(i)$.

Now we state the proposition:

(8) Let us consider a sequence a of real numbers. Suppose a is non-negative yielding, non-increasing, and convergent and $\lim a = 0$. Then

(i) the alternating series of a is summable, and

(ii) for every n, $(\sum_{\alpha=0}^{\kappa}(\text{the alternating series of } a)(\alpha))_{\kappa\in\mathbb{N}}(2\cdot n) \geqslant \sum(\text{the alternating series of } a) \geqslant (\sum_{\alpha=0}^{\kappa}(\text{the alternating series of } a)(\alpha))_{\kappa\in\mathbb{N}}(2\cdot n+1)$.

PROOF: Set $A =$ the alternating series of a. Set $P = (\sum_{\alpha=0}^{\kappa} A(\alpha))_{\kappa\in\mathbb{N}}$. Define $\mathcal{T}[\text{natural number}, \text{object}] \equiv \$_2 = P(2 \cdot \$_1)$. Define $\mathcal{S}[\text{natural number}, \text{object}] \equiv \$_2 = P(2 \cdot \$_1 + 1)$. Consider T being a function from $\mathbb{N}$ into $\mathbb{R}$ such that for every element x of $\mathbb{N}$, $\mathcal{T}[x, T(x)]$ from [5, Sch. 3].
Consider S being a function from $\mathbb{N}$ into $\mathbb{R}$ such that for every element x of $\mathbb{N}$, $\mathcal{S}[x, S(x)]$ from [5, Sch. 3]. For every natural number n, $S(n) \leqslant S(n+1)$. For every natural number n, $T(n) \geqslant T(n+1)$. For every natural number n, $T(n) \geqslant S(n)$. For every natural number n, $T(n) > S(0) - 1$ by [10, (6)]. For every natural number n, $S(n) < T(0) + 1$ by [10, (8)].
Define $\mathcal{D}(\text{natural number}) = 2 \cdot \$_1 + 1$. Consider D being a function from $\mathbb{N}$ into $\mathbb{N}$ such that for every element x of $\mathbb{N}$, $D(x) = \mathcal{D}(x)$ from [5, Sch. 8]. Reconsider $D_1 = D$ as a many sorted set indexed by $\mathbb{N}$. For every natural number n, $D(n) < D(n+1)$ by [2, (13)]. Reconsider $a_2 = a \cdot D_1$ as a sequence of real numbers.
For every object x such that $x \in \mathbb{N}$ holds $a_2(x) = (T - S)(x)$ by [4, (12)]. For every real number p such that $0 < p$ there exists a natural number n such that for every natural number m such that $n \leqslant m$ holds $|P(m) - \lim T| < p$ by [19, (9)]. □

3. Main Theorem

Let us consider r. The Leibniz series of r yielding a sequence of real numbers is defined by

(Def. 2) $it(n) = \frac{(-1)^n \cdot r^{2 \cdot n+1}}{2 \cdot n+1}$.

The Leibniz series yielding a sequence of real numbers is defined by the term

(Def. 3) the Leibniz series of 1.

Now we state the propositions:

(9) Suppose $r \in [-1, 1]$. Then

(i) |the Leibniz series of r| is non-negative yielding, non-increasing, and convergent, and

(ii) lim|the Leibniz series of r| $= 0$.

Proof: Set $r_1 =$ the Leibniz series of r. Set $A = |r_1|$. $A(n) = \frac{|r|^{2 \cdot n+1}}{2 \cdot n+1}$ by [15, (1)], [3, (67), (65)]. $A(n) \geqslant A(n+1)$ by [3, (46)], [15, (1)], [13, (6)], [2, (13)]. Set $C = \{0\}_{n \in \mathbb{N}}$. Define $\mathcal{F}(\text{natural number}) = \frac{\frac{1}{2}}{\$_1 + \frac{1}{2}}$. Consider f being a sequence of real numbers such that $f(n) = \mathcal{F}(n)$ from [11, Sch. 1]. $C(n) \leqslant A(n) \leqslant f(n)$ by [11, (57)], [3, (46)], [13, (11)], [2, (11)]. $\square$

(10) (i) if $r \geqslant 0$, then the alternating series of |the Leibniz series of r| $=$ the Leibniz series of r, and

(ii) if $r < 0$, then $(-1) \cdot$ (the alternating series of |the Leibniz series of r|) $=$ the Leibniz series of r.

Proof: Set $r_1 =$ the Leibniz series of r. Set $A = |r_1|$. Set $a_1 =$ the alternating series of A. $a_1(n) = (-1)^n \cdot (\frac{|r|^{2 \cdot n+1}}{2 \cdot n+1})$ by [15, (1)], [3, (67), (65)]. If $r \geqslant 0$, then $a_1 = r_1$. $\square$

(11) If $r \in [-1, 1]$, then the Leibniz series of r is summable. The theorem is a consequence of (9), (8), and (10).

(12) Suppose $A = [0, r]$ and $r \geqslant 0$. Then (the function arctan)$(r) = (\sum_{\alpha=0}^{\kappa}(\text{the Leibniz series of } r)(\alpha))_{\kappa \in \mathbb{N}}(n) + \int_A ((-1)^{n+1} \cdot (\frac{\square^{2 \cdot (n+1)}}{\square^0 + \square^2}))(x)dx$.

Proof: Set $Z_0 = \square^0$. Set $Z_2 = \square^2$. Set $r_1 =$ the Leibniz series of r. Define $\mathcal{P}[\text{natural number}] \equiv$ (the function arctan)$(r) = (\sum_{\alpha=0}^{\kappa} r_1(\alpha))_{\kappa \in \mathbb{N}}(\$_1) + \int_A ((-1)^{\$_1+1} \cdot (\frac{\square^{2 \cdot (\$_1+1)}}{Z_0 + Z_2}))(x)dx$. $\mathcal{P}[0]$ by (5), [14, (43)], [13, (4)], [9, (21)]. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$ by [13, (11)], [2, (11)], (6). $\mathcal{P}[i]$ from [2, Sch. 2]. $\square$

(13) If $0 \leqslant r \leqslant 1$, then (the function arctan)$(r) = \sum$(the Leibniz series of r).

PROOF: Set r_1 = the Leibniz series of r. Set $P = (\sum_{\alpha=0}^{\kappa} r_1(\alpha))_{\kappa \in \mathbb{N}}$. Set A = (the function arctan)(r). Define $\mathcal{I}$(natural number) $= \frac{\square^{2 \cdot \$_1}}{\square^0 + \square^2}$. P is convergent. For every s such that $0 < s$ there exists n such that for every m such that $n \leqslant m$ holds $|P(m) - A| < s$ by [12, (3)], (4), [7, (11), (10)]. □

(14) LEIBNIZ SERIES FOR π:
$\frac{\pi}{4} = \sum$(the Leibniz series).

(15) $(\sum_{\alpha=0}^{\kappa}$(the Leibniz series)$(\alpha))_{\kappa \in \mathbb{N}}(2 \cdot n + 1) \leqslant \sum$(the Leibniz series) $\leqslant$ $(\sum_{\alpha=0}^{\kappa}$(the Leibniz series)$(\alpha))_{\kappa \in \mathbb{N}}(2 \cdot n)$. The theorem is a consequence of (9), (10), and (8).

(16) (i) $(\sum_{\alpha=0}^{\kappa}$(the Leibniz series)$(\alpha))_{\kappa \in \mathbb{N}}(1) = \frac{2}{3}$, and

(ii) if n is odd, then $(\sum_{\alpha=0}^{\kappa}$(the Leibniz series)$(\alpha))_{\kappa \in \mathbb{N}}(n+2) = (\sum_{\alpha=0}^{\kappa}$(the Leibniz series)$(\alpha))_{\kappa \in \mathbb{N}}(n) + \frac{2}{4 \cdot n^{\mathbf{2}} + 16 \cdot n + 15}$.

(17) π APPROXIMATION:
$\frac{313}{100} < \pi < \frac{315}{100}$. The theorem is a consequence of (16), (14), and (15).

REFERENCES

[1] George E. Andrews, Richard Askey, and Ranjan Roy. *Special Functions*. Cambridge University Press, 1999.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

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

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

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

[6] Lokenath Debnath. *The Legacy of Leonhard Euler: A Tricentennial Tribute*. World Scientific, 2010.

[7] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definition of integrability for partial functions from $\mathbb{R}$ to $\mathbb{R}$ and integrability for continuous functions. *Formalized Mathematics*, 9(**2**):281–284, 2001.

[8] Konrad Knopp. *Infinite Sequences and Series*. Dover Publications, 1956. ISBN 978-0-486-60153-3.

[9] Jarosław Kotowicz. Partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 1(**4**):703–709, 1990.

[10] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1 (**3**):471–475, 1990.

[11] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[12] Jarosław Kotowicz. Convergent real sequences. Upper and lower bound of sets of real numbers. *Formalized Mathematics*, 1(**3**):477–481, 1990.

[13] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[14] Xiquan Liang and Bing Xie. Inverse trigonometric functions arctan and arccot. *Formalized Mathematics*, 16(**2**):147–158, 2008. doi:10.2478/v10037-008-0021-3.

[15] Akira Nishino and Yasunari Shidama. The Maclaurin expansions. *Formalized Mathematics*, 13(**3**):421–425, 2005.

[16] Chanapat Pacharapokin, Kanchun, and Hiroshi Yamazaki. Formulas and identities of trigonometric functions. *Formalized Mathematics*, 12(**2**):139–141, 2004.

[17] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

[18] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.

[19] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[20] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

Received October 18, 2016

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 24, No. 4, Pages 281–290, 2016
DOI: 10.1515/forma-2016-0024

DE GRUYTER OPEN
degruyter.com/view/j/forma

The Axiomatization of Propositional Logic[1]

Mariusz Giero
Faculty of Economics and Informatics
University of Białystok
Kalvariju 135, LT-08221 Vilnius
Lithuania

Summary. This article introduces propositional logic as a formal system ([14], [10], [11]). The formulae of the language are as follows $\phi ::= \bot \mid p \mid \phi \to \phi$. Other connectives are introduced as abbrevations. The notions of model and satisfaction in model are defined. The axioms are all the formulae of the following schemes

- $\alpha \Rightarrow (\beta \Rightarrow \alpha)$,
- $(\alpha \Rightarrow (\beta \Rightarrow \gamma)) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma))$,
- $(\neg\beta \Rightarrow \neg\alpha) \Rightarrow ((\neg\beta \Rightarrow \alpha) \Rightarrow \beta)$.

Modus ponens is the only derivation rule. The soundness theorem and the strong completeness theorem are proved. The proof of the completeness theorem is carried out by a counter-model existence method. In order to prove the completeness theorem, Lindenbaum's Lemma is proved. Some most widely used tautologies are presented.

