Contents

Formaliz. Math. 30 (**4**)

Continued on inside back cover

FORMALIZED MATHEMATICS
Vol. 30, No. 4, Pages 245–253, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0020

sciendo
sciendo.com/journal/forma

Prime Representing Polynomial with 10 Unknowns – Introduction. Part II

Karol Pąk
Institute of Computer Science
University of Białystok
Poland

Summary. In our previous work [7] we prove that the set of prime numbers is diophantine using the 26-variable polynomial proposed in [4]. In this paper, we focus on the reduction of the number of variables to 10 and it is the smallest variables number known today [5], [10]. Using the Mizar [3], [2] system, we formalize the first step in this direction by proving Theorem 1 [5] formulated as follows: Let $k \in \mathbb{N}$. Then k is prime if and only if there exists $f, i, j, m, u \in \mathbb{N}^+$, $r, s, t \in \mathbb{N}$ unknowns such that

$$DFI \texttt{ is square } \wedge (M^2-1)S^2+1 \texttt{ is square } \wedge$$
$$((MU)^2-1)T^2+1 \texttt{ is square } \wedge$$
$$(4f^2-1)(r-mSTU)^2+4u^2S^2T^2 < 8fuST(r-mSTU)$$
$$FL \mid (H-C)Z+F(f+1)Q+F(k+1)((W^2-1)Su-W^2u^2+1) \quad (0.1)$$

where auxiliary variables $A-I, L, M, S-W, Q \in \mathbb{Z}$ are simply abbreviations defined as follows $W = 100fk(k+1)$, $U = 100u^3W^3+1$, $M = 100mUW+1$, $S = (M-1)s+k+1$, $T = (MU-1)t+W-k+1$, $Q = 2MW-W^2-1$, $L = (k+1)Q$, $A = M(U+1)$, $B = W+1$, $C = r+W+1$, $D = (A^2-1)C^2+1$, $E = 2iC^2LD$, $F = (A^2-1)E^2+1$, $G = A+F(F-A)$, $H = B+2(j-1)C$, $I = (G^2-1)H^2+1$. It is easily see that (0.1) uses 8 unknowns explicitly along with five implicit one for each diophantine relationship: `is square`, inequality, and divisibility. Together with k this gives a total of 14 variables. This work has been partially presented in [8].

MSC: 11D45 68V20

Keywords: polynomial reduction; diophantine equation

MML identifier: `HILB10_8`, version: `8.1.12 5.72.1435`

1. Theta Notation

From now on A denotes a non trivial natural number, B, C, n, m, k denote natural numbers, and e denotes a natural number.

Let θ be a real number. We say that θ is theta if and only if

(Def. 1) $-1 \leqslant \theta \leqslant 1$.

Let us observe that 0 is theta and there exists a real number which is theta.

A Theta is a theta real number. Let θ be a Theta. Let us observe that $-\theta$ is theta.

Let u be a Theta. Let us note that $\theta \cdot u$ is theta. Now we state the propositions:

(1) Let us consider a Theta θ. Then $|\theta| \leqslant 1$.

(2) Let us consider a Theta θ, and real numbers λ, ε_1, ε_2. Suppose $\lambda = \theta \cdot \varepsilon_1$ and $|\varepsilon_1| \leqslant |\varepsilon_2|$. Then there exists a Theta θ_1 such that $\lambda = \theta_1 \cdot \varepsilon_2$.

(3) Let us consider Theta's θ_1, θ_2, and real numbers λ, ε_1, ε_2. Suppose $\lambda = (1 + \theta_1 \cdot \varepsilon_1) \cdot (1 + \theta_2 \cdot \varepsilon_2)$ and $0 \leqslant \varepsilon_1 \leqslant 1$ and $0 \leqslant \varepsilon_2$. Then there exists a Theta θ such that $\lambda = 1 + \theta \cdot (\varepsilon_1 + 2 \cdot \varepsilon_2)$.

(4) Let us consider Theta's θ_1, θ_2, and real numbers ε_1, ε_2. Suppose $\theta_1 \cdot \varepsilon_1 \leqslant \varepsilon_2 \leqslant \theta_2 \cdot \varepsilon_1$. Then there exists a Theta θ such that $\varepsilon_2 = \theta \cdot \varepsilon_1$.

(5) Let us consider a Theta θ, and real numbers λ, ε_1, ε_2. Suppose $\lambda = \theta \cdot \varepsilon_1$ and $\varepsilon_1 \leqslant \varepsilon_2$ and $0 \leqslant \varepsilon_1$. Then there exists a Theta θ_1 such that $\lambda = \theta_1 \cdot \varepsilon_2$. The theorem is a consequence of (2).

(6) Let us consider Theta's θ_1, θ_2, and real numbers ε_1, ε_2. Suppose $0 \leqslant \varepsilon_1$ and $0 \leqslant \varepsilon_2$. Then there exists a Theta θ such that $\theta_1 \cdot \varepsilon_1 + \theta_2 \cdot \varepsilon_2 = \theta \cdot (\varepsilon_1 + \varepsilon_2)$. The theorem is a consequence of (4).

(7) Let us consider a Theta θ_1, and a real number ε. Suppose $0 \leqslant \varepsilon \leqslant \frac{1}{2}$. Then there exists a Theta θ_2 such that $\frac{1}{1+\theta_1 \cdot \varepsilon} = 1 + \theta_2 \cdot 2 \cdot \varepsilon$. The theorem is a consequence of (2).

(8) If $m^{\mathbf{2}} \leqslant n$, then there exists a Theta θ such that $\binom{n}{m} = \frac{n^m}{m!} \cdot (1 + \theta \cdot \frac{m^{\mathbf{2}}}{n})$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1^{\mathbf{2}} \leqslant n$, then there exists a Theta θ such that $\binom{n}{\$_1} = \frac{n^{\$_1}}{\$_1!} \cdot (1 + \theta \cdot \frac{\$_1^{\mathbf{2}}}{n})$. For every m such that $\mathcal{P}[m]$ holds $\mathcal{P}[m+1]$. For every m, $\mathcal{P}[m]$. $\square$

(9) Let us consider a Theta θ, and real numbers α, ε. Suppose $\alpha = (1 + \theta \cdot \varepsilon)^n$ and $0 \leqslant \varepsilon \leqslant \frac{1}{2 \cdot n}$. Then there exists a Theta θ_1 such that $\alpha = 1 + \theta_1 \cdot 2 \cdot n \cdot \varepsilon$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every Theta θ for every real numbers α, ε such that $\alpha = (1 + \theta \cdot \varepsilon)^{\$_1}$ and $0 \leqslant \varepsilon \leqslant \frac{1}{2 \cdot \$_1}$ there exists a Theta θ_1 such that $\alpha = 1 + \theta_1 \cdot 2 \cdot \$_1 \cdot \varepsilon$. $\mathcal{P}[0]$. If $\mathcal{P}[m]$, then $\mathcal{P}[m+1]$. $\mathcal{P}[m]$. $\square$

2. More on Solutions to Pell's Equation

In the sequel a denotes a non trivial natural number. Now we state the propositions:

(10) If $n \leqslant a$, then there exists a Theta θ such that $\mathtt{y}_a(n+1) = (2 \cdot a)^n \cdot (1 + \theta \cdot \frac{n}{a})$. The theorem is a consequence of (9) and (4).

(11) Let us consider a non trivial natural number a, and natural numbers y, n. Suppose $y > 0$ and $n > 0$ and $(a^{\mathbf{2}} - 1) \cdot y^{\mathbf{2}} + 1$ is a square and $y \equiv n \pmod{a-1}$ and $y \leqslant \mathtt{y}_a(a-1)$ and $n \leqslant a-1$. Then $y = \mathtt{y}_a(n)$.

(12) Let us consider a non trivial natural number a, and natural numbers s, n. Then $s^{\mathbf{2}} \cdot (s^n)^{\mathbf{2}} - (s^{\mathbf{2}} - 1) \cdot \mathtt{y}_a(n+1) \cdot s^n - 1 \equiv 0 \pmod{2 \cdot a \cdot s - s^{\mathbf{2}} - 1}$.
Proof: Set $S = s^{\mathbf{2}}$. Define $\mathcal{P}[\text{natural number}] \equiv S \cdot (s^{\$_1})^{\mathbf{2}} - (S-1) \cdot \mathtt{y}_a(\$_1 + 1) \cdot s^{\$_1} - 1 \equiv 0 \pmod{2 \cdot a \cdot s - s^{\mathbf{2}} - 1}$. For every natural number k such that for every n such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$. $\mathcal{P}[n]$. $\square$

(13) Let us consider a non trivial natural number a, and natural numbers s, n, r. Suppose $s > 0$ and $r > 0$ and $s^{\mathbf{2}} \cdot r^{\mathbf{2}} - (s^{\mathbf{2}} - 1) \cdot \mathtt{y}_a(n+1) \cdot r - 1 \equiv 0 \pmod{2 \cdot a \cdot s - s^{\mathbf{2}} - 1}$ and $s \cdot (s^n)^{\mathbf{2}} \cdot s^n < a$ and $s \cdot r^{\mathbf{2}} \cdot r < a$. Then $r = s^n$. The theorem is a consequence of (12).

(14) Let us consider natural numbers a, b, c, d. Suppose $a \leqslant b \leqslant c$ and $2 \cdot c \leqslant d$ and $c > 0$. Let us consider a finite sequence f of elements of $\mathbb{R}$. Suppose $\operatorname{len} f = b - a + 1$ and for every natural number i such that $i + 1 \in \operatorname{dom} f$ holds $f(i+1) = \binom{c}{a+i} \cdot d^{c -' (a+i)}$. Then $0 < \sum f < 2 \cdot c^a \cdot d^{c -' a}$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every natural numbers a, b, c, d such that $a \leqslant b \leqslant c$ and $2 \cdot c \leqslant d$ and $c > 0$ and $b - a = \$_1$ for every finite sequence f of elements of $\mathbb{R}$ such that $\operatorname{len} f = b - a + 1$ and for every natural number i such that $i + 1 \in \operatorname{dom} f$ holds $f(i+1) = \binom{c}{a+i} \cdot d^{c -' (a+i)}$ holds $0 \leqslant 1 - (\frac{c}{d})^{b+1-'a}$ and $0 < \sum f \leqslant \frac{1 - (\frac{c}{d})^{b+1-'a}}{1 - \frac{c}{d}} \cdot c^a \cdot d^{c -' a}$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. $\square$

(15) Let us consider natural numbers f, k, m, r, s, t, u, and integers W, M, U, S, T, Q. Suppose $f > 0$ and $k > 0$ and $m > 0$ and $u > 0$ and $(M^{\mathbf{2}} - 1) \cdot S^{\mathbf{2}} + 1$ is a square and $((M \cdot U)^{\mathbf{2}} - 1) \cdot T^{\mathbf{2}} + 1$ is a square and $W^{\mathbf{2}} \cdot u^{\mathbf{2}} - (W^{\mathbf{2}} - 1) \cdot S \cdot u - 1 \equiv 0 \pmod{Q}$ and $(4 \cdot f^{\mathbf{2}} - 1) \cdot (r - m \cdot S \cdot T \cdot U)^{\mathbf{2}} + 4 \cdot u^{\mathbf{2}} \cdot S^{\mathbf{2}} \cdot T^{\mathbf{2}} < 8 \cdot f \cdot u \cdot S \cdot T \cdot (r - m \cdot S \cdot T \cdot U)$ and $W = 100 \cdot f \cdot k \cdot (k+1)$ and $U = 100 \cdot u^3 \cdot W^3 + 1$ and $M = 100 \cdot m \cdot U \cdot W + 1$ and $S = (M-1) \cdot s + k + 1$ and $T = (M \cdot U - 1) \cdot t + W - k + 1$ and $Q = 2 \cdot M \cdot W - W^{\mathbf{2}} - 1$. Then

(i) $M \cdot (U+1)$ is a non trivial natural number, and

(ii) W is a natural number, and

(iii) for every non trivial natural number m_1 and for every natural number w such that $m_1 = M \cdot (U+1)$ and $w = W$ and $r+W+1 = \mathtt{y}_{m_1}(w+1)$ holds $f = k!$.