MSC: 03B05 03B35

Keywords: completeness; formal system; Lindenbaum's lemma

MML identifier: PL_AXIOM, version: 8.1.05 5.39.1282

[1]This work was supported by the University of Bialystok grants: BST447 *Formalization of temporal logics in a proof-assistant. Application to System Verification*, and BST225 *Database of mathematical texts checked by computer.*

ISSN 1426–2630(Print), 1898-9934(Online)

1. Preliminaries

Now we state the propositions:

(1) Let us consider functions f, g. Suppose $\mathrm{dom}\, f \subseteq \mathrm{dom}\, g$ and for every set x such that $x \in \mathrm{dom}\, f$ holds $f(x) = g(x)$. Then $\mathrm{rng}\, f \subseteq \mathrm{rng}\, g$.

(2) Let us consider Boolean objects p, q. Then $p \wedge q \Rightarrow p = \mathit{true}$.

(3) Let us consider a Boolean object p. Then $\neg\neg p \Leftrightarrow p = \mathit{true}$.

Let us consider Boolean objects p, q. Now we state the propositions:

(4) $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q = \mathit{true}$.

(5) $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q = \mathit{true}$.

(6) $p \Rightarrow q \Rightarrow (\neg q \Rightarrow \neg p) = \mathit{true}$.

Let us consider Boolean objects p, q, r. Now we state the propositions:

(7) $p \Rightarrow q \Rightarrow (p \Rightarrow r \Rightarrow (p \Rightarrow q \wedge r)) = \mathit{true}$.

(8) $p \Rightarrow r \Rightarrow (q \Rightarrow r \Rightarrow (p \vee q \Rightarrow r)) = \mathit{true}$.

Let us consider Boolean objects p, q. Now we state the propositions:

(9) $p \wedge q \Leftrightarrow q \wedge p = \mathit{true}$.

(10) $p \vee q \Leftrightarrow q \vee p = \mathit{true}$.

Let us consider Boolean objects p, q, r. Now we state the propositions:

(11) $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r) = \mathit{true}$.

(12) $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r) = \mathit{true}$.

(13) Let us consider Boolean objects p, q. Then $\neg q \Rightarrow \neg p \Rightarrow (\neg q \Rightarrow p \Rightarrow q) = \mathit{true}$.

Let us consider Boolean objects p, q, r. Now we state the propositions:

(14) $p \wedge (q \vee r) \Leftrightarrow p \wedge q \vee p \wedge r = \mathit{true}$.

(15) $p \vee q \wedge r \Leftrightarrow (p \vee q) \wedge (p \vee r) = \mathit{true}$.

(16) Let us consider a finite set X, and a set Y. Suppose Y is $\subseteq$-linear and $X \subseteq \bigcup Y$ and $Y \neq \emptyset$. Then there exists a set Z such that

  (i) $X \subseteq Z$, and

  (ii) $Z \in Y$.

2. The Syntax

Let D be a set. We say that D has propositional variables if and only if

(Def. 1) for every element n of $\mathbb{N}$, $\langle 3 + n \rangle \in D$.

We say that D is PL-closed if and only if

(Def. 2) $D \subseteq \mathbb{N}^*$ and D has FALSUM, implication and propositional variables.

Let us note that every set which is PL-closed is also non empty and has also FALSUM, implication, and propositional variables and every subset of $\mathbb{N}^*$ which has FALSUM, implication, and propositional variables is also PL-closed.

The functor PL-WFF yielding a set is defined by

(Def. 3) *it* is PL-closed and for every set D such that D is PL-closed holds $it \subseteq D$.

Observe that PL-WFF is PL-closed and there exists a set which is PL-closed and non empty and PL-WFF is functional and every element of PL-WFF is finite sequence-like.

The functor $\bot_{\mathrm{PL}}$ yielding an element of PL-WFF is defined by the term

(Def. 4) $\langle 0 \rangle$.

Let p, q be elements of PL-WFF. The functor $p \Rightarrow q$ yielding an element of PL-WFF is defined by the term

(Def. 5) $(\langle 1 \rangle \frown p) \frown q$.

Let n be an element of $\mathbb{N}$. The functor $\mathrm{Prop}\, n$ yielding an element of PL-WFF is defined by the term

(Def. 6) $\langle 3 + n \rangle$.

The functor AP yielding a subset of PL-WFF is defined by

(Def. 7) for every set x, $x \in it$ iff there exists an element n of $\mathbb{N}$ such that $x = \mathrm{Prop}\, n$.

From now on p, q, r, s, A, B denote elements of PL-WFF, F, G, H denote subsets of PL-WFF, k, n denote elements of $\mathbb{N}$, and f, f_1, f_2 denote finite sequences of elements of PL-WFF.

Let D be a subset of PL-WFF. Observe that D has implication if and only if the condition (Def. 8) is satisfied.

(Def. 8) for every p and q such that $p, q \in D$ holds $p \Rightarrow q \in D$.

The scheme *PLInd* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 1) For every r, $\mathcal{P}[r]$

provided

- $\mathcal{P}[\bot_{\mathrm{PL}}]$ and
- for every n, $\mathcal{P}[\mathrm{Prop}\, n]$ and
- for every r and s such that $\mathcal{P}[r]$ and $\mathcal{P}[s]$ holds $\mathcal{P}[r \Rightarrow s]$.

Now we state the proposition:

(17) PL-WFF $\subseteq$ HP-WFF.

Proof: Define $\mathcal{P}[\text{element of PL-WFF}] \equiv \$_1 \in \text{HP-WFF}$. For every n, $\mathcal{P}[\mathrm{Prop}\, n]$. For every r and s such that $\mathcal{P}[r]$ and $\mathcal{P}[s]$ holds $\mathcal{P}[r \Rightarrow s]$. For every A, $\mathcal{P}[A]$ from *PLInd*. □

Let us consider p. The functor $\neg p$ yielding an element of PL-WFF is defined by the term

(Def. 9) $p \Rightarrow \bot_{\mathrm{PL}}$.

The functor $\top_{\mathrm{PL}}$ yielding an element of PL-WFF is defined by the term

(Def. 10) $\neg \bot_{\mathrm{PL}}$.

Let us consider p and q. The functors: $p \wedge q$ and $p \vee q$ yielding elements of PL-WFF are defined by terms

(Def. 11) $\neg(p \Rightarrow \neg q)$,

(Def. 12) $\neg p \Rightarrow q$,

respectively. The functor $p \Leftrightarrow q$ yielding an element of PL-WFF is defined by the term

(Def. 13) $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

3. The Semantics

A PL-model is a subset of AP. From now on M denotes a PL-model.

Let M be a PL-model. The functor SAT_M yielding a function from PL-WFF into *Boolean* is defined by

(Def. 14) $it(\bot_{\mathrm{PL}}) = 0$ and for every k, $it(\mathrm{Prop}\,k) = 1$ iff $\mathrm{Prop}\,k \in M$ and for every p and q, $it(p \Rightarrow q) = it(p) \Rightarrow it(q)$.

Now we state the propositions:

(18) $\mathrm{SAT}_M(A \Rightarrow B) = 1$ if and only if $\mathrm{SAT}_M(A) = 0$ or $\mathrm{SAT}_M(B) = 1$.

(19) $\mathrm{SAT}_M(\neg p) = \neg(\mathrm{SAT}_M(p))$.

(20) $\mathrm{SAT}_M(\neg A) = 1$ if and only if $\mathrm{SAT}_M(A) = 0$. The theorem is a consequence of (19).

(21) $\mathrm{SAT}_M(A \wedge B) = \mathrm{SAT}_M(A) \wedge \mathrm{SAT}_M(B)$. The theorem is a consequence of (19).

(22) $\mathrm{SAT}_M(A \wedge B) = 1$ if and only if $\mathrm{SAT}_M(A) = 1$ and $\mathrm{SAT}_M(B) = 1$. The theorem is a consequence of (21).

(23) $\mathrm{SAT}_M(A \vee B) = \mathrm{SAT}_M(A) \vee \mathrm{SAT}_M(B)$. The theorem is a consequence of (19).

(24) $\mathrm{SAT}_M(A \vee B) = 1$ if and only if $\mathrm{SAT}_M(A) = 1$ or $\mathrm{SAT}_M(B) = 1$. The theorem is a consequence of (23).

(25) $\mathrm{SAT}_M(A \Leftrightarrow B) = \mathrm{SAT}_M(A) \Leftrightarrow \mathrm{SAT}_M(B)$. The theorem is a consequence of (21).

(26) $\mathrm{SAT}_M(A \Leftrightarrow B) = 1$ if and only if $\mathrm{SAT}_M(A) = \mathrm{SAT}_M(B)$. The theorem is a consequence of (25).

Let us consider M and p. We say that $M \models p$ if and only if

(Def. 15) $\mathrm{SAT}_M(p) = 1$.

Let us consider F. We say that $M \models F$ if and only if

(Def. 16) for every p such that $p \in F$ holds $M \models p$.

Let us consider p. We say that $F \models p$ if and only if

(Def. 17) for every M such that $M \models F$ holds $M \models p$.

Let us consider A. We say that A is a tautology if and only if

(Def. 18) for every M, $\mathrm{SAT}_M(A) = 1$.

Now we state the propositions:

(27) A is a tautology if and only if $\emptyset_{\text{PL-WFF}} \models A$.

(28) $p \Rightarrow (q \Rightarrow p)$ is a tautology.

(29) $p \Rightarrow (q \Rightarrow r) \Rightarrow (p \Rightarrow q \Rightarrow (p \Rightarrow r))$ is a tautology.

(30) $\neg q \Rightarrow \neg p \Rightarrow (\neg q \Rightarrow p \Rightarrow q)$ is a tautology. The theorem is a consequence of (19) and (13).

(31) $p \Rightarrow q \Rightarrow (\neg q \Rightarrow \neg p)$ is a tautology. The theorem is a consequence of (19) and (6).

(32) $p \wedge q \Rightarrow p$ is a tautology. The theorem is a consequence of (21) and (2).

(33) $p \wedge q \Rightarrow q$ is a tautology. The theorem is a consequence of (21) and (2).

(34) $p \Rightarrow p \vee q$ is a tautology. The theorem is a consequence of (23).

(35) $q \Rightarrow p \vee q$ is a tautology. The theorem is a consequence of (23).

(36) $p \wedge q \Leftrightarrow q \wedge p$ is a tautology. The theorem is a consequence of (25), (21), and (9).

(37) $p \vee q \Leftrightarrow q \vee p$ is a tautology. The theorem is a consequence of (25), (23), and (10).

(38) $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$ is a tautology. The theorem is a consequence of (25), (21), and (11).

(39) $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$ is a tautology. The theorem is a consequence of (25), (23), and (12).

(40) $p \wedge (q \vee r) \Leftrightarrow p \wedge q \vee p \wedge r$ is a tautology. The theorem is a consequence of (25), (21), (23), and (14).

(41) $p \vee q \wedge r \Leftrightarrow (p \vee q) \wedge (p \vee r)$ is a tautology. The theorem is a consequence of (25), (23), (21), and (15).

(42) $\neg\neg p \Leftrightarrow p$ is a tautology. The theorem is a consequence of (25), (19), and (3).

(43) $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ is a tautology. The theorem is a consequence of (25), (19), (21), (23), and (4).

(44) $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ is a tautology. The theorem is a consequence of (25), (19), (23), (21), and (5).

(45) $p \Rightarrow q \Rightarrow (p \Rightarrow r \Rightarrow (p \Rightarrow q \wedge r))$ is a tautology. The theorem is a consequence of (21) and (7).

(46) $p \Rightarrow r \Rightarrow (q \Rightarrow r \Rightarrow (p \vee q \Rightarrow r))$ is a tautology. The theorem is a consequence of (23) and (8).

(47) If $F \models A$ and $F \models A \Rightarrow B$, then $F \models B$.

4. The Axioms. Derivability.

Let D be a set. We say that D is with axioms of PL if and only if

(Def. 19) for every p, q, and r holds $p \Rightarrow (q \Rightarrow p)$, $p \Rightarrow (q \Rightarrow r) \Rightarrow (p \Rightarrow q \Rightarrow (p \Rightarrow r))$, $\neg q \Rightarrow \neg p \Rightarrow (\neg q \Rightarrow p \Rightarrow q) \in D$.

The functor PL-axioms yielding a subset of PL-WFF is defined by

(Def. 20) *it* is with axioms of PL and for every subset D of PL-WFF such that D is with axioms of PL holds $it \subseteq D$.

One can check that PL-axioms is with axioms of PL.

Let us consider p, q, and r. We say that $\mathrm{MP}(p, q, r)$ if and only if

(Def. 21) $q = p \Rightarrow r$.

Observe that PL-axioms is non empty.

Let us consider A. We say that A is the simplification axiom if and only if

(Def. 22) there exists p and there exists q such that $A = p \Rightarrow (q \Rightarrow p)$.

We say that A is Frege axiom if and only if

(Def. 23) there exists p and there exists q and there exists r such that $A = p \Rightarrow (q \Rightarrow r) \Rightarrow (p \Rightarrow q \Rightarrow (p \Rightarrow r))$.

We say that A is the explosion axiom if and only if

(Def. 24) there exists p and there exists q such that $A = \neg q \Rightarrow \neg p \Rightarrow (\neg q \Rightarrow p \Rightarrow q)$.

Now we state the propositions:

(48) Every element of PL-axioms is the simplification axiom or Frege axiom or the explosion axiom.

(49) If A is the simplification axiom or Frege axiom or the explosion axiom, then $F \models A$. The theorem is a consequence of (28), (29), and (30).

Let i be a natural number. Let us consider f and F. We say that $\mathrm{prc}(f, F, i)$ if and only if

(Def. 25) $f(i) \in$ PL-axioms or $f(i) \in F$ or there exist natural numbers j, k such that $1 \leqslant j < i$ and $1 \leqslant k < i$ and $\mathrm{MP}(f_j, f_k, f_i)$.

Let us consider p. We say that $F \vdash p$ if and only if

(Def. 26) there exists f such that $f(\operatorname{len} f) = p$ and $1 \leqslant \operatorname{len} f$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $\operatorname{prc}(f, F, i)$.

Now we state the propositions:

(50) Let us consider natural numbers i, n. Suppose $n + \operatorname{len} f \leqslant \operatorname{len} f_2$ and for every natural number k such that $1 \leqslant k \leqslant \operatorname{len} f$ holds $f(k) = f_2(k + n)$ and $1 \leqslant i \leqslant \operatorname{len} f$. If $\operatorname{prc}(f, F, i)$, then $\operatorname{prc}(f_2, F, i + n)$.

(51) Suppose $f_2 = f \frown f_1$ and $1 \leqslant \operatorname{len} f$ and $1 \leqslant \operatorname{len} f_1$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $\operatorname{prc}(f, F, i)$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f_1$ holds $\operatorname{prc}(f_1, F, i)$. Let us consider a natural number i. If $1 \leqslant i \leqslant \operatorname{len} f_2$, then $\operatorname{prc}(f_2, F, i)$. The theorem is a consequence of (50).

(52) Suppose $f = f_1 \frown \langle p \rangle$ and $1 \leqslant \operatorname{len} f_1$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f_1$ holds $\operatorname{prc}(f_1, F, i)$ and $\operatorname{prc}(f, F, \operatorname{len} f)$. Then

(i) for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $\operatorname{prc}(f, F, i)$, and

(ii) $F \vdash p$.

The theorem is a consequence of (50).

(53) If $p \in$ PL-axioms or $p \in F$, then $F \vdash p$.
Proof: Define $\mathcal{P}[\text{set}, \text{set}] \equiv \$_2 = p$. Consider f such that $\operatorname{dom} f = \operatorname{Seg} 1$ and for every natural number k such that $k \in \operatorname{Seg} 1$ holds $\mathcal{P}[k, f(k)]$ from [3, Sch. 5]. For every natural number j such that $1 \leqslant j \leqslant \operatorname{len} f$ holds $\operatorname{prc}(f, F, j)$. $\square$

(54) If $F \vdash p$ and $F \vdash p \Rightarrow q$, then $F \vdash q$.
Proof: Consider f such that $f(\operatorname{len} f) = p$ and $1 \leqslant \operatorname{len} f$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $\operatorname{prc}(f, F, i)$. Consider f_1 such that $f_1(\operatorname{len} f_1) = p \Rightarrow q$ and $1 \leqslant \operatorname{len} f_1$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f_1$ holds $\operatorname{prc}(f_1, F, i)$. Set $g = (f \frown f_1) \frown \langle q \rangle$. For every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f_1$ holds $g(\operatorname{len} f + i) = f_1(i)$ by [3, (22), (39)], [1, (12)], [3, (65), (64)]. For every natural number i such that $1 \leqslant i \leqslant \operatorname{len}(f \frown f_1)$ holds $\operatorname{prc}(f \frown f_1, F, i)$. $\square$

(55) If $F \subseteq G$, then if $F \vdash p$, then $G \vdash p$.
Proof: Consider f such that $f(\operatorname{len} f) = p$ and $1 \leqslant \operatorname{len} f$ and for every natural number k such that $1 \leqslant k \leqslant \operatorname{len} f$ holds $\operatorname{prc}(f, F, k)$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $1 \leqslant \$_1 \leqslant \operatorname{len} f$, then $G \vdash f_{\$_1}$. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 4]. $\square$

5. Soundness Theorem. Deduction Theorem.

Now we state the propositions:

(56) If $F \vdash A$, then $F \models A$.

Proof: Consider f such that $f(\operatorname{len} f) = A$ and $1 \leqslant \operatorname{len} f$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $\operatorname{prc}(f, F, i)$. Define $\mathcal{P}$[natural number] $\equiv$ if $1 \leqslant \$_1 \leqslant \operatorname{len} f$, then $F \models f_{\$_1}$. For every natural number i such that for every natural number j such that $j < i$ holds $\mathcal{P}[j]$ holds $\mathcal{P}[i]$ by [1, (14)], [9, (1)], (48), (49). For every natural number i, $\mathcal{P}[i]$ from [1, Sch. 4]. □

(57) $F \vdash A \Rightarrow A$. The theorem is a consequence of (53) and (54).

(58) Deduction theorem:

If $F \cup \{A\} \vdash B$, then $F \vdash A \Rightarrow B$.

Proof: Consider f such that $f(\operatorname{len} f) = B$ and $1 \leqslant \operatorname{len} f$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} f$ holds $\operatorname{prc}(f, F \cup \{A\}, i)$. Define $\mathcal{P}$[natural number] $\equiv$ if $1 \leqslant \$_1 \leqslant \operatorname{len} f$, then $F \vdash A \Rightarrow f_{\$_1}$. For every natural number i such that for every natural number j such that $j < i$ holds $\mathcal{P}[j]$ holds $\mathcal{P}[i]$ by [1, (14)], (53), [9, (1)], (54). For every natural number i, $\mathcal{P}[i]$ from [1, Sch. 4]. □

(59) If $F \vdash A \Rightarrow B$, then $F \cup \{A\} \vdash B$. The theorem is a consequence of (53), (55), and (54).

(60) $F \vdash \neg A \Rightarrow (A \Rightarrow B)$. The theorem is a consequence of (53), (54), and (58).

(61) $F \vdash \neg A \Rightarrow A \Rightarrow A$. The theorem is a consequence of (53), (57), and (54).

6. Strong Completeness Theorem

Let us consider F. We say that F is consistent if and only if

(Def. 27) there exists no p such that $F \vdash p$ and $F \vdash \neg p$.

Now we state the propositions:

(62) F is consistent if and only if there exists A such that $F \nvdash A$. The theorem is a consequence of (60) and (54).

(63) If $F \nvdash A$, then $F \cup \{\neg A\}$ is consistent. The theorem is a consequence of (58), (62), (61), and (54).

(64) $F \vdash A$ if and only if there exists G such that $G \subseteq F$ and G is finite and $G \vdash A$. The theorem is a consequence of (55).

(65) If F is not consistent, then there exists G such that G is finite and G is not consistent and $G \subseteq F$. The theorem is a consequence of (64) and (55).

Let us consider F. We say that F is maximal if and only if

(Def. 28) for every p holds $p \in F$ or $\neg p \in F$.

Now we state the propositions:

(66) If $F \subseteq G$ and F is not consistent, then G is not consistent. The theorem is a consequence of (55).

(67) If F is consistent and $F \cup \{A\}$ is not consistent, then $F \cup \{\neg A\}$ is consistent. The theorem is a consequence of (58), (62), (61), and (54).