Proof: Reconsider $W_2 = W - k$ as a natural number. Reconsider $M_3 = M \cdot U$ as a non trivial natural number. Reconsider $M_1 = M - 1$ as a natural number. Set $R = r - m \cdot S \cdot T \cdot U$. $(\frac{u}{\frac{r}{S \cdot T} - m \cdot U} - f) \cdot (\frac{u}{\frac{r}{S \cdot T} - m \cdot U} - f) < \frac{1}{4}$. $r < \mathtt{y}_M(M_1)$ and $r < \mathtt{y}_M(M_3 - 1)$. $S = \mathtt{y}_M(k+1)$. $T = \mathtt{y}_{M_3}(W_2 + 1)$. $R < 3 \cdot u \cdot S \cdot T$. $m \cdot U + 3 \cdot u > \frac{r}{S \cdot T}$. Consider θ_1 being a Theta such that $\mathtt{y}_{m_1}(w+1) = (2 \cdot m_1)^w \cdot (1 + \theta_1 \cdot \frac{w}{m_1})$. Reconsider $I = 1$ as a Theta. Consider θ_2 being a Theta such that $\theta_1 \cdot \frac{w}{m_1} - \frac{W+1}{(2 \cdot m_1)^W} = \theta_2 \cdot \frac{1}{M}$. $u = W^k$. Consider θ_3 being a Theta such that $\mathtt{y}_M(k+1) = (2 \cdot M)^k \cdot (1 + \theta_3 \cdot \frac{k}{M})$. Consider θ_4 being a Theta such that $\mathtt{y}_{M_3}(W_2+1) = (2 \cdot M_3)^{W_2} \cdot (1 + \theta_4 \cdot \frac{W_2}{M_3})$. Consider θ'_3 being a Theta such that $\frac{1}{1+\theta_3 \cdot \frac{k}{M}} = 1 + \theta'_3 \cdot 2 \cdot \frac{k}{M}$. Consider θ'_4 being a Theta such that $\frac{1}{1+\theta_4 \cdot \frac{W_2}{M_3}} = 1 + \theta'_4 \cdot 2 \cdot \frac{W_2}{M_3}$. Consider θ_5 being a Theta such that $(1 + \theta'_3 \cdot (2 \cdot \frac{k}{M})) \cdot (1 + \theta_2 \cdot \frac{1}{M}) = 1 + \theta_5 \cdot (2 \cdot \frac{k}{M} + 2 \cdot \frac{1}{M})$.

Consider θ_6 being a Theta such that $(1 + \theta_5 \cdot (2 \cdot \frac{k}{M} + 2 \cdot \frac{1}{M})) \cdot (1 + \theta'_4 \cdot (2 \cdot \frac{W_2}{M_3})) = 1 + \theta_6 \cdot (2 \cdot \frac{k}{M} + 2 \cdot \frac{1}{M} + 2 \cdot (2 \cdot \frac{W_2}{M_3}))$. Consider θ_7 being a Theta such that $\theta_6 \cdot (2 \cdot \frac{k}{M} + 2 \cdot \frac{1}{M} + 2 \cdot (2 \cdot \frac{W_2}{M_3})) = \theta_7 \cdot \frac{5 \cdot k}{M}$. Set $I_1 = \langle \binom{W}{0} U^0 1^W, \ldots, \binom{W}{W} U^W 1^0 \rangle$. Set $I_3 = I_1 \restriction k$. Consider I_2 being a finite sequence such that $I_1 = I_3 \frown I_2$. For every natural number i such that $i + 1 \in \operatorname{dom} I_3$ holds $I_3(i+1) = \binom{W}{0+i} \cdot U^{W -' (0+i)}$. $0 < \sum I_3 < 2 \cdot W^0 \cdot U^{W -' 0}$. Set $U_2 = \frac{1}{U^{W_2+1}} \cdot I_3$. $\operatorname{rng} U_2 \subseteq \mathbb{N}$. Reconsider $Z = \sum U_2$ as an element of $\mathbb{N}$. For every natural number i such that $i + 1 \in \operatorname{dom} I_2$ holds $I_2(i+1) = \binom{W}{k+i} \cdot U^{W -' (k+i)}$. $0 < \sum I_2 < 2 \cdot W^k \cdot U^{W -' k}$. $|\theta_7| \leqslant 1$ and $|\frac{5 \cdot k}{M}| \leqslant 1$. $|\theta_7 \cdot (Z \cdot \frac{5 \cdot k}{M})| \leqslant 1 \cdot |Z \cdot \frac{5 \cdot k}{M}|$. Consider θ_8 being a Theta such that $(1 + I \cdot \frac{1}{U})^W = 1 + \theta_8 \cdot 2 \cdot W \cdot \frac{1}{U}$. Consider θ_9 being a Theta such that $\theta_7 \cdot (1 + \theta_8 \cdot 2 \cdot W \cdot \frac{1}{U}) = \theta_9 \cdot 2$.

Consider i_3 being a finite sequence of elements of $\mathbb{R}$, x being an element of $\mathbb{R}$ such that $I_2 = \langle x \rangle \frown i_3$. For every natural number i such that $i + 1 \in \operatorname{dom} i_3$ holds $i_3(i+1) = \binom{W}{k+1+i} \cdot U^{W -' (k+1+i)}$. $0 < \sum i_3 < 2 \cdot W^{k+1} \cdot U^{W -' (k+1)}$. Consider θ_{10} being a Theta such that $I \cdot (\frac{1}{U^{W_2}} \cdot (\sum i_3)) = \theta_{10} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U})$. Reconsider $\theta_{12} = \frac{1}{\binom{W}{k}}$ as a Theta. Consider θ_{11} being a Theta such that $\theta_{10} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U}) + \theta_9 \cdot \frac{U^k \cdot 10 \cdot k}{M} = \theta_{11} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})$. Consider θ'_{13} being a Theta such that $\binom{W}{k} = \frac{W^k}{k!} \cdot (1 + \theta'_{13} \cdot \frac{k^{\mathbf{2}}}{W})$. Consider θ_{13} being a Theta such that $\frac{1}{1+\theta'_{13} \cdot \frac{k^{\mathbf{2}}}{W}} = 1 + \theta_{13} \cdot 2 \cdot \frac{k^{\mathbf{2}}}{W}$. Consider θ_{14} being a Theta such that $\frac{1}{1+\theta_{12} \cdot \theta_{11} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})} = 1 + \theta_{14} \cdot 2 \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})$.

Consider θ_{15} being a Theta such that $(1+\theta_{14}\cdot(2\cdot(2\cdot W^{k+1}\cdot\frac{1}{U}+\frac{U^k\cdot 10\cdot k}{M})))\cdot(1+\theta_{13}\cdot(2\cdot\frac{k^{\mathbf{2}}}{W}))=1+\theta_{15}\cdot(2\cdot(2\cdot W^{k+1}\cdot\frac{1}{U}+\frac{U^k\cdot 10\cdot k}{M})+2\cdot(2\cdot\frac{k^{\mathbf{2}}}{W}))$. □

(16) Let us consider natural numbers f, k. Suppose $f=k!$ and $k>0$. Then there exist natural numbers m, r, s, t, u and there exist natural numbers W, U, S, T, Q and there exists a non trivial natural number M such that $m>0$ and $u>0$ and $r+W+1=\mathtt{y}_{M\cdot(U+1)}(W+1)$ and $(M^{\mathbf{2}}-1)\cdot S^{\mathbf{2}}+1$ is a square and $((M\cdot U)^{\mathbf{2}}-1)\cdot T^{\mathbf{2}}+1$ is a square and $W^{\mathbf{2}}\cdot u^{\mathbf{2}}-(W^{\mathbf{2}}-1)\cdot S\cdot u-1\equiv 0\ (\mathrm{mod}\, Q)$ and $(4\cdot f^{\mathbf{2}}-1)\cdot(r-m\cdot S\cdot T\cdot U)^{\mathbf{2}}+4\cdot u^{\mathbf{2}}\cdot S^{\mathbf{2}}\cdot T^{\mathbf{2}}<8\cdot f\cdot u\cdot S\cdot T\cdot(r-m\cdot S\cdot T\cdot U)$ and $W=100\cdot f\cdot k\cdot(k+1)$ and $U=100\cdot u^3\cdot W^3+1$ and $M=100\cdot m\cdot U\cdot W+1$ and $S=(M-1)\cdot s+k+1$ and $T=(M\cdot U-1)\cdot t+W-k+1$ and $Q=2\cdot M\cdot W-W^{\mathbf{2}}-1$.

PROOF: Set $W=100\cdot f\cdot k\cdot(k+1)$. Set $u=W^k$. Set $U=100\cdot u^3\cdot W^3+1$. Set $I_1=\langle\binom{W}{0}U^0 1^W,\ldots,\binom{W}{W}U^W 1^0\rangle$. Set $I_3=I_1{\restriction}k$. Reconsider $W_2=W-k$ as a natural number. Consider I_2 being a finite sequence such that $I_1=I_3\frown I_2$. For every natural number i such that $i+1\in\operatorname{dom}I_3$ holds $I_3(i+1)=\binom{W}{0+i}\cdot U^{W-'(0+i)}$. $0<\sum I_3<2\cdot W^0\cdot U^{W-'0}$. Set $U_2=\frac{1}{U^{W_2+1}}\cdot I_3$. $\operatorname{rng}U_2\subseteq\mathbb{N}$. Reconsider $Z=\sum U_2$ as an element of $\mathbb{N}$. Set $m=Z$. Set $M=100\cdot m\cdot U\cdot W+1$. Set $m_1=M\cdot(U+1)$. Reconsider $M_3=M\cdot U$ as a non trivial natural number. Set $S=\mathtt{y}_M(k+1)$. Set $T=\mathtt{y}_{M_3}(W_2+1)$. Reconsider $r=\mathtt{y}_{m_1}(W+1)-(W+1)$ as a natural number. Consider s being an integer such that $(M-1)\cdot s=S-(k+1)$.

Consider t being an integer such that $(M_3-1)\cdot t=T-(W_2+1)$. For every natural number i such that $i+1\in\operatorname{dom}I_2$ holds $I_2(i+1)=\binom{W}{k+i}\cdot U^{W-'(k+i)}$. $0<\sum I_2<2\cdot W^k\cdot U^{W-'k}$. Consider θ_1 being a Theta such that $\mathtt{y}_{m_1}(W+1)=(2\cdot m_1)^W\cdot(1+\theta_1\cdot\frac{W}{m_1})$. Reconsider $I=1$ as a Theta. Consider θ_3 being a Theta such that $\mathtt{y}_M(k+1)=(2\cdot M)^k\cdot(1+\theta_3\cdot\frac{k}{M})$. Consider θ_4 being a Theta such that $\mathtt{y}_{M_3}(W_2+1)=(2\cdot M_3)^{W_2}\cdot(1+\theta_4\cdot\frac{W_2}{M_3})$. Consider θ'_3 being a Theta such that $\frac{1}{1+\theta_3\cdot\frac{k}{M}}=1+\theta'_3\cdot 2\cdot\frac{k}{M}$. Consider θ'_4 being a Theta such that $\frac{1}{1+\theta_4\cdot\frac{W_2}{M_3}}=1+\theta'_4\cdot 2\cdot\frac{W_2}{M_3}$. Consider θ_2 being a Theta such that $\theta_1\cdot\frac{W}{m_1}-\frac{W+1}{(2\cdot m_1)^W}=\theta_2\cdot\frac{1}{M}$. Consider θ_5 being a Theta such that $(1+\theta'_3\cdot(2\cdot\frac{k}{M}))\cdot(1+\theta_2\cdot\frac{1}{M})=1+\theta_5\cdot(2\cdot\frac{k}{M}+2\cdot\frac{1}{M})$. Consider θ_6 being a Theta such that $(1+\theta_5\cdot(2\cdot\frac{k}{M}+2\cdot\frac{1}{M}))\cdot(1+\theta'_4\cdot(2\cdot\frac{W_2}{M_3}))=1+\theta_6\cdot(2\cdot\frac{k}{M}+2\cdot\frac{1}{M}+2\cdot(2\cdot\frac{W_2}{M_3}))$. Consider θ_7 being a Theta such that $\theta_6\cdot(2\cdot\frac{k}{M}+2\cdot\frac{1}{M}+2\cdot(2\cdot\frac{W_2}{M_3}))=\theta_7\cdot\frac{5\cdot k}{M}$.

Consider u_1 being a finite sequence of elements of $\mathbb{N}$, y being an element of $\mathbb{N}$ such that $U_2=\langle y\rangle\frown u_1$. Consider θ_8 being a Theta such that $(1+I\cdot\frac{1}{U})^W=1+\theta_8\cdot 2\cdot W\cdot\frac{1}{U}$. Consider θ_9 being a Theta such that

$\theta_7 \cdot (1+\theta_8 \cdot 2 \cdot W \cdot \frac{1}{U}) = \theta_9 \cdot 2$. Consider i_3 being a finite sequence of elements of $\mathbb{R}$, x being an element of $\mathbb{R}$ such that $I_2 = \langle x \rangle \frown i_3$. For every natural number i such that $i+1 \in \operatorname{dom} i_3$ holds $i_3(i+1) = \binom{W}{k+1+i} \cdot U^{W-'(k+1+i)}$. $0 < \sum i_3 < 2 \cdot W^{k+1} \cdot U^{W-'(k+1)}$. Consider θ_{10} being a Theta such that $I \cdot (\frac{1}{U^{W_2}} \cdot (\sum i_3)) = \theta_{10} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U})$. Reconsider $\theta_{12} = \frac{1}{\binom{W}{k}}$ as a Theta.