In the sequel x, y denote sets. Now we state the propositions:

(68) LINDENBAUM'S LEMMA:
If F is consistent, then there exists G such that $F \subseteq G$ and G is consistent and maximal.
PROOF: Set L = PL-WFF. Consider R being a binary relation such that R well orders L. Reconsider $R_2 = R\,|^2\,L$ as a binary relation on L. Reconsider $R_1 = \langle L, R_2 \rangle$ as a non empty relational structure. Set c = the carrier of R_1. Define $\mathcal{H}[\text{object}, \text{object}, \text{object}] \equiv$ for every p for every partial function f from c to 2^L such that $\$_1 = p$ and $\$_2 = f$ holds if $(\bigcup \text{rng}(f$ **qua** (2^L)-valued binary relation$) \cup F) \cup \{p\}$ is consistent, then $\$_3 = (\bigcup \text{rng}\, f \cup F) \cup \{p\}$ and if $(\bigcup \text{rng}(f$ **qua** (2^L)-valued binary relation$) \cup F) \cup \{p\}$ is not consistent, then $\$_3 = \bigcup \text{rng}\, f \cup F$. For every objects x, y such that $x \in c$ and $y \in c \dot{\to} 2^L$ there exists an object z such that $z \in 2^L$ and $\mathcal{H}[x, y, z]$ by [8, (46)]. Consider h being a function from $c \times (c \dot{\to} 2^L)$ into 2^L such that for every objects x, y such that $x \in c$ and $y \in c \dot{\to} 2^L$ holds $\mathcal{H}[x, y, h(x, y)]$ from [5, Sch. 1]. Consider f being a function from c into 2^L such that f is recursively expressed by h. Reconsider $G = \bigcup \text{rng}(f$ **qua** (2^L)-valued binary relation) as a subset of PL-WFF. Set i_1 = the internal relation of R_1. For every A and B such that $\langle A, B \rangle \in R_2$ holds $f(A) \subseteq f(B)$ by [4, (1)], [2, (4), (29), (9)]. rng f is $\subseteq$-linear. Define $\mathcal{S}[\text{element of } R_1] \equiv f(\$_1)$ is consistent. For every element x of R_1 such that for every element y of R_1 such that $y \neq x$ and $\langle y, x \rangle \in i_1$ holds $\mathcal{S}[y]$ holds $\mathcal{S}[x]$ by [2, (9)], [7, (32)], [2, (1)], [15, (42)]. For every element A of R_1, $\mathcal{S}[A]$ from [12, Sch. 3]. $F \subseteq G$ by [6, (3)]. G is consistent by (65), (16), [15, (42)], (66). G is maximal by [6, (3)], (17), [13, (16)], (66). $\square$

(69) If F is maximal and consistent, then for every p, $F \vdash p$ iff $p \in F$. The theorem is a consequence of (53).

(70) If $F \models A$, then $F \vdash A$.
PROOF: Consider G such that $F \cup \{\neg A\} \subseteq G$ and G is consistent and G is maximal. Set $M = \{\text{Prop}\, n$, where n is an element of $\mathbb{N} : \text{Prop}\, n \in G\}$.

$M \subseteq AP$. Define $\mathcal{P}[\text{element of PL-WFF}] \equiv \$_1 \in G$ iff $M \models \$_1$. $\mathcal{P}[\bot_{\text{PL}}]$. For every n, $\mathcal{P}[\text{Prop}\, n]$. For every r and s such that $\mathcal{P}[r]$ and $\mathcal{P}[s]$ holds $\mathcal{P}[r \Rightarrow s]$. For every B, $\mathcal{P}[B]$ from *PLInd*. $M \not\models A$. $\square$

(71) A is a tautology if and only if $\emptyset_{\text{PL-WFF}} \vdash A$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Grzegorz Bancerek. The well ordering relations. *Formalized Mathematics*, 1(**1**):123–129, 1990.

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

[4] Leszek Borys. On paracompactness of metrizable spaces. *Formalized Mathematics*, 3(**1**): 81–84, 1992.

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

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

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

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

[9] Mariusz Giero. Propositional linear temporal logic with initial validity semantics. *Formalized Mathematics*, 23(**4**):379–386, 2015. doi:10.1515/forma-2015-0030.

[10] Witold Pogorzelski. *Dictionary of Formal Logic*. Wydawnictwo UwB, Bialystok, 1992.

[11] Witold Pogorzelski. *Notions and theorems of elementary formal logic*. Wydawnictwo UwB, Bialystok, 1994.

[12] Piotr Rudnicki and Andrzej Trybulec. On same equivalents of well-foundedness. *Formalized Mathematics*, 6(**3**):339–343, 1997.

[13] Andrzej Trybulec. Defining by structural induction in the positive propositional language. *Formalized Mathematics*, 8(**1**):133–137, 1999.

[14] Anita Wasilewska. *An Introduction to Classical and Non-Classical Logics*. SUNY Stony Brook, 2005.

[15] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received October 18, 2016

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 24, No. 4, Pages 291–299, 2016
DOI: 10.1515/forma-2016-0025

DE GRUYTER OPEN
degruyter.com/view/j/forma

Algebraic Numbers

Yasushige Watase
Suginami-ku Matsunoki 6
3-21 Tokyo, Japan

Summary. This article provides definitions and examples upon an integral element of unital commutative rings. An algebraic number is also treated as consequence of a concept of "integral". Definitions for an integral closure, an algebraic integer and a transcendental numbers [14], [1], [10] and [7] are included as well. As an application of an algebraic number, this article includes a formal proof of a ring extension of rational number field $\mathbb{Q}$ induced by substitution of an algebraic number to the polynomial ring of $\mathbb{Q}[x]$ turns to be a field.

MSC: 11R04 13B21 03B35

Keywords: algebraic number; integral dependency

MML identifier: ALGNUM_1, version: 8.1.05 5.39.1282

1. Preliminaries

From now on i, j denote natural numbers and A, B denote rings.

Now we state the propositions:

(1) Let us consider rings L_1, L_2, L_3. Suppose L_1 is a subring of L_2 and L_2 is a subring of L_3. Then L_1 is a subring of L_3.

(2) $\mathbb{F}_{\mathbb{Q}}$ is a subfield of $\mathbb{C}_{\mathrm{F}}$.

(3) $\mathbb{F}_{\mathbb{Q}}$ is a subring of $\mathbb{C}_{\mathrm{F}}$.

(4) $\mathbb{Z}^{\mathrm{R}}$ is a subring of $\mathbb{C}_{\mathrm{F}}$.

Let us consider elements x, y of B and elements x_1, y_1 of A. Now we state the propositions:

(5) If A is a subring of B and $x = x_1$ and $y = y_1$, then $x + y = x_1 + y_1$.

(6) If A is a subring of B and $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.

Let c be a complex. Observe that $c(\in \mathbb{C}_{\mathrm{F}})$ reduces to c.

ISSN 1426–2630(Print), 1898-9934(Online)

2. Extended Evaluation Function

Let A, B be rings, p be a polynomial over A, and x be an element of B. The functor $\mathrm{ExtEval}(p, x)$ yielding an element of B is defined by

(Def. 1) there exists a finite sequence F of elements of B such that $it = \sum F$ and $\mathrm{len}\, F = \mathrm{len}\, p$ and for every element n of $\mathbb{N}$ such that $n \in \mathrm{dom}\, F$ holds $F(n) = p(n -' 1)(\in B) \cdot \mathrm{power}_B(x, n -' 1)$.

Now we state the proposition:

(7) Let us consider an element n of $\mathbb{N}$, rings A, B, and an element z of A. Suppose A is a subring of B. Then $\mathrm{power}_B(z(\in B), n) = \mathrm{power}_A(z, n)(\in B)$. The theorem is a consequence of (6).

Let us consider elements x_1, x_2 of A. Now we state the propositions:

(8) If A is a subring of B, then $x_1(\in B) + x_2(\in B) = (x_1 + x_2)(\in B)$. The theorem is a consequence of (5).

(9) If A is a subring of B, then $x_1(\in B) \cdot x_2(\in B) = (x_1 \cdot x_2)(\in B)$. The theorem is a consequence of (6).

(10) Let us consider a finite sequence F of elements of A, and a finite sequence G of elements of B. If A is a subring of B and $F = G$, then $(\sum F)(\in B) = \sum G$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence F of elements of A for every finite sequence G of elements of B such that $\mathrm{len}\, F = \$_1$ and $F = G$ holds $(\sum F)(\in B) = \sum G$. $\mathcal{P}[0]$ by [13, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [4, (4)], [5, (3)], [4, (59)], [3, (11)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(11) Let us consider a natural number n, an element x of A, and a polynomial p over A. Suppose A is a subring of B. Then $p(n -' 1)(\in B) \cdot \mathrm{power}_B(x(\in B), n -' 1) = (p(n -' 1) \cdot \mathrm{power}_A(x, n -' 1))(\in B)$. The theorem is a consequence of (9) and (7).

(12) Let us consider an element x of A, and a polynomial p over A. Suppose A is a subring of B. Then $\mathrm{ExtEval}(p, x(\in B)) = (\mathrm{eval}(p, x))(\in B)$.

Proof: Consider F_1 being a finite sequence of elements of B such that $\mathrm{ExtEval}(p, x(\in B)) = \sum F_1$ and $\mathrm{len}\, F_1 = \mathrm{len}\, p$ and for every element n of $\mathbb{N}$ such that $n \in \mathrm{dom}\, F_1$ holds $F_1(n) = p(n -' 1)(\in B) \cdot \mathrm{power}_B(x(\in B), n -' 1)$. Consider F_2 being a finite sequence of elements of A such that $\mathrm{eval}(p, x) = \sum F_2$ and $\mathrm{len}\, F_2 = \mathrm{len}\, p$ and for every element n of $\mathbb{N}$ such that $n \in \mathrm{dom}\, F_2$ holds $F_2(n) = p(n -' 1) \cdot \mathrm{power}_A(x, n -' 1)$. $F_1 = F_2$ by [12, (29)], [5, (3)], (19). □

(13) Let us consider an element x of B. Then $\mathrm{ExtEval}(\mathbf{0}.\, A, x) = 0_B$.

(14) Let us consider non degenerated rings A, B, and an element x of B. If A is a subring of B, then $\mathrm{ExtEval}(\mathbf{1}.\, A, x) = 1_B$.

(15) Let us consider an element x of B, and polynomials p, q over A. Suppose A is a subring of B. Then $\mathrm{ExtEval}(p+q, x) = \mathrm{ExtEval}(p, x)+\mathrm{ExtEval}(q, x)$. The theorem is a consequence of (8).

(16) Let us consider polynomials p, q over A. Suppose A is a subring of B and $\mathrm{len}\, p > 0$ and $\mathrm{len}\, q > 0$. Let us consider an element x of B. Then $\mathrm{ExtEval}(\text{Leading-Monomial}\, p * \text{Leading-Monomial}\, q, x) = (p(\mathrm{len}\, p -' 1) \cdot q(\mathrm{len}\, q -' 1))(\in B) \cdot \mathrm{power}_B(x, \mathrm{len}\, p + \mathrm{len}\, q -' 2)$. The theorem is a consequence of (13).

(17) Let us consider a polynomial p over A, and an element x of B. Suppose A is a subring of B. Then $\mathrm{ExtEval}(\text{Leading-Monomial}\, p, x) = p(\mathrm{len}\, p -' 1)(\in B) \cdot \mathrm{power}_B(x, \mathrm{len}\, p -' 1)$. The theorem is a consequence of (13).

Let us consider a commutative ring B, polynomials p, q over A, and an element x of B. Now we state the propositions:

(18) Suppose A is a subring of B. Then $\mathrm{ExtEval}(\text{Leading-Monomial}\, p * \text{Leading-Monomial}\, q, x) = \mathrm{ExtEval}(\text{Leading-Monomial}\, p, x) \cdot \mathrm{ExtEval}(\text{Leading-Monomial}\, q, x)$. The theorem is a consequence of (16), (9), (17), and (13).