Consider θ_{11} being a Theta such that $\theta_{10} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U}) + \theta_9 \cdot \frac{U^k \cdot 10 \cdot k}{M} = \theta_{11} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})$. Consider θ'_{13} being a Theta such that $\binom{W}{k} = \frac{W^k}{k!} \cdot (1+\theta'_{13} \cdot \frac{k^{\mathbf{2}}}{W})$. Consider θ_{13} being a Theta such that $\frac{1}{1+\theta'_{13} \cdot \frac{k^{\mathbf{2}}}{W}} = 1+\theta_{13} \cdot 2 \cdot \frac{k^{\mathbf{2}}}{W}$. Consider θ_{14} being a Theta such that $\frac{1}{1+\theta_{12} \cdot \theta_{11} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})} = 1+\theta_{14} \cdot 2 \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})$. Consider θ_{15} being a Theta such that $(1+\theta_{14} \cdot (2 \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M}))) \cdot (1+\theta_{13} \cdot (2 \cdot \frac{k^{\mathbf{2}}}{W})) = 1+\theta_{15} \cdot (2 \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M}) + 2 \cdot (2 \cdot \frac{k^{\mathbf{2}}}{W}))$. Set $R = r - m \cdot S \cdot T \cdot U$. $R \neq 0$. □

(17) Let us consider a non trivial natural number A, natural numbers C, B, and e. Suppose $0 < B$. Suppose $C = \mathtt{y}_A(B)$. Then there exist natural numbers i, j and there exist natural numbers D, E, F, G, H, I such that $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $B \leqslant C$ and $D = (A^{\mathbf{2}} - 1) \cdot C^{\mathbf{2}} + 1$ and $E = 2 \cdot (i+1) \cdot D \cdot (e+1) \cdot C^{\mathbf{2}}$ and $F = (A^{\mathbf{2}} - 1) \cdot E^{\mathbf{2}} + 1$ and $G = A + F \cdot (F - A)$ and $H = B + 2 \cdot j \cdot C$ and $I = (G^{\mathbf{2}} - 1) \cdot H^{\mathbf{2}} + 1$.

PROOF: Set $x = \mathtt{x}_A(B)$. Set $D = x^{\mathbf{2}}$. There exist natural numbers q, i such that $2 \cdot D \cdot (e+1) \cdot C^{\mathbf{2}} \cdot (i+1) = \mathtt{y}_A(q)$ by [1, (14)], [6, (4)]. Consider q, i being natural numbers such that $2 \cdot D \cdot (e+1) \cdot C^{\mathbf{2}} \cdot (i+1) = \mathtt{y}_A(q)$. Set $F = (\mathtt{x}_A(q))^{\mathbf{2}}$. Reconsider $G = A + F \cdot (F - A)$ as a non trivial natural number. Set $H = \mathtt{y}_G(B)$. $H \equiv B \pmod{2 \cdot C}$. Consider j being an integer such that $H - B = 2 \cdot C \cdot j$. □

(18) Let us consider a non trivial natural number A, natural numbers C, B, and a natural number e. Suppose $0 < B$. Let us consider natural numbers i, j, and integers D, E, F, G, H, I. Suppose $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $B \leqslant C$ and $D = (A^{\mathbf{2}} - 1) \cdot C^{\mathbf{2}} + 1$ and $E = 2 \cdot (i+1) \cdot D \cdot (e+1) \cdot C^{\mathbf{2}}$ and $F = (A^{\mathbf{2}} - 1) \cdot E^{\mathbf{2}} + 1$ and $G = A + F \cdot (F - A)$ and $H = B + 2 \cdot j \cdot C$ and $I = (G^{\mathbf{2}} - 1) \cdot H^{\mathbf{2}} + 1$. Then $C = \mathtt{y}_A(B)$.

PROOF: Consider d being a natural number such that $d^{\mathbf{2}} = D$. Consider f being a natural number such that $f^{\mathbf{2}} = F$. Consider i_2 being a natural number such that $i_2{}^{\mathbf{2}} = I$. Consider i_1 being a natural number such that $d = \mathtt{x}_A(i_1)$ and $C = \mathtt{y}_A(i_1)$. Consider n_1 being a natural number such that $f = \mathtt{x}_A(n_1)$ and $E = \mathtt{y}_A(n_1)$. Consider j_1 being a natural number such that $i_2 = \mathtt{x}_G(j_1)$ and $H = \mathtt{y}_G(j_1)$. $\mathtt{y}_G(j_1) \equiv j_1 \pmod{2 \cdot C}$. □

(19) DIOPHANTINE REPRESENTATION OF SOLUTIONS TO PELL'S EQUATION: Let us consider a non trivial natural number A, natural numbers C, B, and e. Suppose $0 < B$. Then $C = \mathtt{y}_A(B)$ if and only if there exist natural numbers i, j and there exist integers D, E, F, G, H, I such that $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $B \leqslant C$ and $D = (A^{\mathbf{2}} - 1) \cdot C^{\mathbf{2}} + 1$ and $E = 2 \cdot (i+1) \cdot D \cdot (e+1) \cdot C^{\mathbf{2}}$ and $F = (A^{\mathbf{2}} - 1) \cdot E^{\mathbf{2}} + 1$ and $G = A + F \cdot (F - A)$ and $H = B + 2 \cdot j \cdot C$ and $I = (G^{\mathbf{2}} - 1) \cdot H^{\mathbf{2}} + 1$. The theorem is a consequence of (17) and (18).

(20) Let us consider a non trivial natural number A, a natural number C, and positive natural numbers B, L. Then $C = \mathtt{y}_A(B)$ if and only if there exist positive natural numbers i, j and there exist integers D, E, F, G, H, I such that $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $B \leqslant C$ and $D = (A^{\mathbf{2}} - 1) \cdot C^{\mathbf{2}} + 1$ and $E = 2 \cdot i \cdot C^{\mathbf{2}} \cdot L \cdot D$ and $F = (A^{\mathbf{2}} - 1) \cdot E^{\mathbf{2}} + 1$ and $G = A + F \cdot (F - A)$ and $H = B + 2 \cdot (j - 1) \cdot C$ and $I = (G^{\mathbf{2}} - 1) \cdot H^{\mathbf{2}} + 1$. The theorem is a consequence of (17) and (18).

3. Prime Diophantine Representation

Now we state the propositions:

(21) Let us consider a natural number k, and a positive natural number L. Suppose $k > 0$. Then $k + 1$ is prime if and only if there exist positive natural numbers f, i, j, m, u and there exist natural numbers r, s, t and there exist integers A, B, C, D, E, F, G, H, I, W, U, M, S, T, Q such that $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $(M^{\mathbf{2}} - 1) \cdot S^{\mathbf{2}} + 1$ is a square and $((M \cdot U)^{\mathbf{2}} - 1) \cdot T^{\mathbf{2}} + 1$ is a square and $W^{\mathbf{2}} \cdot u^{\mathbf{2}} - (W^{\mathbf{2}} - 1) \cdot S \cdot u - 1 \equiv 0 \pmod{Q}$ and $(4 \cdot f^{\mathbf{2}} - 1) \cdot (r - m \cdot S \cdot T \cdot U)^{\mathbf{2}} + 4 \cdot u^{\mathbf{2}} \cdot S^{\mathbf{2}} \cdot T^{\mathbf{2}} < 8 \cdot f \cdot u \cdot S \cdot T \cdot (r - m \cdot S \cdot T \cdot U)$ and $k+1 \mid f+1$ and $A = M \cdot (U+1)$ and $B = W+1$ and $C = r+W+1$ and $D = (A^{\mathbf{2}} - 1) \cdot C^{\mathbf{2}} + 1$ and $E = 2 \cdot i \cdot C^{\mathbf{2}} \cdot L \cdot D$ and $F = (A^{\mathbf{2}} - 1) \cdot E^{\mathbf{2}} + 1$ and $G = A + F \cdot (F - A)$ and $H = B + 2 \cdot (j - 1) \cdot C$ and $I = (G^{\mathbf{2}} - 1) \cdot H^{\mathbf{2}} + 1$ and $W = 100 \cdot f \cdot k \cdot (k+1)$ and $U = 100 \cdot u^3 \cdot W^3 + 1$ and $M = 100 \cdot m \cdot U \cdot W + 1$ and $S = (M - 1) \cdot s + k + 1$ and $T = (M \cdot U - 1) \cdot t + W - k + 1$ and $Q = 2 \cdot M \cdot W - W^{\mathbf{2}} - 1$.

PROOF: If $k + 1$ is prime, then there exist positive natural numbers f, i, j, m, u and there exist natural numbers r, s, t and there exist integers A, B, C, D, E, F, G, H, I, W, U, M, S, T, Q such that $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $(M^{\mathbf{2}} - 1) \cdot S^{\mathbf{2}} + 1$ is a square and $((M \cdot U)^{\mathbf{2}} - 1) \cdot T^{\mathbf{2}} + 1$ is a square and $W^{\mathbf{2}} \cdot u^{\mathbf{2}} - (W^{\mathbf{2}} - 1) \cdot S \cdot u - 1 \equiv 0 \pmod{Q}$ and $(4 \cdot f^{\mathbf{2}} - 1) \cdot (r - m \cdot S \cdot T \cdot U)^{\mathbf{2}} + 4 \cdot u^{\mathbf{2}} \cdot S^{\mathbf{2}} \cdot T^{\mathbf{2}} < 8 \cdot f \cdot u \cdot S \cdot T \cdot (r - m \cdot S \cdot T \cdot U)$ and $k + 1 \mid f + 1$ and $A = M \cdot (U + 1)$ and $B = W + 1$ and $C = r + W + 1$ and $D = (A^{\mathbf{2}} - 1) \cdot C^{\mathbf{2}} + 1$ and $E = 2 \cdot i \cdot C^{\mathbf{2}} \cdot L \cdot D$ and $F = (A^{\mathbf{2}} - 1) \cdot E^{\mathbf{2}} + 1$ and

$G = A+F\cdot(F-A)$ and $H = B+2\cdot(j-1)\cdot C$ and $I = (G^{\mathbf{2}}-1)\cdot H^{\mathbf{2}}+1$ and $W = 100\cdot f\cdot k\cdot(k+1)$ and $U = 100\cdot u^3\cdot W^3+1$ and $M = 100\cdot m\cdot U\cdot W+1$ and $S = (M-1)\cdot s+k+1$ and $T = (M\cdot U-1)\cdot t+W-k+1$ and $Q = 2\cdot M\cdot W - W^{\mathbf{2}}-1$. $C = \mathtt{y}_A(B)$. $f = k!$. □

(22) Let us consider integers a, b, A, B. Suppose a and b are relatively prime. Then $a \mid A$ and $b \mid B$ if and only if $a\cdot b \mid a\cdot B + b\cdot A$.

(23) Diophantine Representation of Prime Numbers with 8 Explicite Unknowns:

Let us consider a natural number k. Suppose $k > 0$. Then $k+1$ is prime if and only if there exist positive natural numbers f, i, j, m, u and there exist natural numbers r, s, t and there exist integers A, B, C, D, E, F, G, H, I, L, W, U, M, S, T, Q such that $D\cdot F\cdot I$ is a square and $(M^{\mathbf{2}}-1)\cdot S^{\mathbf{2}}+1$ is a square and $((M\cdot U)^{\mathbf{2}}-1)\cdot T^{\mathbf{2}}+1$ is a square and $(4\cdot f^{\mathbf{2}}-1)\cdot(r-m\cdot S\cdot T\cdot U)^{\mathbf{2}}+4\cdot u^{\mathbf{2}}\cdot S^{\mathbf{2}}\cdot T^{\mathbf{2}} < 8\cdot f\cdot u\cdot S\cdot T\cdot(r-m\cdot S\cdot T\cdot U)$ and $F\cdot L \mid (H-C)\cdot L+F\cdot(f+1)\cdot Q+F\cdot(k+1)\cdot((W^{\mathbf{2}}-1)\cdot S\cdot u-W^{\mathbf{2}}\cdot u^{\mathbf{2}}+1)$ and $A = M\cdot(U+1)$ and $B = W+1$ and $C = r+W+1$ and $D = (A^{\mathbf{2}}-1)\cdot C^{\mathbf{2}}+1$ and $E = 2\cdot i\cdot C^{\mathbf{2}}\cdot L\cdot D$ and $F = (A^{\mathbf{2}}-1)\cdot E^{\mathbf{2}}+1$ and $G = A+F\cdot(F-A)$ and $H = B+2\cdot(j-1)\cdot C$ and $I = (G^{\mathbf{2}}-1)\cdot H^{\mathbf{2}}+1$ and $L = (k+1)\cdot Q$ and $W = 100\cdot f\cdot k\cdot(k+1)$ and $U = 100\cdot u^3\cdot W^3+1$ and $M = 100\cdot m\cdot U\cdot W+1$ and $S = (M-1)\cdot s+k+1$ and $T = (M\cdot U-1)\cdot t+W-k+1$ and $Q = 2\cdot M\cdot W-W^{\mathbf{2}}-1$.