(19) Suppose A is a subring of B. Then $\mathrm{ExtEval}(\text{Leading-Monomial}\, p * q, x) = \mathrm{ExtEval}(\text{Leading-Monomial}\, p, x) \cdot \mathrm{ExtEval}(q, x)$.

PROOF: Set $p = \text{Leading-Monomial}\, p_1$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every polynomial q over A such that $\mathrm{len}\, q = \$_1$ holds $\mathrm{ExtEval}(p * q, x) = \mathrm{ExtEval}(p, x) \cdot \mathrm{ExtEval}(q, x)$. For every natural number k such that for every natural number n such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$ by [9, (16)], [8, (31)], (15), (18). For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 4]. □

(20) If A is a subring of B, then $\mathrm{ExtEval}(p*q, x) = \mathrm{ExtEval}(p, x)\cdot\mathrm{ExtEval}(q, x)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every polynomial p over A such that $\mathrm{len}\, p = \$_1$ holds $\mathrm{ExtEval}(p * q, x) = \mathrm{ExtEval}(p, x) \cdot \mathrm{ExtEval}(q, x)$. For every natural number k such that for every natural number n such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$ by [9, (16)], [8, (32)], (15), (19). For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 4]. □

(21) Let us consider an element x of B, and an element z_0 of A. Suppose A is a subring of B. Then $\mathrm{ExtEval}(\langle z_0 \rangle, x) = z_0(\in B)$. The theorem is a consequence of (13).

(22) Let us consider an element x of B, and elements z_0, z_1 of A. Suppose A is a subring of B. Then $\mathrm{ExtEval}(\langle z_0, z_1 \rangle, x) = z_0(\in B) + z_1(\in B) \cdot x$. The theorem is a consequence of (13).

3. Integral Element and Algebraic Numbers

Let A, B be rings and x be an element of B. We say that x is integral over A if and only if

(Def. 2) there exists a polynomial f over A such that $\mathrm{LC}\, f = 1_A$ and $\mathrm{ExtEval}(f, x) = 0_B$.

Now we state the proposition:

(23) Let us consider a non degenerated ring A, and an element a of A. If A is a subring of B, then $a(\in B)$ is integral over A. The theorem is a consequence of (12).

Let A be a non degenerated ring and B be a ring. Assume A is a subring of B. The integral closure over A in B yielding a non empty subset of B is defined by the term

(Def. 3) $\{z$, where z is an element of $B : z$ is integral over $A\}$.

Let c be a complex. We say that c is algebraic if and only if

(Def. 4) there exists an element x of $\mathbb{C}_{\mathrm{F}}$ such that $x = c$ and x is integral over $\mathbb{F}_{\mathbb{Q}}$.

Let x be an element of $\mathbb{C}_{\mathrm{F}}$. Note that x is algebraic if and only if the condition (Def. 5) is satisfied.

(Def. 5) x is integral over $\mathbb{F}_{\mathbb{Q}}$.

Let c be a complex. We say that c is algebraic integer if and only if

(Def. 6) there exists an element x of $\mathbb{C}_{\mathrm{F}}$ such that $x = c$ and x is integral over $\mathbb{Z}^{\mathrm{R}}$.

Let x be an element of $\mathbb{C}_{\mathrm{F}}$. Observe that x is algebraic integer if and only if the condition (Def. 7) is satisfied.

(Def. 7) x is integral over $\mathbb{Z}^{\mathrm{R}}$.

Let x be a complex. We introduce the notation x is transcendental as an antonym for x is algebraic.

Note that every complex which is rational is also algebraic and there exists a complex which is algebraic and there exists an element of $\mathbb{C}_{\mathrm{F}}$ which is algebraic and every complex which is integer is also algebraic integer and there exists a complex which is algebraic integer and there exists an element of $\mathbb{C}_{\mathrm{F}}$ which is algebraic integer.

Let A, B be rings and x be an element of B. The functor $\mathrm{AnnPoly}(x, A)$ yielding a non empty subset of $\mathrm{PolyRing}(A)$ is defined by the term

(Def. 8) $\{p$, where p is a polynomial over $A : \mathrm{ExtEval}(p, x) = 0_B\}$.

Now we state the propositions:

(24) Let us consider rings A, B, an element w of B, and elements x, y of PolyRing(A). Suppose A is a subring of B and x, $y \in$ AnnPoly(w, A). Then $x + y \in$ AnnPoly(w, A). The theorem is a consequence of (15).

(25) Let us consider a commutative ring B, an element z of B, and elements p, x of PolyRing(A). Suppose A is a subring of B and $x \in$ AnnPoly(z, A). Then $p \cdot x \in$ AnnPoly(z, A). The theorem is a consequence of (20).

(26) Let us consider a commutative ring B, an element w of B, and elements p, x of PolyRing(A). Suppose A is a subring of B and $x \in$ AnnPoly(w, A). Then $x \cdot p \in$ AnnPoly(w, A). The theorem is a consequence of (20).

(27) Let us consider a non degenerated ring A, a non degenerated commutative ring B, and an element w of B. Suppose A is a subring of B. Then AnnPoly(w, A) is a proper ideal of PolyRing(A).
PROOF: AnnPoly(w, A) is closed under addition. AnnPoly(w, A) is left ideal. AnnPoly(w, A) is right ideal. AnnPoly(w, A) is proper by [8, (37)], (14). □

4. PROPERTIES OF POLYNOMIAL RING OVER PRINCIPAL IDEAL DOMAIN

From now on K, L denote fields.

Now we state the propositions:

(28) Let us consider fields K, L, and an element w of L. Suppose K is a subring of L. Then there exists an element g of PolyRing(K) such that $\{g\}$–ideal = AnnPoly(w, K). The theorem is a consequence of (27).

(29) Let us consider fields K, L, and an element z of L. Suppose z is integral over K. Then AnnPoly(z, K) $\neq \{0_{\mathrm{PolyRing}(K)}\}$.
PROOF: Consider f being a polynomial over K such that LC $f = 1_K$ and ExtEval(f, z) $= 0_L$. $f \notin \{0_{\mathrm{PolyRing}(K)}\}$ by [2, (47), (64)], [11, (7)]. □

(30) Let us consider a field K, and an element p of PolyRing(K). Suppose $p \neq \mathbf{0}.K$. Then p is a non zero element of the carrier of PolyRing(K).

Let us consider fields K, L and an element w of L. Now we state the propositions:

(31) If K is a subring of L, then AnnPoly(w, K) is quasi-prime. The theorem is a consequence of (20).

(32) If K is a subring of L and w is integral over K, then AnnPoly(w, K) is prime. The theorem is a consequence of (31) and (27).

(33) Let us consider fields K, L, and an element z of L. Suppose K is a subring of L and z is integral over K. Then there exists an element f of PolyRing(K) such that

(i) $f \neq \mathbf{0}.\,K$, and

(ii) $\{f\}$–ideal $=$ AnnPoly(z, K), and

(iii) $f =$ NormPoly f.

The theorem is a consequence of (28), (29), and (30).

(34) Let us consider fields K, L, an element z of L, and elements f, g of PolyRing(K). Suppose z is integral over K and $\{f\}$–ideal $=$ AnnPoly(z, K) and $f =$ NormPoly f and $\{g\}$–ideal $=$ AnnPoly(z, K) and $g =$ NormPoly g. Then $f = g$. The theorem is a consequence of (29) and (30).

Let K, L be fields and z be an element of L. Assume K is a subring of L and z is integral over K. The minimal polynomial of z over K yielding an element of the carrier of PolyRing(K) is defined by

(Def. 9) $it \neq \mathbf{0}.\,K$ and $\{it\}$–ideal $=$ AnnPoly(z, K) and $it =$ NormPoly it.

Assume K is a subring of L and z is integral over K. The degree of algebraic number z over K yielding an element of $\mathbb{N}$ is defined by the term

(Def. 10) deg(the minimal polynomial of z over K).

Let A, B be rings and x be an element of B. The functor HomExtEval(x, A) yielding a function from PolyRing(A) into B is defined by

(Def. 11) for every polynomial p over A, $it(p) =$ ExtEval(p, x).

Let x be an element of $\mathbb{C}_{\rm F}$. Note that HomExtEval$(x, \mathbb{F}_{\mathbb{Q}})$ is unity-preserving, additive, and multiplicative.

Now we state the propositions:

(35) Let us consider an element x of $\mathbb{C}_{\rm F}$.
Then $\mathbb{C}_{\rm F}$ is (PolyRing$(\mathbb{F}_{\mathbb{Q}})$)-homomorphic.

(36) Let us consider an element x of B, and an object z.
If $z \in$ rng HomExtEval(x, A), then $z \in B$.

Let x be an element of $\mathbb{C}_{\rm F}$. The functor FQ(x) yielding a subset of $\mathbb{C}_{\rm F}$ is defined by the term

(Def. 12) rng HomExtEval$(x, \mathbb{F}_{\mathbb{Q}})$.

Let us note that FQ(x) is non empty.

Let us consider elements x, z_1, z_2 of $\mathbb{C}_{\rm F}$. Now we state the propositions:

(37) If z_1, $z_2 \in$ FQ(x), then $z_1 + z_2 \in$ FQ(x). The theorem is a consequence of (3) and (15).

(38) If z_1, $z_2 \in$ FQ(x), then $z_1 \cdot z_2 \in$ FQ(x). The theorem is a consequence of (3) and (20).

(39) Let us consider an element x of $\mathbb{C}_{\rm F}$, and an element a of $\mathbb{F}_{\mathbb{Q}}$. Then $a \in$ FQ(x). The theorem is a consequence of (3) and (21).

Let x be an element of $\mathbb{C}_{\mathrm{F}}$. The functor FQ-add(x) yielding a binary operation on FQ(x) is defined by the term

(Def. 13) $+_{\mathbb{C}} \restriction \mathrm{FQ}(x)$.

The functor FQ-mult(x) yielding a binary operation on FQ(x) is defined by the term

(Def. 14) $\cdot_{\mathbb{C}} \restriction \mathrm{FQ}(x)$.

Let us consider an element x of $\mathbb{C}_{\mathrm{F}}$ and elements z, w of FQ(x). Now we state the propositions:

(40) $(\mathrm{FQ\text{-}add}(x))(z, w) = z + w$.

(41) $(\mathrm{FQ\text{-}mult}(x))(z, w) = z \cdot w$.

(42) Let us consider an element x of $\mathbb{C}_{\mathrm{F}}$. Then $1_{\mathbb{C}_{\mathrm{F}}}(\in \mathrm{FQ}(x)) = 1_{\mathbb{C}_{\mathrm{F}}}$. The theorem is a consequence of (3) and (39).