Proof: If $k+1$ is prime, then there exist positive natural numbers f, i, j, m, u and there exist natural numbers r, s, t and there exist integers A, B, C, D, E, F, G, H, I, L, W, U, M, S, T, Q such that $D\cdot F\cdot I$ is a square and $(M^{\mathbf{2}}-1)\cdot S^{\mathbf{2}}+1$ is a square and $((M\cdot U)^{\mathbf{2}}-1)\cdot T^{\mathbf{2}}+1$ is a square and $(4\cdot f^{\mathbf{2}}-1)\cdot(r-m\cdot S\cdot T\cdot U)^{\mathbf{2}}+4\cdot u^{\mathbf{2}}\cdot S^{\mathbf{2}}\cdot T^{\mathbf{2}} < 8\cdot f\cdot u\cdot S\cdot T\cdot(r-m\cdot S\cdot T\cdot U)$ and $F\cdot L \mid (H-C)\cdot L+F\cdot(f+1)\cdot Q+F\cdot(k+1)\cdot((W^{\mathbf{2}}-1)\cdot S\cdot u-W^{\mathbf{2}}\cdot u^{\mathbf{2}}+1)$ and $A = M\cdot(U+1)$ and $B = W+1$ and $C = r+W+1$ and $D = (A^{\mathbf{2}}-1)\cdot C^{\mathbf{2}}+1$ and $E = 2\cdot i\cdot C^{\mathbf{2}}\cdot L\cdot D$ and $F = (A^{\mathbf{2}}-1)\cdot E^{\mathbf{2}}+1$ and $G = A+F\cdot(F-A)$ and $H = B+2\cdot(j-1)\cdot C$ and $I = (G^{\mathbf{2}}-1)\cdot H^{\mathbf{2}}+1$ and $L = (k+1)\cdot Q$ and $W = 100\cdot f\cdot k\cdot(k+1)$ and $U = 100\cdot u^3\cdot W^3+1$ and $M = 100\cdot m\cdot U\cdot W+1$ and $S = (M-1)\cdot s+k+1$ and $T = (M\cdot U-1)\cdot t+W-k+1$ and $Q = 2\cdot M\cdot W-W^{\mathbf{2}}-1$ by [9, (22)], (16).

$F \mid H-C$ and $Q\cdot(k+1) \mid (f+1)\cdot Q+(k+1)\cdot((W^{\mathbf{2}}-1)\cdot S\cdot u-W^{\mathbf{2}}\cdot u^{\mathbf{2}}+1)$. $Q \mid (W^{\mathbf{2}}-1)\cdot S\cdot u-W^{\mathbf{2}}\cdot u^{\mathbf{2}}+1$ and $k+1 \mid f+1$. $C = \mathtt{y}_A(B)$. $f = k!$. □

References

[1] Marcin Acewicz and Karol Pąk. Pell's equation. *Formalized Mathematics*, 25(**3**):197–204, 2017. doi:10.1515/forma-2017-0019.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Ma-

tuszewski, 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.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[4] James P. Jones, Sato Daihachiro, Hideo Wada, and Douglas Wiens. Diophantine representation of the set of prime numbers. *The American Mathematical Monthly*, 83(6):449–464, 1976.

[5] Yuri Matiyasevich. Primes are nonnegative values of a polynomial in 10 variables. *Journal of Soviet Mathematics*, 15:33–44, 1981. doi:10.1007/BF01404106.

[6] Karol Pąk. The Matiyasevich theorem. Preliminaries. *Formalized Mathematics*, 25(**4**): 315–322, 2017. doi:10.1515/forma-2017-0029.

[7] Karol Pąk. Prime representing polynomial. *Formalized Mathematics*, 29(**4**):221–228, 2021. doi:10.2478/forma-2021-0020.

[8] Karol Pąk and Cezary Kaliszyk. Formalizing a diophantine representation of the set of prime numbers. In June Andronick and Leonardo de Moura, editors, *13th International Conference on Interactive Theorem Proving, ITP 2022, August 7-10, 2022, Haifa, Israel*, volume 237 of *LIPIcs*, pages 26:1–26:8. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. doi:10.4230/LIPIcs.ITP.2022.26.

[9] Marco Riccardi. The perfect number theorem and Wilson's theorem. *Formalized Mathematics*, 17(**2**):123–128, 2009. doi:10.2478/v10037-009-0013-y.

[10] Zhi-Wei Sun. Further results on Hilbert's Tenth Problem. *Science China Mathematics*, 64:281–306, 2021. doi:10.1007/s11425-020-1813-5.

Accepted December 27, 2022

FORMALIZED MATHEMATICS
Vol. **30**, No. **4**, Pages 255–279, **2022**
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0021

sciendo
sciendo.com/journal/forma

Prime Representing Polynomial with 10 Unknowns

Karol Pąk
Institute of Computer Science
University of Białystok
Poland

Summary. In this article we formalize in Mizar [1], [2] the final step of our attempt to formally construct a prime representing polynomial with 10 variables proposed by Yuri Matiyasevich in [4].

The first part of the article includes many auxiliary lemmas related to multivariate polynomials. We start from the properties of monomials, among them their evaluation as well as the power function on polynomials to define the substitution for multivariate polynomials. For simplicity, we assume that a polynomial and substituted ones as i-th variable have the same number of variables. Then we study the number of variables that are used in given multivariate polynomials. By the used variable we mean a variable that is raised at least once to a non-zero power. We consider both adding unused variables and eliminating them.

The second part of the paper deals with the construction of the polynomial proposed by Yuri Matiyasevich. First, we introduce a diophantine polynomial over 4 variables that has roots in integers if and only if indicated variable is the square of a natural number, and another two is the square of an odd natural number. We modify the polynomial by adding two variables in such a way that the root additionally requires the divisibility of these added variables. Then we modify again the polynomial by adding two variables to also guarantee the non-negativity condition of one of these variables. Finally, we combine the prime diophantine representation proved in [7] with the obtained polynomial constructing a prime representing polynomial with 10 variables. This work has been partially presented in [8] with the obtained polynomial constructing a prime representing polynomial with 10 variables in Theorem (85).

MSC: 11D45 68V20

Keywords: polynomial reduction; prime representing polynomial

MML identifier: POLYNOM9, version: 8.1.12 5.72.1435

1. Preliminaries

From now on i, j, k, n, m denote natural numbers, X denotes a set, b, s denote bags of X, and x denotes an object. Now we state the propositions:

(1) Let us consider an integer i. Then $i \star \mathbf{1}_{\mathbb{C}_{\mathrm{F}}} = i$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \$_1 \star \mathbf{1}_{\mathbb{C}_{\mathrm{F}}} = \$_1$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$ by [9, (62),(60)]. $\mathcal{P}[n]$. Consider k being a natural number such that $i = k$ or $i = -k$. $\square$

(2) Let us consider complex numbers z_1, z_2. Suppose $\Re(z_1) \geqslant 0$ and $\Re(z_2) \geqslant 0$ and $\Im(z_1) \geqslant 0$ and $\Im(z_2) \geqslant 0$ and $z_1{}^{\mathbf{2}} = z_2{}^{\mathbf{2}}$ and $z_1{}^{\mathbf{2}}$ is a real number. Then $z_1 = z_2$.

(3) Let us consider integers a, b. If $a^{\mathbf{2}} \mid b^{\mathbf{2}}$, then $a \mid b$.

(4) Let us consider a positive natural number m. Then $\overline{\overline{2^{(\mathrm{Seg}\,m)\setminus\{1\}}}} = 2^{m -' 1}$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \overline{\overline{2^{(\mathrm{Seg}(1+\$_1))\setminus\{1\}}}} = 2^{\$_1}$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. $\square$

(5) Let us consider an ordinal number n, and a finite subset A of n. Then $\subseteq_n$ linearly orders A.

(6) Let us consider an element x of $\mathbb{R}_{\mathrm{F}}$. Suppose $x \neq 0_{\mathbb{R}_{\mathrm{F}}}$.
Then $\mathrm{power}_{\mathbb{R}_{\mathrm{F}}}(x, n) \neq 0_{\mathbb{R}_{\mathrm{F}}}$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \mathrm{power}_{\mathbb{R}_{\mathrm{F}}}(x, \$_1) \neq 0_{\mathbb{R}_{\mathrm{F}}}$. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. $\square$

2. More on Bags

Let us consider a bag b of X. Now we state the propositions:

(7) $\mathrm{support}(n \cdot b) \subseteq \mathrm{support}\, b$.

(8) If $n \neq 0$, then $\mathrm{support}(n \cdot b) = \mathrm{support}\, b$. The theorem is a consequence of (7).

(9) $\mathrm{support}(b +\cdot (x, n)) \subseteq \{x\} \cup \mathrm{support}\, b$.

Let X be a set, b be a bag of X, and n be a natural number. Observe that $n \cdot b$ is finite-support. Let x be an object. One can check that $b +\cdot (x, n)$ is finite-support. Now we state the propositions:

(10) Let us consider a bag b of X. Then $0 \cdot b = \mathrm{EmptyBag}\, X$.

(11) Let us consider an ordinal number n, a right zeroed, add-associative, right complementable, well unital, distributive, Abelian, non trivial, commutative, associative, non empty double loop structure L, a function x from n into L, a bag b of n, and a natural number i. If $i \neq 0$, then $\mathrm{eval}(i \cdot b, x) = \mathrm{power}_L(\mathrm{eval}(b, x), i)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \neq 0$, then $\mathrm{eval}(\$_1 \cdot b, x) = \mathrm{power}_L(\mathrm{eval}(b, x), \$_1)$. If $\mathcal{P}[j]$, then $\mathcal{P}[j+1]$. $\mathcal{P}[j]$. $\square$

(12) Let us consider a non empty set X, an element x of X, and an element i of $\mathbb{N}$. Then $\mathrm{EmptyBag}\, X +\cdot (x, i) = (\{x\}, i)$-bag.

(13) Let us consider a set X, x, and i. Suppose $x \in X$ and $i \neq 0$. Then $\mathrm{support}(\mathrm{EmptyBag}\, X +\cdot (x, i)) = \{x\}$. The theorem is a consequence of (12).

(14) Let us consider an ordinal number n, a well unital, non trivial double loop structure L, and a function y from n into L. Suppose $x \in n$. Then $\mathrm{eval}(\mathrm{EmptyBag}\, n +\cdot (x, i), y) = \mathrm{power}_L(y(x), i)$. The theorem is a consequence of (13).

Let us consider a bag b of X. Now we state the propositions:

(15) $b = (b +\cdot (x, 0)) + (\mathrm{EmptyBag}\, X +\cdot (x, b(x)))$.
PROOF: Set $E = \mathrm{EmptyBag}\, X$. Set $b_5 = b +\cdot (x, 0)$. Set $E_6 = E +\cdot (x, b(x))$. For every object y such that $y \in \mathrm{dom}\, b$ holds $b(y) = (b_5 + E_6)(y)$. $\square$

(16) $\mathrm{support}(b +\cdot (x, 0)) = (\mathrm{support}\, b) \setminus \{x\}$.
PROOF: $\mathrm{support}(b +\cdot (x, 0)) \subseteq (\mathrm{support}\, b) \setminus \{x\}$. $\square$

(17) Let us consider an ordinal number n, a right zeroed, add-associative, right complementable, well unital, distributive, Abelian, non trivial, commutative, associative, non empty double loop structure L, a function x from n into L, a bag b of n, an object i, and a natural number j. Suppose $i \in n$. Then $(\mathrm{eval}(b +\cdot (i, j), x)) \cdot \mathrm{power}_L(x_{/i}, b(i)) = (\mathrm{eval}(b, x)) \cdot \mathrm{power}_L(x_{/i}, j)$. The theorem is a consequence of (15) and (14).

Let A, B be sets, f be a function from A into B, x be an object, and b be an element of B. Observe that the functor $f +\cdot (x, b)$ yields a function from A into B. Now we state the propositions:

(18) Let us consider an ordinal number n, a well unital, non trivial double loop structure L, a bag b of n, a function f from n into L, and an element u of L. If $b(x) = 0$, then $\mathrm{eval}(b, f +\cdot (x, u)) = \mathrm{eval}(b, f)$.
PROOF: Set $S = \mathrm{SgmX}(\subseteq_n, \mathrm{support}\, b)$. Set $f_6 = f +\cdot (x, u)$. Consider y being a finite sequence of elements of L such that $\mathrm{len}\, y = \mathrm{len}\, S$ and $\mathrm{eval}(b, f_6) = \prod y$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y$ holds $y_{/i} = \mathrm{power}_L(f_6 \cdot S_{/i}, b \cdot S_{/i})$. For every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y$ holds $y_{/i} = \mathrm{power}_L(f \cdot S_{/i}, b \cdot S_{/i})$. $\square$

(19) Let us consider a natural number n, a bag b of n, and i. If $b(i) = \mathrm{degree}(b)$, then $b = \mathrm{EmptyBag}\, n +\cdot (i, b(i))$. The theorem is a consequence of (15) and (13).

(20) Let us consider a set X, and bags b_1, b_2 of X. Suppose $2 \cdot b_1 +\cdot (0, b_1(0)) =$

$2 \cdot b_2 +\cdot (0, b_2(0))$. Then $b_1 = b_2$.