(43) $(-1_{\mathbb{F}_{\mathbb{Q}}})(\in \mathbb{C}_{\mathrm{F}}) = -1_{\mathbb{C}_{\mathrm{F}}}$. The theorem is a consequence of (3).

Let x be an element of $\mathbb{C}_{\mathrm{F}}$. The functor $\mathbb{Q}[x]$ yielding a strict, non empty double loop structure is defined by the term

(Def. 15) $\langle \mathrm{FQ}(x), \mathrm{FQ\text{-}add}(x), \mathrm{FQ\text{-}mult}(x), 1_{\mathbb{C}_{\mathrm{F}}}(\in \mathrm{FQ}(x)), 0_{\mathbb{C}_{\mathrm{F}}}(\in \mathrm{FQ}(x))\rangle$.

Now we state the proposition:

(44) Let us consider an element x of $\mathbb{C}_{\mathrm{F}}$. Then $\mathbb{Q}[x]$ is a ring.

PROOF: Reconsider $Z = \langle \mathrm{FQ}(x), \mathrm{FQ\text{-}add}(x), \mathrm{FQ\text{-}mult}(x), 1_{\mathbb{C}_{\mathrm{F}}}(\in \mathrm{FQ}(x)), 0_{\mathbb{C}_{\mathrm{F}}}(\in \mathrm{FQ}(x))\rangle$ as a non empty double loop structure. For every elements v, w of Z, $v + w = w + v$. For every elements u, v, w of Z, $(u + v) + w = u + (v + w)$. For every element v of Z, $v + 0_Z = v$. Every element of Z is right complementable by (36), [6, (9)], (39), (43). For every elements a, b, v of Z, $(a + b) \cdot v = a \cdot v + b \cdot v$. For every elements a, v, w of Z, $a \cdot (v + w) = a \cdot v + a \cdot w$ and $(v + w) \cdot a = v \cdot a + w \cdot a$. For every elements a, b, v of Z, $(a \cdot b) \cdot v = a \cdot (b \cdot v)$. For every element v of Z, $v \cdot 1_Z = v$ and $1_Z \cdot v = v$. □

Let x be an element of $\mathbb{C}_{\mathrm{F}}$. One can verify that $\mathbb{Q}[x]$ is Abelian, add-associative, right zeroed, right complementable, associative, well unital, and distributive.

Let z be an element of $\mathbb{C}_{\mathrm{F}}$. One can verify that $\mathbb{Q}[z]$ is integral domain-like, commutative, and non degenerated.

Now we state the proposition:

(45) Let us consider an element x of $\mathbb{C}_{\mathrm{F}}$. Then $\mathbb{Q} \times \mathbb{Q} \subseteq \mathrm{FQ}(x) \times \mathrm{FQ}(x) \subseteq \mathbb{C} \times \mathbb{C}$. The theorem is a consequence of (39).

Let us consider an element x of $\mathbb{C}_{\mathrm{F}}$. Now we state the propositions:

(46) The addition of $\mathbb{F}_{\mathbb{Q}} =$ (the addition of $\mathbb{Q}[x]$) $\restriction \mathbb{Q}$. The theorem is a consequence of (45).

(47) The multiplication of $\mathbb{F}_{\mathbb{Q}}$ = (the multiplication of $\mathbb{Q}[x]$) $\restriction \mathbb{Q}$. The theorem is a consequence of (45).

(48) $\mathbb{F}_{\mathbb{Q}}$ is a subring of $\mathbb{Q}[x]$. The theorem is a consequence of (46), (47), (42), (3), and (39).

Let us consider elements f, g of PolyRing(K). Now we state the propositions:

(49) Suppose $f \neq 0_{\mathrm{PolyRing}(K)}$ and $\{f\}$–ideal is prime and $g \notin \{f\}$–ideal. Then $\{f, g\}$–ideal = the carrier of PolyRing(K).

(50) Suppose $f \neq 0_{\mathrm{PolyRing}(K)}$ and $\{f\}$–ideal is prime and $g \notin \{f\}$–ideal. Then $\{f\}$–ideal and $\{g\}$–ideal are co-prime. The theorem is a consequence of (49).

(51) Let us consider an element x of $\mathbb{C}_{\mathrm{F}}$, and an element a of $\mathbb{Q}[x]$. Then there exists an element g of PolyRing$(\mathbb{F}_{\mathbb{Q}})$ such that $a = (\mathrm{HomExtEval}(x, \mathbb{F}_{\mathbb{Q}}))(g)$.

Let us consider elements x, a of $\mathbb{C}_{\mathrm{F}}$. Now we state the propositions:

(52) Suppose $a \neq 0_{\mathbb{C}_{\mathrm{F}}}$ and $a \in$ the carrier of $\mathbb{Q}[x]$. Then there exists an element g of PolyRing$(\mathbb{F}_{\mathbb{Q}})$ such that

   (i) $g \notin \mathrm{AnnPoly}(x, \mathbb{F}_{\mathbb{Q}})$, and

   (ii) $a = (\mathrm{HomExtEval}(x, \mathbb{F}_{\mathbb{Q}}))(g)$.

   The theorem is a consequence of (51).

(53) Suppose x is algebraic and $a \neq 0_{\mathbb{C}_{\mathrm{F}}}$ and $a \in$ the carrier of $\mathbb{Q}[x]$. Then there exist elements f, g of PolyRing$(\mathbb{F}_{\mathbb{Q}})$ such that

   (i) $\{f\}$–ideal = $\mathrm{AnnPoly}(x, \mathbb{F}_{\mathbb{Q}})$, and

   (ii) $g \notin \mathrm{AnnPoly}(x, \mathbb{F}_{\mathbb{Q}})$, and

   (iii) $a = (\mathrm{HomExtEval}(x, \mathbb{F}_{\mathbb{Q}}))(g)$, and

   (iv) $\{f\}$–ideal and $\{g\}$–ideal are co-prime.

   The theorem is a consequence of (28), (3), (52), (32), (29), and (50).

(54) Suppose x is algebraic and $a \neq 0_{\mathbb{C}_{\mathrm{F}}}$ and $a \in$ the carrier of $\mathbb{Q}[x]$. Then there exists an element b of $\mathbb{C}_{\mathrm{F}}$ such that

   (i) $b \in$ the carrier of $\mathbb{Q}[x]$, and

   (ii) $a \cdot b = 1_{\mathbb{C}_{\mathrm{F}}}$.

   The theorem is a consequence of (53), (3), (14), (15), and (20).

(55) Let us consider an element x of $\mathbb{C}_{\mathrm{F}}$. If x is algebraic, then $\mathbb{Q}[x]$ is a field. The theorem is a consequence of (54), (41), and (42).

References

[1] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to Commutative Algebra*, volume 2. Addison-Wesley Reading, 1969.

[2] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Formalized Mathematics*, 9(**3**):565–582, 2001.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

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

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

[6] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[7] Hideyuki Matsumura. *Commutative Ring Theory*. Cambridge University Press, 2nd edition, 1989. Cambridge Studies in Advanced Mathematics.

[8] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.

[9] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.

[10] Masayoshi Nagata. *Theory of Commutative Fields*, volume 125. American Mathematical Society, 1985. Translations of Mathematical Monographs.

[11] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

[12] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[13] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[14] Oscar Zariski and Pierre Samuel. *Commutative Algebra I*. Springer, 2nd edition, 1975.

Received December 15, 2016

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 24, No. 4, Pages 301–308, 2016
DOI: 10.1515/forma-2016-0026

DE GRUYTER OPEN
degruyter.com/view/j/forma

Niven's Theorem[1]

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Adam Naumowicz
Institute of Informatics
University of Białystok
Poland

Summary. This article formalizes the proof of Niven's theorem [12] which states that if x/π and $sin(x)$ are both rational, then the sine takes values 0, $\pm 1/2$, and ± 1. The main part of the formalization follows the informal proof presented at Pr∞fWiki (`https://proofwiki.org/wiki/Niven's_Theorem#Source_of_Name`). For this proof, we have also formalized the rational and integral root theorems setting constraints on solutions of polynomial equations with integer coefficients [8, 9].

MSC: 97G60 12D10 03B35

Keywords: Niven's theorem; rational root theorem; integral root theorem

MML identifier: `NIVEN`, version: `8.1.05 5.39.1282`

From now on r, t denote real numbers, i denotes an integer, k, n denote natural numbers, p denotes a polynomial over $\mathbb{R}_{\rm F}$, e denotes an element of $\mathbb{R}_{\rm F}$, L denotes a non empty zero structure, and z, z_0, z_1, z_2 denote elements of L.

Now we state the propositions:

(1) Let us consider complexes a, b, c, d. If $b \neq 0$ and $\frac{a}{b} = \frac{c}{d}$, then $a = \frac{b \cdot c}{d}$.

(2) Let us consider real numbers a, b. If $|a| = b$, then $a = b$ or $a = -b$.

(3) If $|i| \leqslant 2$, then $i = -2$ or $i = -1$ or $i = 0$ or $i = 1$ or $i = 2$. The theorem is a consequence of (2).

(4) If $n \neq 0$, then $i \mid i^n$.

(5) If $t > 0$, then there exists i such that $t \cdot i \leqslant r \leqslant t \cdot (i + 1)$.

[1]The work on the formalization presented in this article was completed thanks to the Mizar Mathematical Library maintenance and refactoring carried out at the Computer Center of the University of Białystok.

PROOF: Define $\mathcal{P}[\text{integer}] \equiv t \cdot \$_1 \leqslant r$. There exists an integer i_1 such that $\mathcal{P}[i_1]$. Set $F = \lceil \frac{r}{t} \rceil$. For every integer i_1 such that $\mathcal{P}[i_1]$ holds $i_1 \leqslant F$. Consider i such that $\mathcal{P}[i]$ and for every integer i_1 such that $\mathcal{P}[i_1]$ holds $i_1 \leqslant i$ from [15, Sch. 6]. □

(6) Let us consider a finite sequence p of elements of $\mathbb{R}_\mathrm{F}$, and a real-valued finite sequence q. If $p = q$, then $\sum p = \sum q$.
PROOF: Define $\mathcal{P}[\text{finite sequence}] \equiv$ for every finite sequence p of elements of $\mathbb{R}_\mathrm{F}$ for every real-valued finite sequence q such that $p = q$ and $p = \$_1$ holds $\sum p = \sum q$. $\mathcal{P}[\emptyset]$ by [16, (43)], [4, (72)]. For every finite sequence f and for every object x such that $\mathcal{P}[f]$ holds $\mathcal{P}[f \frown \langle x \rangle]$ by [2, (36), (38)], [5, (31)], [16, (41), (44)]. For every finite sequence f, $\mathcal{P}[f]$ from [2, Sch. 3]. □

(7) Let us consider a natural number i, and an element r of $\mathbb{R}_\mathrm{F}$. Then $\mathrm{power}_{\mathbb{R}_\mathrm{F}}(r, i) = r^i$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \mathrm{power}_{\mathbb{R}_\mathrm{F}}(r, \$_1) = r^{\$_1}$. For every natural number n, $\mathcal{P}[n]$ from [1, Sch. 2]. □

(8) $\sin(\frac{5 \cdot \pi}{6}) = \frac{1}{2}$.