PROOF: For every x such that $x \in X$ holds $b_1(x) = b_2(x)$. □

(21) Let us consider a set X, and a bag b of X. Then $\mathrm{support}(2 \cdot b +\cdot (0, b(0))) = \mathrm{support}\, b$.

PROOF: $\mathrm{support}(2 \cdot b +\cdot (0, b(0))) \subseteq \mathrm{support}\, b$. $\mathrm{support}\, b \subseteq \mathrm{support}(2 \cdot b +\cdot (0, b(0)))$. □

(22) Let us consider a bag b of X. Then $b +\cdot (x, i + k) = (b +\cdot (x, i)) + (\mathrm{EmptyBag}\, X +\cdot (x, k))$.

PROOF: Set $E_3 = \mathrm{EmptyBag}\, X$. For every object y such that $y \in X$ holds $(b +\cdot (x, i + k))(y) = ((b +\cdot (x, i)) + (E_3 +\cdot (x, k)))(y)$. □

(23) Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure L, an element a of L, and a bag b of X. Then $\mathrm{Monom}(-a, b) = -\mathrm{Monom}(a, b)$.

PROOF: If $x \in \mathrm{Bags}\, X$, then $(\mathrm{Monom}(-a, b))(x) = (-\mathrm{Monom}(a, b))(x)$. □

(24) Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure L, elements a_1, a_2 of L, and a bag b of X. Then $\mathrm{Monom}(a_1, b) + \mathrm{Monom}(a_2, b) = \mathrm{Monom}(a_1 + a_2, b)$.

PROOF: If $x \in \mathrm{Bags}\, X$, then $(\mathrm{Monom}(a_1, b) + \mathrm{Monom}(a_2, b))(x) = (\mathrm{Monom}(a_1 + a_2, b))(x)$. □

(25) Let us consider a non empty zero structure L, and a bag b of X. Then $\mathrm{Monom}(0_L, b) = 0_X L$.

PROOF: If $x \in \mathrm{Bags}\, X$, then $(\mathrm{Monom}(0_L, b))(x) = (0_X L)(x)$. □

(26) Let us consider an ordinal number O, a right zeroed, add-associative, right complementable, right unital, distributive, non trivial double loop structure R, a polynomial p of O,R, and a bag b of O. Then $\mathrm{Support}(p - \mathrm{Monom}(p(b), b)) = (\mathrm{Support}\, p) \setminus \{b\}$. The theorem is a consequence of (25).

(27) Let us consider a natural number n, and an object p. Suppose $p \in n$. Let us consider an integer element i of $\mathbb{R}_{\mathrm{F}}$, and a function x from n into $\mathbb{R}_{\mathrm{F}}$. Then $\mathrm{eval}(\mathrm{Monom}(i, \mathrm{EmptyBag}\, n +\cdot (p, 1)), x) = i \cdot (x_{/p})$. The theorem is a consequence of (14).

Let X be a set, b be a bag of X, and i be an integer element of $\mathbb{R}_{\mathrm{F}}$. One can check that $\mathrm{Monom}(i, b)$ is $\mathbb{Z}$-valued.

3. Power of Multivariate Polynomial

From now on O denotes an ordinal number, R denotes a right zeroed, add-associative, right complementable, right unital, distributive, non trivial double loop structure, and p denotes a polynomial of O,R.

Let n be an ordinal number, R be a right zeroed, add-associative, right complementable, right unital, distributive, non trivial double loop structure,

p be a polynomial of n,R, and k be a natural number. The functor p^k yielding a polynomial of n,R is defined by the term

(Def. 1) $\mathrm{power}_{\mathrm{PolyRing}(n,R)}(p, k)$.

Now we state the propositions:

(28) If R is well unital, then $p^0 = 1\_(O, R)$ and $p^1 = p$.
PROOF: Set $P_7 = \mathrm{PolyRing}(O, R)$. Reconsider $E = 1\_(O, R)$ as an element of P_7. For every element H of P_7, $H \cdot E = H$ and $E \cdot H = H$. P_7 is unital. □

(29) $p^{n+1} = p^n * p$.

(30) Let us consider an Abelian, well unital, commutative, associative, right zeroed, add-associative, right complementable, right unital, distributive, non trivial double loop structure R, a polynomial p of O,R, and a function f from O into R. Then $\mathrm{eval}(p^k, f) = \mathrm{power}_R(\mathrm{eval}(p, f), k)$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \mathrm{eval}(p^{\$_1}, f) = \mathrm{power}_R(\mathrm{eval}(p, f), \$_1)$. $\mathrm{eval}(p^0, f) = \mathrm{eval}(1\_(O, R), f)$. If $\mathcal{P}[n]$, then $\mathcal{P}[n + 1]$. $\mathcal{P}[n]$. □

Let O be an ordinal number, p be a $\mathbb{Z}$-valued polynomial of O,$\mathbb{R}_{\mathrm{F}}$, and n be a natural number. Observe that p^n is $\mathbb{Z}$-valued.

4. SUBSTITUTION IN MULTIVARIATE POLYNOMIALS

Let X be a set, b, s be bags of X, and x be an object. The functor $\mathrm{Subst}(b, x, s)$ yielding a bag of X is defined by the term

(Def. 2) $(b +\cdot (x, 0)) + s$.

Now we state the propositions:

(31) $\mathrm{support}\,\mathrm{Subst}(b, x, s) = (\mathrm{support}\, b) \setminus \{x\} \cup \mathrm{support}\, s$. The theorem is a consequence of (16).

(32) Let us consider bags s_1, s_2, b of X. If $\mathrm{Subst}(b, x, s_1) = \mathrm{Subst}(b, x, s_2)$, then $s_1 = s_2$.

Let X be an ordinal number, L be a right zeroed, add-associative, right complementable, right unital, distributive, non trivial double loop structure, t be a bag of X, p be a polynomial of X,L, and x be an object. The functor $\mathrm{Subst}(t, x, p)$ yielding a series of X, L is defined by

(Def. 3) for every bag b of X, if there exists a bag s of X such that $b = \mathrm{Subst}(t, x, s)$, then for every bag s of X such that $b = \mathrm{Subst}(t, x, s)$ holds $it(b) = (p^{t(x)})(s)$ and if for every bag s of X, $b \neq \mathrm{Subst}(t, x, s)$, then $it(b) = 0_L$.

In the sequel O denotes an ordinal number, R denotes a right zeroed, add-associative, right complementable, right unital, distributive, non trivial double loop structure, and p denotes a polynomial of O,R.

Now we state the propositions:

(33) Let us consider bags t, s of O. Then $(\mathrm{Subst}(t,x,p))(\mathrm{Subst}(t,x,s)) = (p^{t(x)})(s)$.

(34) Let us consider a bag t of O, and a one-to-one finite sequence o_1 of elements of Bags O. Suppose $\mathrm{rng}\, o_1 = \mathrm{Support}\, p^{t(x)}$. Then there exists a one-to-one finite sequence o_2 of elements of Bags O such that

(i) $\mathrm{rng}\, o_2 = \mathrm{Support}\,\mathrm{Subst}(t,x,p)$, and

(ii) $\mathrm{len}\, o_2 = \mathrm{len}\, o_1$, and

(iii) for every j such that $1 \leqslant j \leqslant \mathrm{len}\, o_2$ holds $o_2(j) = \mathrm{Subst}(t,x,o_{1/j})$.

Proof: Set $S = \mathrm{Subst}(t,x,p)$. Define $\mathcal{O}(\text{object}) = \mathrm{Subst}(t,x,o_{1/\$_1})$. Consider o_2 being a finite sequence such that $\mathrm{len}\, o_2 = \mathrm{len}\, o_1$ and for every k such that $k \in \mathrm{dom}\, o_2$ holds $o_2(k) = \mathcal{O}(k)$. $\mathrm{rng}\, o_2 \subseteq \mathrm{Support}\, S$. $\mathrm{Support}\, S \subseteq \mathrm{rng}\, o_2$. o_2 is one-to-one. □

Let O be an ordinal number, R be a right zeroed, add-associative, right complementable, right unital, distributive, non trivial double loop structure, t be a bag of O, p be a polynomial of O,R, and x be an object. Let us note that $\mathrm{Subst}(t,x,p)$ is finite-Support.

Now we state the proposition:

(35) Let us consider a commutative, associative, Abelian, right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure R, a bag t of O, a polynomial p of O,R, an object i, and a function x from O into R. Suppose $i \in O$. Then $\mathrm{eval}(\mathrm{Subst}(t,i,p),x) = \mathrm{eval}(t, x +\cdot (i, \mathrm{eval}(p,x)))$.

Proof: Set $x_4 = x +\cdot (i, \mathrm{eval}(p,x))$. Set $P = p^{t(i)}$. Set $t_0 = t +\cdot (i,0)$. Set $S_7 = \mathrm{SgmX}(\mathrm{BagOrder}\, O, \mathrm{Support}\, P)$. Set $S_{13} = \mathrm{Subst}(t,i,p)$. Consider y being a finite sequence of elements of R such that $\mathrm{len}\, y = \mathrm{len}\, S_7$ and $\mathrm{eval}(P,x) = \sum y$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y$ holds $y_{/i} = P \cdot S_{7/i} \cdot (\mathrm{eval}(S_{7/i},x))$. Consider t_2 being a one-to-one finite sequence of elements of Bags O such that $\mathrm{rng}\, t_2 = \mathrm{Support}\, S_{13}$ and $\mathrm{len}\, t_2 = \mathrm{len}\, S_7$ and for every j such that $1 \leqslant j \leqslant \mathrm{len}\, t_2$ holds $t_2(j) = \mathrm{Subst}(t,i,S_{7/j})$. Consider Y being a finite sequence of elements of R such that $\mathrm{len}\, Y = \overline{\overline{\mathrm{Support}\, S_{13}}}$ and $\mathrm{eval}(S_{13},x) = \sum Y$ and for every natural number i such that $1 \leqslant i \leqslant \mathrm{len}\, Y$ holds $Y_{/i} = S_{13} \cdot t_{2/i} \cdot (\mathrm{eval}(t_{2/i},x))$. $\mathrm{eval}(P,x) = \mathrm{power}_R(\mathrm{eval}(p,x), t(i))$. For every j such that $1 \leqslant j \leqslant \mathrm{len}\, Y$ holds $Y(j) = (y \cdot (\mathrm{eval}(t_0,x)))(j)$. $(\mathrm{eval}(t_0,x_4)) \cdot \mathrm{power}_R(x_{4/i}, t(i)) = (\mathrm{eval}(t,x_4)) \cdot (1_R)$. □

Let X be a set, L be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure, p be a finite-Support series of X, L, and a be an element of L. One can verify that $a \cdot p$ is finite-Support.

Let X be an ordinal number, L be a right zeroed, add-associative, right complementable, right unital, well unital, distributive, non trivial double loop structure, p, s be polynomials of X,L, and x be an object. The functor $\mathrm{Subst}(p, x, s)$ yielding a polynomial of X,L is defined by

(Def. 4) there exists a finite sequence S of elements of $\mathrm{PolyRing}(X, L)$ such that $it = \sum S$ and $\mathrm{len}\,\mathrm{SgmX}(\mathrm{BagOrder}\,X, \mathrm{Support}\,p) = \mathrm{len}\,S$ and for every i such that $i \in \mathrm{dom}\,S$ holds $S(i) = p((\mathrm{SgmX}(\mathrm{BagOrder}\,X, \mathrm{Support}\,p))_{/i}) \cdot (\mathrm{Subst}((\mathrm{SgmX}(\mathrm{BagOrder}\,X, \mathrm{Support}\,p))_{/i}, x, s))$.

Let O be an ordinal number, t be a bag of O, and p be a $\mathbb{Z}$-valued polynomial of O,$\mathbb{R}_{\mathrm{F}}$. Let us observe that $\mathrm{Subst}(t, x, p)$ is $\mathbb{Z}$-valued.

Let p, s be $\mathbb{Z}$-valued polynomials of O,$\mathbb{R}_{\mathrm{F}}$. Observe that $\mathrm{Subst}(p, x, s)$ is $\mathbb{Z}$-valued.