(9) $\sin(\frac{5 \cdot \pi}{6} + 2 \cdot \pi \cdot i) = \frac{1}{2}$.

(10) $\sin(\frac{7 \cdot \pi}{6}) = -\frac{1}{2}$.

(11) $\sin(\frac{7 \cdot \pi}{6} + 2 \cdot \pi \cdot i) = -\frac{1}{2}$.

(12) $\sin(\frac{11 \cdot \pi}{6}) = -\frac{1}{2}$.

(13) $\sin(\frac{11 \cdot \pi}{6} + 2 \cdot \pi \cdot i) = -\frac{1}{2}$.

(14) $\cos(\frac{4 \cdot \pi}{3}) = -\frac{1}{2}$.

(15) $\cos(\frac{4 \cdot \pi}{3} + 2 \cdot \pi \cdot i) = -\frac{1}{2}$.

(16) $\cos(\frac{5 \cdot \pi}{3}) = \frac{1}{2}$.

(17) $\cos(\frac{5 \cdot \pi}{3} + 2 \cdot \pi \cdot i) = \frac{1}{2}$.

(18) If $0 \leqslant r \leqslant \frac{\pi}{2}$ and $\cos r = \frac{1}{2}$, then $r = \frac{\pi}{3}$.

(19) Let us consider an add-associative, right zeroed, right complementable, left distributive, non empty double loop structure L, and a sequence p of L. Then $\mathbf{0}.\, L * p = \mathbf{0}.\, L$.

Let us consider L, z, and n. One can verify that $\mathbf{0}.\, L +\cdot (n, z)$ is finite-Support as a sequence of L.

Let us consider a polynomial p over L. Now we state the propositions:

(20) If $z \neq 0_L$, then if $p = \mathbf{0}.\, L +\cdot (n, z)$, then $\mathrm{len}\, p = n + 1$.
PROOF: the length of p is at most $n + 1$ by [1, (13)], [3, (32)], [14, (7)]. For every natural number m such that the length of p is at most m holds $n + 1 \leqslant m$ by [14, (13)], [3, (31)], [1, (13)]. □

(21) If $z \neq 0_L$, then if $p = \mathbf{0}.\,L +\cdot (n, z)$, then $\deg p = n$. The theorem is a consequence of (20).

Note that $\mathbf{0}.\,\mathbb{R}_{\rm F}$ is $\mathbb{Z}$-valued and $\mathbf{1}.\,\mathbb{R}_{\rm F}$ is $\mathbb{Z}$-valued and there exists an element of $\mathbb{R}_{\rm F}$ which is integer.

Now we state the proposition:

(22) $\operatorname{rng}\langle z\rangle = \{z, 0_L\}$.

Proof: Set $p = \langle z\rangle$. $\operatorname{rng} p \subseteq \{z, 0_L\}$ by [11, (32)], [1, (14)]. □

Let us consider L, z_0, z_1, and z_2. The functor $\langle z_0, z_1, z_2\rangle$ yielding a sequence of L is defined by the term

(Def. 1) $((\mathbf{0}.\,L +\cdot (0, z_0)) +\cdot (1, z_1)) +\cdot (2, z_2)$.

Now we state the propositions:

(23) $\langle z_0, z_1, z_2\rangle(0) = z_0$.

(24) $\langle z_0, z_1, z_2\rangle(1) = z_1$.

(25) $\langle z_0, z_1, z_2\rangle(2) = z_2$.

(26) If $3 \leqslant n$, then $\langle z_0, z_1, z_2\rangle(n) = 0_L$.

Let us consider L, z_0, z_1, and z_2. Let us observe that $\langle z_0, z_1, z_2\rangle$ is finite-Support.

Now we state the propositions:

(27) $\operatorname{len}\langle z_0, z_1, z_2\rangle \leqslant 3$. The theorem is a consequence of (26).

(28) If $z_2 \neq 0_L$, then $\operatorname{len}\langle z_0, z_1, z_2\rangle = 3$. The theorem is a consequence of (25) and (26).

(29) Let us consider a right zeroed, non empty additive loop structure L, and elements z_0, z_1 of L. Then $\langle z_0\rangle + \langle z_1\rangle = \langle z_0 + z_1\rangle$.

(30) Let us consider a right zeroed, non empty additive loop structure L, and elements z_0, z_1, z_2, z_3 of L. Then $\langle z_0, z_1\rangle + \langle z_2, z_3\rangle = \langle z_0 + z_2, z_1 + z_3\rangle$.

(31) Let us consider a right zeroed, non empty additive loop structure L, and elements z_0, z_1, z_2, z_3, z_4, z_5 of L. Then $\langle z_0, z_1, z_2\rangle + \langle z_3, z_4, z_5\rangle = \langle z_0 + z_3, z_1 + z_4, z_2 + z_5\rangle$. The theorem is a consequence of (23), (24), (25), and (26).

(32) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, and an element z_0 of L. Then $-\langle z_0\rangle = \langle -z_0\rangle$.

(33) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, and elements z_0, z_1 of L. Then $-\langle z_0, z_1\rangle = \langle -z_0, -z_1\rangle$.

(34) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, and elements z_0, z_1, z_2 of L. Then

$-\langle z_0, z_1, z_2 \rangle = \langle -z_0, -z_1, -z_2 \rangle$. The theorem is a consequence of (23), (24), (25), and (26).

(35) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, and elements z_0, z_1 of L. Then $\langle z_0 \rangle - \langle z_1 \rangle = \langle z_0 - z_1 \rangle$. The theorem is a consequence of (32) and (29).

(36) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, and elements z_0, z_1, z_2, z_3 of L. Then $\langle z_0, z_1 \rangle - \langle z_2, z_3 \rangle = \langle z_0 - z_2, z_1 - z_3 \rangle$. The theorem is a consequence of (33) and (30).

(37) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, and elements z_0, z_1, z_2, z_3, z_4, z_5 of L. Then $\langle z_0, z_1, z_2 \rangle - \langle z_3, z_4, z_5 \rangle = \langle z_0 - z_3, z_1 - z_4, z_2 - z_5 \rangle$. The theorem is a consequence of (34) and (31).

(38) Let us consider an add-associative, right zeroed, right complementable, left distributive, unital, associative, non empty double loop structure L, and elements z_0, z_1, z_2, x of L. Then $\mathrm{eval}(\langle z_0, z_1, z_2 \rangle, x) = z_0 + z_1 \cdot x + z_2 \cdot x \cdot x$. The theorem is a consequence of (23), (24), (27), and (25).

Let a be an integer element of $\mathbb{R}_{\mathrm{F}}$. Note that $\langle a \rangle$ is $\mathbb{Z}$-valued.

Let a, b be integer elements of $\mathbb{R}_{\mathrm{F}}$. One can verify that $\langle a, b \rangle$ is $\mathbb{Z}$-valued.

Let a, b, c be integer elements of $\mathbb{R}_{\mathrm{F}}$. Observe that $\langle a, b, c \rangle$ is $\mathbb{Z}$-valued and there exists a polynomial over $\mathbb{R}_{\mathrm{F}}$ which is monic and $\mathbb{Z}$-valued and there exists a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$ which is $\mathbb{Z}$-valued.

Let F be a $\mathbb{Z}$-valued finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$. One can check that $\sum F$ is integer.

Let f be a $\mathbb{Z}$-valued sequence of $\mathbb{R}_{\mathrm{F}}$. Let us note that $-f$ is $\mathbb{Z}$-valued.

Let g be a $\mathbb{Z}$-valued sequence of $\mathbb{R}_{\mathrm{F}}$. Observe that $f+g$ is $\mathbb{Z}$-valued and $f-g$ is $\mathbb{Z}$-valued and $f * g$ is $\mathbb{Z}$-valued.

Now we state the proposition:

(39) Let us consider a non degenerated, non empty double loop structure L, and an element z of L. Then $\mathrm{LC}\langle z, 1_L \rangle = 1_L$.

Let L be a non degenerated, non empty double loop structure and z be an element of L. One can check that $\langle z, 1_L \rangle$ is monic.

Now we state the proposition:

(40) Let us consider a non degenerated, non empty double loop structure L, and elements z_1, z_2 of L. Then $\mathrm{LC}\langle z_1, z_2, 1_L \rangle = 1_L$. The theorem is a consequence of (28) and (25).

Let L be a non degenerated, non empty double loop structure and z_1, z_2 be elements of L. Let us observe that $\langle z_1, z_2, 1_L \rangle$ is monic.

Let p be a $\mathbb{Z}$-valued polynomial over $\mathbb{R}_{\mathrm{F}}$. Let us note that $\mathrm{LC}\, p$ is integer.

Now we state the proposition:

(41) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, and a polynomial p over L. Then $\deg(-p) = \deg p$.

Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L and polynomials p, q over L. Now we state the propositions:

(42) If $\deg p > \deg q$, then $\deg(p + q) = \deg p$.

(43) If $\deg p > \deg q$, then $\deg(p - q) = \deg p$.

(44) If $\deg p < \deg q$, then $\deg(p - q) = \deg q$.

(45) Let us consider an add-associative, right zeroed, right complementable, distributive, non degenerated double loop structure L, and a polynomial p over L. Then $\mathrm{LC}\, p = -\mathrm{LC}(-p)$.

(46) Let us consider an add-associative, right zeroed, right complementable, associative, commutative, well unital, almost left invertible, distributive, non degenerated double loop structure L, and polynomials p, q over L. Then $\mathrm{LC}(p * q) = \mathrm{LC}\, p \cdot \mathrm{LC}\, q$. The theorem is a consequence of (19).

Let us consider an add-associative, right zeroed, right complementable, distributive, non degenerated double loop structure L, a monic polynomial p over L, and a polynomial q over L. Now we state the propositions:

(47) If $\deg p > \deg q$, then $p + q$ is monic. The theorem is a consequence of (42).

(48) If $\deg p > \deg q$, then $p - q$ is monic. The theorem is a consequence of (43).

Let L be an add-associative, right zeroed, right complementable, associative, commutative, well unital, almost left invertible, distributive, non degenerated double loop structure and p, q be monic polynomials over L. Let us note that $p * q$ is monic.

Now we state the propositions:

(49) Let us consider an Abelian, add-associative, right zeroed, right complementable, unital, distributive, non empty double loop structure L, elements z_1, z_2 of L, and a polynomial p over L. Suppose $\mathrm{eval}(p, z_1) = z_2$. Then $\mathrm{eval}(p - \langle z_2 \rangle, z_1) = 0_L$.