Now we state the propositions:

(36) Let us consider an ordinal number O, a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, non trivial double loop structure L, a polynomial p of O,L, a function x from O into L, and a finite sequence P of elements of $\mathrm{PolyRing}(O, L)$. Suppose $p = \sum P$. Let us consider a finite sequence E of elements of L. Suppose $\mathrm{len}\,E = \mathrm{len}\,P$ and for every polynomial s of O,L and for every i such that $i \in \mathrm{dom}\,E$ and $s = P(i)$ holds $E(i) = \mathrm{eval}(s, x)$. Then $\mathrm{eval}(p, x) = \sum E$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every natural number i such that $\$_1 = i$ and $i \leqslant \mathrm{len}\,P$ for every polynomial q of O,L such that $q = \sum(P{\restriction}i)$ holds $\sum(E{\restriction}i) = \mathrm{eval}(q, x)$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. $\square$

(37) Let us consider a commutative, associative, Abelian, right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure R, polynomials p, s of O,R, an object i, and a function x from O into R. Suppose $i \in O$. Then $\mathrm{eval}(\mathrm{Subst}(p, i, s), x) = \mathrm{eval}(p, x +\cdot (i, \mathrm{eval}(s, x)))$.
Proof: Set $x_4 = x +\cdot (i, \mathrm{eval}(s, x))$. Set $B = \mathrm{SgmX}(\mathrm{BagOrder}\,O, \mathrm{Support}\,p)$. Consider f being a finite sequence of elements of R such that $\mathrm{len}\,f = \mathrm{len}\,B$ and $\mathrm{eval}(p, x_4) = \sum f$ and for every element j of $\mathbb{N}$ such that $1 \leqslant j \leqslant \mathrm{len}\,f$ holds $f_{/j} = p \cdot B_{/j} \cdot (\mathrm{eval}(B_{/j}, x_4))$. Consider S being a finite sequence of elements of $\mathrm{PolyRing}(O, R)$ such that $\mathrm{Subst}(p, i, s) = \sum S$ and $\mathrm{len}\,B = \mathrm{len}\,S$ and for every j such that $j \in \mathrm{dom}\,S$ holds $S(j) = p(B_{/j}) \cdot (\mathrm{Subst}(B_{/j}, i, s))$. For every polynomial q of O,R and for every j such that $j \in \mathrm{dom}\,f$ and $q = S(j)$ holds $f(j) = \mathrm{eval}(q, x)$. $\square$

5. Set of Variables Used in Multivariate Polynomial

Let X be a set, S be a zero structure, and p be a series of X, S. The functor vars(p) yielding a subset of X is defined by

(Def. 5) for every object x, $x \in it$ iff there exists a bag b of X such that $b \in \mathrm{Support}\, p$ and $b(x) \neq 0$.

Now we state the propositions:

(38) Let us consider an ordinal number X, a non empty zero structure S, and a series p of X, S. Then $\mathrm{vars}(p) = \emptyset$ if and only if p is constant.

(39) Let us consider a set X, a zero structure S, and a series p of X, S. Then $\mathrm{vars}(p) = \bigcup\{\mathrm{support}\, b$, where b is an element of $\mathrm{Bags}\, X : b \in \mathrm{Support}\, p\}$.

(40) Let us consider a set X, a zero structure S, a series p of X, S, and a bag b of X. If $b \in \mathrm{Support}\, p$, then $\mathrm{support}\, b \subseteq \mathrm{vars}(p)$. The theorem is a consequence of (39).

Let X be an ordinal number, S be a non empty zero structure, and p be a polynomial of X,S. Let us observe that vars(p) is finite.

Now we state the propositions:

(41) Let us consider a set X, a right zeroed, non empty additive loop structure S, and series p, q of X, S. Then $\mathrm{vars}(p+q) \subseteq \mathrm{vars}(p) \cup \mathrm{vars}(q)$.

(42) Let us consider a set X, an add-associative, right zeroed, right complementable, non empty additive loop structure S, and a series p of X, S. Then $\mathrm{vars}(p) = \mathrm{vars}(-p)$.

Proof: $\mathrm{vars}(p) \subseteq \mathrm{vars}(-p)$. Consider b being a bag of X such that $b \in \mathrm{Support}(-p)$ and $b(x) \neq 0$. □

(43) Let us consider an ordinal number X, an add-associative, right complementable, right zeroed, right unital, distributive, non empty double loop structure S, and polynomials p, q of X,S. Then $\mathrm{vars}(p * q) \subseteq \mathrm{vars}(p) \cup \mathrm{vars}(q)$.

(44) Let us consider a set X, an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure S, a series p of X, S, and an element a of S. Then $\mathrm{vars}(a \cdot p) \subseteq \mathrm{vars}(p)$.

(45) Let us consider an ordinal number X, a right zeroed, add-associative, right complementable, right unital, distributive, well unital, non trivial double loop structure S, a polynomial p of X,S, and a natural number k. Then $\mathrm{vars}(p^k) \subseteq \mathrm{vars}(p)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \mathrm{vars}(p^{\$_1}) \subseteq \mathrm{vars}(p)$. $p^0 = 1\_(X, S)$. $\mathrm{vars}(p^0) = \emptyset$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(46) Let us consider an ordinal number X, a right zeroed, add-associative, right complementable, right unital, distributive, well unital, non trivial double loop structure S, a polynomial p of X,S, and a bag t of X. Then $\mathrm{vars}(\mathrm{Subst}(t, x, p)) \subseteq (\mathrm{support}\, t) \setminus \{x\} \cup \mathrm{vars}(p)$. The theorem is a consequence of (45).

(47) Let us consider an ordinal number X, a right zeroed, add-associative, right complementable, right unital, distributive, well unital, non trivial double loop structure S, and polynomials p, s of X,S.
Then $\mathrm{vars}(\mathrm{Subst}(p, x, s)) \subseteq (\mathrm{vars}(p)) \setminus \{x\} \cup \mathrm{vars}(s)$.
Proof:
Set $P_7 = \mathrm{PolyRing}(X, S)$. Set $S_{11} = \mathrm{SgmX}(\mathrm{BagOrder}\, X, \mathrm{Support}\, p)$. Consider F being a finite sequence of elements of P_7 such that $\mathrm{Subst}(p, x, s) = \sum F$ and $\mathrm{len}\, S_{11} = \mathrm{len}\, F$ and for every i such that $i \in \mathrm{dom}\, F$ holds $F(i) = p(S_{11/i}) \cdot (\mathrm{Subst}(S_{11/i}, x, s))$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every natural number i such that $i = \$_1$ and $i \leqslant \mathrm{len}\, F$ for every polynomial q of X,S such that $q = \sum(F \restriction i)$ holds $\mathrm{vars}(q) \subseteq (\mathrm{vars}(p)) \setminus \{x\} \cup \mathrm{vars}(s)$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n + 1]$. $\mathcal{P}[n]$. □

(48) Let us consider a set X, a non empty zero structure S, and an element s of S. Then $\mathrm{vars}(\mathrm{Monom}(s, \mathrm{EmptyBag}\, X +\cdot (x, n))) \subseteq \{x\}$.

6. Polynomial Without the Last Variable

Let n be a natural number, L be a non empty zero structure, and p be a series of $n + 1$, L. The functor p-removed_last yielding a series of n, L is defined by

(Def. 6) for every bag b of n, $it(b) = p(b$ extended by $0)$.

Let p be a polynomial of $n + 1$,L. One can check that p-removed_last is finite-Support. Now we state the propositions:

(49) Let us consider a natural number n, a non empty zero structure L, and a series p of n, L. Then (the p extended by 0)-removed_last $= p$.
Proof: Set $e_0 =$ the p extended by 0. For every element a of $\mathrm{Bags}\, n$, $p(a) = (e_0\text{-removed\_last})(a)$ by [5, (6)]. □

(50) Let us consider a natural number n, a non empty zero structure L, and a series p of $n + 1$, L. Suppose $n \notin \mathrm{vars}(p)$. Then the p-removed_last extended by $0 = p$.
Proof: Set $r = p$-removed_last. For every element a of $\mathrm{Bags}(n+1)$, $p(a) =$ (the r extended by $0)(a)$. □

(51) Let us consider a natural number n, a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure L, a polynomial p of $n + 1$,L, a function x from n into L, and

a function y from $n+1$ into L. Suppose $n \notin \mathrm{vars}(p)$ and $y \restriction n = x$. Then $\mathrm{eval}(p\text{-removed\_last}, x) = \mathrm{eval}(p, y)$. The theorem is a consequence of (50).

(52) Let us consider a natural number n, a non empty zero structure L, and a series p of $n+1$, L. Then $\mathrm{vars}(p\text{-removed\_last}) \subseteq (\mathrm{vars}(p)) \setminus \{n\}$.

(53) Let us consider an ordinal number X, a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure S, a polynomial p of X,S, an object i, and a function x from X into S. Suppose $i \in X \setminus (\mathrm{vars}(p))$. Let us consider an element s of S. Then $\mathrm{eval}(p, x) = \mathrm{eval}(p, x +\cdot (i, s))$.

PROOF: Set $x_9 = x +\cdot (o, s)$. Set $S_4 = \mathrm{SgmX}(\mathrm{BagOrder}\, X, \mathrm{Support}\, p)$. Consider y being a finite sequence of elements of the carrier of S such that $\mathrm{len}\, y = \mathrm{len}\, S_4$ and $\mathrm{eval}(p, x) = \sum y$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y$ holds $y_{/i} = p \cdot S_{4/i} \cdot (\mathrm{eval}(S_{4/i}, x))$. Consider y_3 being a finite sequence of elements of the carrier of S such that $\mathrm{len}\, y_3 = \mathrm{len}\, S_4$ and $\mathrm{eval}(p, x_9) = \sum y_3$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y_3$ holds $y_{3/i} = p \cdot S_{4/i} \cdot (\mathrm{eval}(S_{4/i}, x_9))$. For every natural number i such that $1 \leqslant i \leqslant \mathrm{len}\, S_4$ holds $y(i) = y_3(i)$. $\square$

7. Square Root Function – Some Generalization

Let n be an ordinal number, x be an object, A be a finite subset of n, and f be a real-valued function. The functor $f(x) + \sqrt[\mathbb{C}]{f(A_1)} + \sqrt[\mathbb{C}]{f(A_2)} + \ldots$ yielding a finite sequence of elements of $\mathbb{C}_{\mathrm{F}}$ is defined by

(Def. 7) $\mathrm{len}\, it = 1 + \overline{\overline{A}}$ and $it(1) = f(x)$ and for every natural number i such that $i \in \mathrm{dom}(\mathrm{SgmX}(\subseteq_n, A))$ holds $it(i+1)^{\mathbf{2}} = f((\mathrm{SgmX}(\subseteq_n, A))(i))$ and $\Re(it(i+1)) \geqslant 0$ and $\Im(it(i+1)) \geqslant 0$.

Let n be a natural number and f be a finite function.

The functor $\mathrm{count\_reps}(f, n)$ yielding a bag of n is defined by

(Def. 8) for every natural number i such that $i \in n$ holds $it(i) = \overline{\overline{f^{-1}(\{i+1\})}}$.

Now we state the propositions:

(54) $\mathrm{count\_reps}(\emptyset, n) = \mathrm{EmptyBag}\, n$.

(55) Let us consider a finite sequence f. Then $\mathrm{count\_reps}(f \frown \langle i+1 \rangle, n) = \mathrm{count\_reps}(f, n) + (\mathrm{EmptyBag}\, n +\cdot (i, 1))$.

PROOF: Set $s_1 = \mathrm{count\_reps}(f \frown \langle i+1 \rangle, n)$. Set $s = \mathrm{count\_reps}(f, n)$. Set $E = \mathrm{EmptyBag}\, n$. For every object x such that $x \in \mathrm{dom}\, s_1$ holds $s_1(x) = (s + (E +\cdot (i, 1)))(x)$. $\square$

Let f be a finite function, L be a double loop structure, and E be a function. The functor $\mathrm{Sgn}_{L,E}(f)$ yielding an element of L is defined by

(Def. 9) for every natural number c such that $c = \overline{\overline{\{x, \text{ where } x \text{ is an element of } \operatorname{dom} f : x \in \operatorname{dom} f \text{ and } f(x) \in E(x)\}}}$ holds if c is even, then $it = 1_L$ and if c is odd, then $it = -1_L$.

Now we state the propositions:

(56) Let us consider a double loop structure L, and a function E. Then $\operatorname{Sgn}_{L,E}(\emptyset) = 1_L$.

(57) Let us consider a double loop structure L, finite sequences f, e, an object x, and a set E. Suppose $\operatorname{len} f = \operatorname{len} e$ and $x \notin E$. Then $\operatorname{Sgn}_{L,(e^\frown \langle E\rangle)}(f ^\frown \langle x\rangle) = \operatorname{Sgn}_{L,e}(f)$.
PROOF: Set $f_5 = f ^\frown \langle x\rangle$. Set $e_7 = e ^\frown \langle E\rangle$. Set $X_1 = \{x$, where x is an element of $\operatorname{dom} f_5 : x \in \operatorname{dom} f_5$ and $f_5(x) \in e_7(x)\}$. Set $X = \{x$, where x is an element of $\operatorname{dom} f : x \in \operatorname{dom} f$ and $f(x) \in e(x)\}$. $X \subseteq \operatorname{dom} f$. $X = X_1$. $\square$

(58) Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure L, finite sequences f, e, an object x, and a set E. Suppose $\operatorname{len} f = \operatorname{len} e$ and $x \in E$. Then $\operatorname{Sgn}_{L,(e^\frown \langle E\rangle)}(f ^\frown \langle x\rangle) = -\operatorname{Sgn}_{L,e}(f)$.
PROOF: Set $f_5 = f ^\frown \langle x\rangle$. Set $e_7 = e ^\frown \langle E\rangle$. Set $X_1 = \{x$, where x is an element of $\operatorname{dom} f_5 : x \in \operatorname{dom} f_5$ and $f_5(x) \in e_7(x)\}$. Set $X = \{x$, where x is an element of $\operatorname{dom} f : x \in \operatorname{dom} f$ and $f(x) \in e(x)\}$. $X \subseteq X_1$. $X_1 \subseteq \operatorname{dom} f_5$. $\operatorname{len} f + 1 \notin X$. $X_1 \subseteq X \cup \{\operatorname{len} f + 1\}$. $\square$

(59) Let us consider an add-associative, right zeroed, right complementable, well unital, distributive, associative, Abelian, commutative, non empty, non trivial double loop structure L, a natural number n, a finite sequence f of elements of L, and a function x_6 from n into L. Suppose $x_6 = \text{FS2XFS}(f)$.

Let us consider a finite set F, an enumeration E of F, and a finite sequence d. Suppose $d \in \operatorname{dom}_\kappa(\text{SignGenOp}(f, (\text{the addition of } L), F)) \cdot E(\kappa)$. Then (the multiplication of $L) \odot (\text{App}((\text{SignGenOp}(f, (\text{the addition of } L), F)) \cdot E))(d) = \text{eval}(\text{Monom}(\operatorname{Sgn}_{L,E}(d), \text{count\_reps}(d, n)), x_6)$.
PROOF: Set $M =$ the multiplication of L. Set $A =$ the addition of L. Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite set F such that $\overline{\overline{F}} = \$_1$ for every enumeration E of F for every finite sequence d such that $d \in \operatorname{dom}_\kappa(\text{SignGenOp}(f, A, F)) \cdot E(\kappa)$ holds $M \odot (\text{App}((\text{SignGenOp}(f, A, F)) \cdot E))(d) = \text{eval}(\text{Monom}(\operatorname{Sgn}_{L,E}(d), \text{count\_reps}(d, n)), x_6)$. $\mathcal{P}[0]$. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. $\square$

(60) Let us consider a finite function f. Suppose f has evenly repeated values. Then $(\text{count\_reps}(f, n))(x)$ is even.

(61) Let us consider a finite sequence f of elements of $\operatorname{Seg} n$.

Then $\text{degree}(\text{count\_reps}(f, n)) = \text{len}\, f$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence f of elements of $\text{Seg}\, n$ such that $\text{len}\, f = \$_1$ holds $\text{degree}(\text{count\_reps}(f, n)) = \text{len}\, f$. $\mathcal{P}[0]$. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. $\square$

(62) Let us consider a double loop structure L, a finite function f, and a function E. Then

(i) $\text{Sgn}_{L,E}(f) = 1_L$, or

(ii) $\text{Sgn}_{L,E}(f) = -1_L$.

(63) Let us consider a finite sequence f of elements of $\text{Seg}\, n$, and i. Suppose $i \in n$ and $\text{count\_reps}(f, n) = \text{EmptyBag}\, n +\cdot (i, \text{len}\, f)$. Then $f = \text{len}\, f \mapsto (i + 1)$.

(64) If $i \in n$, then $\text{count\_reps}(m \mapsto (i + 1), n) = \text{EmptyBag}\, n +\cdot (i, m)$.

PROOF: Set $E = \text{EmptyBag}\, n$. Set $s = \text{count\_reps}(m \mapsto (i + 1), n)$. For every x such that $x \in n$ holds $s(x) = (E +\cdot (i, m))(x)$. $\square$

8. Jpolynom

Let L be an Abelian, commutative, add-associative, right zeroed, right complementable, associative, well unital, distributive, non empty, non trivial double loop structure and m be a natural number. Assume $m > 1$.

A J_{poly} of m, L is a polynomial of m,L defined by

(Def. 10) $it(\text{EmptyBag}\, m +\cdot (0, 2^{m-'1})) = 1_L$ and for every bag b of m such that $b \in \text{Support}\, it$ holds $\text{degree}(b) = 2^{m-'1}$ and there exists an integer i such that $it(b) = i \star \mathbf{1}_L$ and if $2^{m-'1} \in \text{rng}\, b$, then $it(b) = 1_L$ or $it(b) = -1_L$ and for every n, $b(n)$ is even and for every finite sequence f of elements of L and for every function x_6 from m into L such that $x_6 = \text{FS2XFS}(f)$ holds $\text{eval}(it, x_6) = \text{SignGenOp}(f, (\text{the multiplication of } L), (\text{the addition of } L), (\text{Seg}\, m) \setminus \{1\})$.

Let f be a real-valued finite sequence. The functor $\sqrt[\mathbb{C}]{f}$ yielding a finite sequence of elements of $\mathbb{C}_{\text{F}}$ is defined by

(Def. 11) $\text{len}\, it = \text{len}\, f$ and $it(1) = f(1)$ and for every natural number i such that $i \in \text{dom}\, f$ and $i \neq 1$ holds $it(i)^{\mathbf{2}} = f(i)$ and $\Re(it(i)) \geqslant 0$ and $\Im(it(i)) \geqslant 0$.

Let L be a non empty 1-sorted structure, m be a set, and P be a series of m, L. The functor $\text{J}^{\sqrt{\cdot}}(P)$ yielding a series of m, L is defined by

(Def. 12) for every bag b of m, $it(b) = P(2 \cdot b +\cdot (0, b(0)))$.

Let L be a non empty zero structure, m be an ordinal number, and P be a polynomial of m,L. Observe that $\text{J}^{\sqrt{\cdot}}(P)$ is finite-Support. Now we state the propositions:

(65) Let us consider a non empty zero structure L, a natural number m, and a polynomial p of m,L. Suppose for every bag b of m for every n such that $b \in \operatorname{Support} p$ holds $b(n)$ is even. Let us consider a one-to-one finite sequence C_2 of elements of $\operatorname{Bags} m$. Suppose $\operatorname{rng} C_2 = \operatorname{Support} \mathrm{J}^{\sqrt{\cdot}}(p)$. Then there exists a one-to-one finite sequence S of elements of $\operatorname{Bags} m$ such that

(i) $\operatorname{len} S = \operatorname{len} C_2$, and

(ii) $\operatorname{rng} S = \operatorname{Support} p$, and

(iii) for every i such that $i \in \operatorname{dom} S$ holds $S(i) = 2 \cdot C_{2/i} +\cdot (0, (C_{2/i})(0))$.

PROOF: Define $\mathcal{B}(\text{bag of } m) = 2 \cdot \$_1 +\cdot (0, \$_1(0))$. Define $\mathcal{F}(\text{object}) = \mathcal{B}(C_{2/\$_1})$. Consider S being a finite sequence such that $\operatorname{len} S = \operatorname{len} C_2$ and for every k such that $k \in \operatorname{dom} S$ holds $S(k) = \mathcal{F}(k)$. $\operatorname{rng} S \subseteq \operatorname{Support} p$. $\operatorname{Support} p \subseteq \operatorname{rng} S$. S is one-to-one. □

(66) Let us consider a non trivial natural number m, a J_{poly} of m, $\mathbb{C}_{\mathrm{F}}$, a finite sequence f of elements of $\mathbb{R}$, and functions x_6, c_2 from m into $\mathbb{C}_{\mathrm{F}}$. Suppose $x_6 = \operatorname{FS2XFS}(f)$ and $c_2 = \operatorname{FS2XFS}(\sqrt[\mathbb{C}]{f})$. Then $\operatorname{eval}(p, c_2) = \operatorname{eval}(\mathrm{J}^{\sqrt{\cdot}}(p), x_6)$.

PROOF: Reconsider $L = \mathbb{C}_{\mathrm{F}}$ as a field. Reconsider $x_7 = x_6$, $c_3 = c_2$ as a function from m into L. Set $c = \mathrm{J}^{\sqrt{\cdot}}(p)$. Reconsider $P = p$, $C = c$ as a polynomial of m,L. Set $C_2 = \operatorname{SgmX}(\operatorname{BagOrder} m, \operatorname{Support} C)$. Consider C_3 being a finite sequence of elements of L such that $\operatorname{len} C_3 = \operatorname{len} C_2$ and $\operatorname{eval}(C, x_7) = \sum C_3$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} C_3$ holds $C_{3/i} = C \cdot C_{2/i} \cdot (\operatorname{eval}(C_{2/i}, x_7))$. Consider S being a one-to-one finite sequence of elements of $\operatorname{Bags} m$ such that $\operatorname{len} S = \operatorname{len} C_2$ and $\operatorname{rng} S = \operatorname{Support} p$ and for every i such that $i \in \operatorname{dom} S$ holds $S(i) = 2 \cdot C_{2/i} +\cdot (0, (C_{2/i})(0))$. Consider y being a finite sequence of elements of L such that $\operatorname{len} y = \overline{\overline{\operatorname{Support} p}}$ and $\operatorname{eval}(P, c_3) = \sum y$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} y$ holds $y_{/i} = P \cdot S_{/i} \cdot (\operatorname{eval}(S_{/i}, c_3))$. For every i such that $1 \leqslant i \leqslant \operatorname{len} y$ holds $y(i) = C_3(i)$. □

(67) Let us consider a finite sequence f_2 of elements of $\mathbb{C}_{\mathrm{F}}$, and a finite sequence f_4 of elements of $\mathbb{R}_{\mathrm{F}}$. If $f_2 = f_4$, then $\prod f_2 = \prod f_4$.

PROOF: Reconsider $F_1 = \mathbb{C}_{\mathrm{F}}$, $F_2 = \mathbb{R}_{\mathrm{F}}$ as a field. Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence f_2 of elements of F_1 for every finite sequence f_4 of elements of F_2 such that $f_2 = f_4$ and $\operatorname{len} f_2 = \$_1$ holds $\prod f_2 = \prod f_4$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

(68) Let us consider an ordinal number m, a bag b of m, a function x_5 from m into $\mathbb{C}_{\mathrm{F}}$, and a function x_{10} from m into $\mathbb{R}_{\mathrm{F}}$. If $x_5 = x_{10}$, then $\operatorname{eval}(b, x_5) = \operatorname{eval}(b, x_{10})$.

PROOF: Reconsider $F_1 = \mathbb{C}_{\mathrm{F}}$, $F_2 = \mathbb{R}_{\mathrm{F}}$ as a field.

Set $S = \mathrm{SgmX}(\subseteq_m, \mathrm{support}\, b)$. Consider y_1 being a finite sequence of elements of F_1 such that $\mathrm{len}\, y_1 = \mathrm{len}\, S$ and $\mathrm{eval}(b, x_5) = \prod y_1$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y_1$ holds $y_{1/i} = \mathrm{power}_{F_1}(x_5 \cdot S_{/i}, b \cdot S_{/i})$. Consider y_2 being a finite sequence of elements of F_2 such that $\mathrm{len}\, y_2 = \mathrm{len}\, S$ and $\mathrm{eval}(b, x_{10}) = \prod y_2$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y_2$ holds $y_{2/i} = \mathrm{power}_{F_2}(x_{10} \cdot S_{/i}, b \cdot S_{/i})$. For every i such that $1 \leqslant i \leqslant \mathrm{len}\, S$ holds $y_1(i) = y_2(i)$ by [3, (7)]. □

(69) Let us consider an ordinal number m, a polynomial P_8 of m,$\mathbb{C}_{\mathrm{F}}$, and a polynomial P_{14} of m,$\mathbb{R}_{\mathrm{F}}$. Suppose $P_8 = P_{14}$. Let us consider a function x_5 from m into $\mathbb{C}_{\mathrm{F}}$, and a function x_{10} from m into $\mathbb{R}_{\mathrm{F}}$. Suppose $x_5 = x_{10}$. Then $\mathrm{eval}(P_8, x_5) = \mathrm{eval}(P_{14}, x_{10})$.

PROOF: Reconsider $F_1 = \mathbb{C}_{\mathrm{F}}$, $F_2 = \mathbb{R}_{\mathrm{F}}$ as a field.

Set $S = \mathrm{SgmX}(\mathrm{BagOrder}\, m, \mathrm{Support}\, P_8)$. Consider C_3 being a finite sequence of elements of the carrier of F_1 such that $\mathrm{len}\, C_3 = \mathrm{len}\, S$ and $\mathrm{eval}(P_8, x_5) = \sum C_3$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, C_3$ holds $C_{3/i} = P_8 \cdot S_{/i} \cdot (\mathrm{eval}(S_{/i}, x_5))$.