(50) RATIONAL ROOT THEOREM:
Let us consider a $\mathbb{Z}$-valued polynomial p over $\mathbb{R}_{\mathrm{F}}$, and an element e of $\mathbb{R}_{\mathrm{F}}$. Suppose e is a root of p. Let us consider integers k, l. Suppose $l \neq 0$ and $e = \frac{k}{l}$ and k and l are relatively prime. Then

(i) $k \mid p(0)$, and

(ii) $l \mid \mathrm{LC}\, p$.

The theorem is a consequence of (7), (6), and (4).

(51) Integral root theorem:
Let us consider a monic, $\mathbb{Z}$-valued polynomial p over $\mathbb{R}_{\mathrm{F}}$, and a rational element e of $\mathbb{R}_{\mathrm{F}}$. If e is a root of p, then e is integer. The theorem is a consequence of (50).

(52) Suppose $1 \leqslant n$ and $e = 2 \cdot \cos t$. Then there exists a monic, $\mathbb{Z}$-valued polynomial p over $\mathbb{R}_{\mathrm{F}}$ such that

(i) $\mathrm{eval}(p, e) = 2 \cdot \cos(n \cdot t)$, and

(ii) $\deg p = n$, and

(iii) if $n = 1$, then $p = \langle 0_{\mathbb{R}_{\mathrm{F}}}, 1_{\mathbb{R}_{\mathrm{F}}} \rangle$, and

(iv) if $n = 2$, then there exists an element r of $\mathbb{R}_{\mathrm{F}}$ such that $r = -2$ and $p = \langle r, 0_{\mathbb{R}_{\mathrm{F}}}, 1_{\mathbb{R}_{\mathrm{F}}} \rangle$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if $1 \leqslant \$_1$, then there exists a monic, $\mathbb{Z}$-valued polynomial p over $\mathbb{R}_{\mathrm{F}}$ such that $\mathrm{eval}(p, e) = 2 \cdot \cos(\$_1 \cdot t)$ and $\deg p = \$_1$ and if $\$_1 = 1$, then $p = \langle 0_{\mathbb{R}_{\mathrm{F}}}, 1_{\mathbb{R}_{\mathrm{F}}} \rangle$ and if $\$_1 = 2$, then there exists an element r of $\mathbb{R}_{\mathrm{F}}$ such that $r = -2$ and $p = \langle r, 0_{\mathbb{R}_{\mathrm{F}}}, 1_{\mathbb{R}_{\mathrm{F}}} \rangle$. $\mathcal{P}[1]$ by [11, (48), (40)]. $\mathcal{P}[2]$ by [6, (7)], (38), (28). For every non zero natural number k such that $\mathcal{P}[k]$ and $\mathcal{P}[k+1]$ holds $\mathcal{P}[k+2]$ by [1, (13)], [13, (38)], (48), [10, (24)]. For every non zero natural number k, $\mathcal{P}[k]$ from [7, Sch. 1]. $\square$

(53) If $0 \leqslant r \leqslant \frac{\pi}{2}$ and $\frac{r}{\pi}$ is rational and $\cos r$ is rational, then $r \in \{0, \frac{\pi}{3}, \frac{\pi}{2}\}$. The theorem is a consequence of (52), (1), (49), (48), (51), (3), and (18).

(54) Suppose $2 \cdot \pi \cdot i \leqslant r \leqslant \frac{\pi}{2} + 2 \cdot \pi \cdot i$ and $\frac{r}{\pi}$ is rational and $\cos r$ is rational. Then $r \in \{2 \cdot \pi \cdot i, \frac{\pi}{3} + 2 \cdot \pi \cdot i, \frac{\pi}{2} + 2 \cdot \pi \cdot i\}$. The theorem is a consequence of (53).

(55) If $\frac{\pi}{2} \leqslant r \leqslant \pi$ and $\frac{r}{\pi}$ is rational and $\cos r$ is rational, then $r \in \{\frac{\pi}{2}, \frac{2 \cdot \pi}{3}, \pi\}$. The theorem is a consequence of (53).

(56) Suppose $\frac{\pi}{2} + 2 \cdot \pi \cdot i \leqslant r \leqslant \pi + 2 \cdot \pi \cdot i$ and $\frac{r}{\pi}$ is rational and $\cos r$ is rational. Then $r \in \{\frac{\pi}{2} + 2 \cdot \pi \cdot i, \frac{2 \cdot \pi}{3} + 2 \cdot \pi \cdot i, \pi + 2 \cdot \pi \cdot i\}$. The theorem is a consequence of (55).

(57) Suppose $\pi \leqslant r \leqslant \frac{3 \cdot \pi}{2}$ and $\frac{r}{\pi}$ is rational and $\cos r$ is rational. Then $r \in \{\pi, \frac{4 \cdot \pi}{3}, \frac{3 \cdot \pi}{2}\}$. The theorem is a consequence of (53).

(58) Suppose $\pi + 2 \cdot \pi \cdot i \leqslant r \leqslant \frac{3 \cdot \pi}{2} + 2 \cdot \pi \cdot i$ and $\frac{r}{\pi}$ is rational and $\cos r$ is rational. Then $r \in \{\pi + 2 \cdot \pi \cdot i, \frac{4 \cdot \pi}{3} + 2 \cdot \pi \cdot i, \frac{3 \cdot \pi}{2} + 2 \cdot \pi \cdot i\}$. The theorem is a consequence of (57).

(59) Suppose $\frac{3 \cdot \pi}{2} \leqslant r \leqslant 2 \cdot \pi$ and $\frac{r}{\pi}$ is rational and $\cos r$ is rational. Then $r \in \{\frac{3 \cdot \pi}{2}, \frac{5 \cdot \pi}{3}, 2 \cdot \pi\}$. The theorem is a consequence of (53).

(60) Suppose $\frac{3\cdot\pi}{2} + 2\cdot\pi\cdot i \leqslant r \leqslant 2\cdot\pi + 2\cdot\pi\cdot i$ and $\frac{r}{\pi}$ is rational and $\cos r$ is rational. Then $r \in \{\frac{3\cdot\pi}{2} + 2\cdot\pi\cdot i, \frac{5\cdot\pi}{3} + 2\cdot\pi\cdot i, 2\cdot\pi + 2\cdot\pi\cdot i\}$. The theorem is a consequence of (59).

(61) If $\frac{r}{\pi}$ is rational and $\cos r$ is rational, then $\cos r \in \{0, 1, -1, \frac{1}{2}, -\frac{1}{2}\}$.

(62) If $0 \leqslant r \leqslant \frac{\pi}{2}$ and $\frac{r}{\pi}$ is rational and $\sin r$ is rational, then $r \in \{0, \frac{\pi}{6}, \frac{\pi}{2}\}$. The theorem is a consequence of (53).

(63) Suppose $2\cdot\pi\cdot i \leqslant r \leqslant \frac{\pi}{2} + 2\cdot\pi\cdot i$ and $\frac{r}{\pi}$ is rational and $\sin r$ is rational. Then $r \in \{2\cdot\pi\cdot i, \frac{\pi}{6} + 2\cdot\pi\cdot i, \frac{\pi}{2} + 2\cdot\pi\cdot i\}$. The theorem is a consequence of (62).

(64) If $\frac{\pi}{2} \leqslant r \leqslant \pi$ and $\frac{r}{\pi}$ is rational and $\sin r$ is rational, then $r \in \{\frac{\pi}{2}, \frac{5\cdot\pi}{6}, \pi\}$. The theorem is a consequence of (62).

(65) Suppose $\frac{\pi}{2} + 2\cdot\pi\cdot i \leqslant r \leqslant \pi + 2\cdot\pi\cdot i$ and $\frac{r}{\pi}$ is rational and $\sin r$ is rational. Then $r \in \{\frac{\pi}{2} + 2\cdot\pi\cdot i, \frac{5\cdot\pi}{6} + 2\cdot\pi\cdot i, \pi + 2\cdot\pi\cdot i\}$. The theorem is a consequence of (64).

(66) Suppose $\pi \leqslant r \leqslant \frac{3\cdot\pi}{2}$ and $\frac{r}{\pi}$ is rational and $\sin r$ is rational. Then $r \in \{\pi, \frac{7\cdot\pi}{6}, \frac{3\cdot\pi}{2}\}$. The theorem is a consequence of (62).

(67) Suppose $\pi + 2\cdot\pi\cdot i \leqslant r \leqslant \frac{3\cdot\pi}{2} + 2\cdot\pi\cdot i$ and $\frac{r}{\pi}$ is rational and $\sin r$ is rational. Then $r \in \{\pi + 2\cdot\pi\cdot i, \frac{7\cdot\pi}{6} + 2\cdot\pi\cdot i, \frac{3\cdot\pi}{2} + 2\cdot\pi\cdot i\}$. The theorem is a consequence of (66).

(68) Suppose $\frac{3\cdot\pi}{2} \leqslant r \leqslant 2\cdot\pi$ and $\frac{r}{\pi}$ is rational and $\sin r$ is rational. Then $r \in \{\frac{3\cdot\pi}{2}, \frac{11\cdot\pi}{6}, 2\cdot\pi\}$. The theorem is a consequence of (62).

(69) Suppose $\frac{3\cdot\pi}{2} + 2\cdot\pi\cdot i \leqslant r \leqslant 2\cdot\pi + 2\cdot\pi\cdot i$ and $\frac{r}{\pi}$ is rational and $\sin r$ is rational. Then $r \in \{\frac{3\cdot\pi}{2} + 2\cdot\pi\cdot i, \frac{11\cdot\pi}{6} + 2\cdot\pi\cdot i, 2\cdot\pi + 2\cdot\pi\cdot i\}$. The theorem is a consequence of (68).

(70) NIVEN'S THEOREM:
If $\frac{r}{\pi}$ is rational and $\sin r$ is rational, then $\sin r \in \{0, 1, -1, \frac{1}{2}, -\frac{1}{2}\}$.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

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

[3] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

[4] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[5] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[6] Yuzhong Ding and Xiquan Liang. Formulas and identities of trigonometric functions. *Formalized Mathematics*, 12(**3**):243–246, 2004.

[7] Magdalena Jastrzębska and Adam Grabowski. Some properties of Fibonacci numbers. *Formalized Mathematics*, 12(**3**):307–313, 2004.

[8] J.D. King. Integer roots of polynomials. *The Mathematical Gazette*, 90(519):455–456, 2006. doi:http://dx.doi.org/10.1017/S0025557200180295.

[9] Serge Lang. *Algebra*. Addison-Wesley, 1980.

[10] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.

[11] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.

[12] Ivan Niven. *Irrational numbers*. The Carus Mathematical Monographs, No. 11. The Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, N.Y., 1956.

[13] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2004.

[14] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[15] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[16] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

Received December 15, 2016

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.