Support $P_8 \subseteq$ Support P_{14}. Support $P_{14} \subseteq$ Support P_8. Consider R_4 being a finite sequence of elements of the carrier of F_2 such that $\mathrm{len}\, R_4 = \mathrm{len}\, S$ and $\mathrm{eval}(P_{14}, x_{10}) = \sum R_4$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, R_4$ holds $R_{4/i} = P_{14} \cdot S_{/i} \cdot (\mathrm{eval}(S_{/i}, x_{10}))$. Define $\mathcal{P}$[natural number] $\equiv$ for every natural number i such that $i = \$_1 \leqslant \mathrm{len}\, S$ holds $\sum(R_4 \restriction i) = \sum(C_3 \restriction i)$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

Let m be a natural number. Assume $m > 1$. Let M be a $\mathrm{J}_{\mathrm{poly}}$ of m, $\mathbb{C}_{\mathrm{F}}$. The functor $\mathrm{J}^{\sqrt{\mathbb{C}}}(M)$ yielding a $\mathbb{Z}$-valued polynomial of m,$\mathbb{R}_{\mathrm{F}}$ is defined by the term

(Def. 13) $\mathrm{J}^{\sqrt{\cdot}}(M)$.

Now we state the proposition:

(70) Let us consider a non trivial natural number m, a $\mathrm{J}_{\mathrm{poly}}$ of m, $\mathbb{C}_{\mathrm{F}}$, and a function f from m into $\mathbb{R}_{\mathrm{F}}$. Then $\mathrm{eval}(\mathrm{J}^{\sqrt{\mathbb{C}}}(M), f) = 0$ if and only if there exists a subset A of $(\mathrm{Seg}\, m) \setminus \{1\}$ such that (the addition of $\mathbb{C}_{\mathrm{F}}) \odot \mathrm{SignGen}(\sqrt[\mathbb{C}]{\mathrm{XFS2FS}(^{@}f)}, (\text{the addition of } \mathbb{C}_{\mathrm{F}}), A) = 0$.

PROOF: Reconsider $F = \mathrm{XFS2FS}(^{@}f)$ as a finite sequence of elements of $\mathbb{R}$. Set $M_3 =$ the multiplication of $\mathbb{C}_{\mathrm{F}}$. Set $A_1 =$ the addition of $\mathbb{C}_{\mathrm{F}}$. Reconsider $x_6 = \mathrm{FS2XFS}(F)$ as a function from m into $\mathbb{C}_{\mathrm{F}}$. Reconsider $c_1 = \sqrt[\mathbb{C}]{F}$ as an m-elements finite sequence of elements of $\mathbb{C}_{\mathrm{F}}$. Reconsider $f_3 = \mathrm{FS2XFS}(c_1)$ as a function from m into $\mathbb{C}_{\mathrm{F}}$. $\mathrm{eval}(\mathrm{J}^{\sqrt{\mathbb{C}}}(M), f) = \mathrm{eval}(\mathrm{J}^{\sqrt{\cdot}}(M), x_6)$. $\mathrm{eval}(\mathrm{J}^{\sqrt{\mathbb{C}}}(M), f) = \mathrm{eval}(M, f_3)$. Set $B = (\mathrm{Seg}\, m) \setminus \{1\}$. Set $t_1 =$ the enumeration of 2^B. Set $C_1 = (\mathrm{SignGenOp}(c_1, A_1, 2^B)) \cdot t_1$. Define $\mathcal{P}$[set] $\equiv$ for every element X of $\mathrm{Fin\,dom}\, C_1$ such that $X = \$_1$

holds M_3-$\sum_X(A_1 \odot C_1) = 0_{\mathbb{C}_\mathrm{F}}$ iff there exists x such that $x \in X$ and $0_{\mathbb{C}_\mathrm{F}} = (A_1 \odot C_1)(x)$.

For every element B_9 of $\mathrm{Fin}\,\mathrm{dom}\,C_1$ and for every element b of $\mathrm{dom}\,C_1$ such that $\mathcal{P}[B_9]$ and $b \notin B_9$ holds $\mathcal{P}[B_9 \cup \{b\}]$. For every element B of $\mathrm{Fin}\,\mathrm{dom}\,C_1$, $\mathcal{P}[B]$. If $\mathrm{eval}(\mathrm{J}^{\sqrt{\mathbb{C}}}(M), f) = 0$, then there exists a subset A of $(\mathrm{Seg}\,m) \setminus \{1\}$ such that $A_1 \odot \mathrm{SignGen}(\sqrt[\mathbb{C}]{\mathrm{XFS2FS}(^{@}f)}, A_1, A) = 0$ by [6, (80)]. Consider x such that $x \in \mathrm{dom}\,t_1$ and $t_1(x) = A$. $\square$

Let x, y, z, t be objects. Let us note that $\langle x, y, z, t\rangle$ is 4-elements. Let x be a real number. Note that $\langle x\rangle$ is $\mathbb{R}$-valued. Let x, y, z, t be real numbers. One can check that $\langle x, y, z, t\rangle$ is $\mathbb{R}$-valued. Now we state the propositions:

(71) Let us consider a real-valued finite sequence f. If $i > 1$ and $f(i) \geqslant 0$, then $(\sqrt[\mathbb{C}]{f})(i) = \sqrt{f(i)}$. The theorem is a consequence of (2).

(72) Let us consider a finite sequence f of elements of $\mathbb{C}_\mathrm{F}$, and a set A. Then there exists an integer i such that

(i) $i = 1$ or $i = -1$, and

(ii) $(\mathrm{SignGen}(f, (\text{the addition of } \mathbb{C}_\mathrm{F}), A))(x) = i \cdot f(x)$.

9. PRIME REPRESENTING POLYNOMIAL CONSTRUCTION

Now we state the propositions:

(73) Let us consider a $\mathrm{J}_{\mathrm{poly}}$ of 4, $\mathbb{C}_\mathrm{F}$, and natural numbers x_1, x_2, x_3. Suppose x_1 is odd and x_2 is odd. Let us consider an integer z. Suppose $\mathrm{eval}(\mathrm{J}^{\sqrt{\mathbb{C}}}(M), {}^{@}\langle z, x_1, 4 \cdot x_2, 16 \cdot x_3\rangle) = 0$. Then

(i) x_1 is a square, and

(ii) x_2 is a square, and

(iii) x_3 is a square, and

(iv) $-z \leqslant \sqrt{x_1} + 2 \cdot \sqrt{x_2} + 4 \cdot \sqrt{x_3}$.

PROOF: Set $A_2 =$ the addition of $\mathbb{C}_\mathrm{F}$. Set $f = \langle z, x_1, 4 \cdot x_2, 16 \cdot x_3\rangle$. Consider A being a subset of $(\mathrm{Seg}\,4) \setminus \{1\}$ such that $A_2 \odot \mathrm{SignGen}(\sqrt[\mathbb{C}]{\mathrm{XFS2FS}(^{@@}f)}, A_2, A) = 0$. Set $c = \sqrt[\mathbb{C}]{\mathrm{XFS2FS}(f)}$. Set $S = \mathrm{SignGen}(c, A_2, A)$. Set $i_4 = 1$. Consider i_1 being an integer such that ($i_1 = 1$ or $i_1 = -1$) and $S(2) = i_1 \cdot c(2)$. Consider i_2 being an integer such that ($i_2 = 1$ or $i_2 = -1$) and $S(3) = i_2 \cdot c(3)$. Consider i_3 being an integer such that ($i_3 = 1$ or $i_3 = -1$) and $S(4) = i_3 \cdot c(4)$. $c(2) = \sqrt{x_1}$. $c(3) = \sqrt{4 \cdot x_2}$. $c(4) = \sqrt{4 \cdot 4 \cdot x_3}$. $S(1) \neq 0$. Set $Y = z \cdot z + 16 \cdot x_3 - x_1 - 4 \cdot x_2$. $Y \neq 0$. Reconsider $Y_1 = 2 \cdot Y \cdot 8 \cdot (i_4 \cdot i_3) \cdot z \cdot \sqrt{x_3}$ as an integer. $16 \cdot Y \cdot z \mid Y_1$. Consider m being an integer such that $16 \cdot Y \cdot z \cdot m = Y_1$. Reconsider $S_3 = \sqrt{x_3}$ as an integer. Set $Z_1 = i_4 \cdot 2 \cdot z - 1 + i_3 \cdot 8 \cdot S_3$. $Z_1 \neq 0$. Set $Y_1 = Z_1 \cdot Z_1 + 16 \cdot x_2 - 1 - 4 \cdot x_1$. $Y_1 \neq 0$. Reconsider $Y_2 = 16 \cdot Y_1 \cdot Z_1 \cdot i_2 \cdot \sqrt{x_2}$ as an integer. Consider m_1 being an integer such that $16 \cdot Y_1 \cdot Z_1 \cdot m_1 = Y_2$. Reconsider $Y_3 = 2 \cdot i_1 \cdot \sqrt{x_1}$ as an integer. Consider m_2 being an integer such that $2 \cdot m_2 = Y_3$. □

(74) Let us consider a $\mathrm{J_{poly}}$ of 4, $\mathbb{C}_\mathrm{F}$, and natural numbers x_1, x_2, x_3. Suppose x_1 is a square and x_2 is a square and x_3 is a square. Then there exists an integer z such that

(i) $-z = \sqrt{x_1} + 2 \cdot \sqrt{x_2} + 4 \cdot \sqrt{x_3}$, and

(ii) $\mathrm{eval}(\mathrm{J}^{\sqrt{\mathbb{C}}}(M), {}^{@}\langle z, x_1, 4 \cdot x_2, 16 \cdot x_3\rangle) = 0$.

The theorem is a consequence of (71) and (70).

(75) Let us consider a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure L, and a polynomial p of n,L. Then there exists a polynomial q of $n+m$,L such that

(i) $\mathrm{rng}\, q \subseteq \mathrm{rng}\, p \cup \{0_L\}$, and

(ii) for every bag b of $n+m$, $b \in \mathrm{Support}\, q$ iff $b \restriction n \in \mathrm{Support}\, p$ and for every i such that $i \geqslant n$ holds $b(i) = 0$, and

(iii) for every bag b of $n+m$ such that $b \in \mathrm{Support}\, q$ holds $q(b) = p(b \restriction n)$, and

(iv) for every function x from n into L and for every function y from $n+m$ into L such that $y \restriction n = x$ holds $\mathrm{eval}(p, x) = \mathrm{eval}(q, y)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ there exists a polynomial q of $n+\$_1$,$L$ such that $\mathrm{rng}\, q \subseteq \mathrm{rng}\, p \cup \{0_L\}$ and for every bag b of $n+\$_1$, $b \in \mathrm{Support}\, q$ iff $b \restriction n \in \mathrm{Support}\, p$ and for every i such that $i \geqslant n$ holds $b(i) = 0$ and for every bag b of $n+\$_1$ such that $b \in \mathrm{Support}\, q$ holds $q(b) = p(b \restriction n)$ and for every function x from n into L and for every function y from $n+\$_1$ into L such that $y \restriction n = x$ holds $\mathrm{eval}(p, x) = \mathrm{eval}(q, y)$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(76) Let us consider a $\mathrm{J_{poly}}$ of 4, $\mathbb{C}_\mathrm{F}$. Then there exists a $\mathbb{Z}$-valued polynomial K_2 of 6,$\mathbb{R}_\mathrm{F}$ such that

(i) for every function f from 6 into $\mathbb{R}_\mathrm{F}$ such that $f(5) \neq 0$ holds $\mathrm{eval}(K_2, f) = \mathrm{power}_{\mathbb{R}_\mathrm{F}}(f_{/5}, 8) \cdot (\mathrm{eval}(\mathrm{J}^{\sqrt{\mathbb{C}}}(M), {}^{@}\langle -f(0) + \frac{f(4)}{f(5)}, f(1), f(2), f(3)\rangle))$, and

(ii) for every $\mathbb{Z}$-valued function f from 6 into $\mathbb{R}_\mathrm{F}$ such that $f(5) \neq 0$ and $\mathrm{eval}(K_2, f) = 0$ holds $f(5) \mid f(4)$.

PROOF: Set $p = \mathrm{J}^{\sqrt{\mathbb{C}}}(M)$. Set $R = \mathbb{R}_\mathrm{F}$. Consider q being a polynomial of $4+2$,R such that $\mathrm{rng}\, q \subseteq \mathrm{rng}\, p \cup \{0_R\}$ and for every bag b of $4+$

2, $b \in \operatorname{Support} q$ iff $b{\restriction}4 \in \operatorname{Support} p$ and for every i such that $i \geqslant 4$ holds $b(i) = 0$ and for every bag b of $4+2$ such that $b \in \operatorname{Support} q$ holds $q(b) = p(b{\restriction}4)$ and for every function x from 4 into R and for every function y from $4+2$ into R such that $y{\restriction}4 = x$ holds $\operatorname{eval}(p, x) = \operatorname{eval}(q, y)$. Set $Y_5 = \operatorname{EmptyBag} 6 +\cdot (0, 1)$. Set $Y = \operatorname{Monom}(-1_R, Y_5)$. Set $Z_9 = \operatorname{EmptyBag} 6 +\cdot (4, 1)$. Set $Z = \operatorname{Monom}(1_R, Z_9)$. Set $Y_4 = Y + Z$. Set $S_{15} = \operatorname{SgmX}(\operatorname{BagOrder} 6, \operatorname{Support} q)$.

Consider S being a finite sequence of elements of $\operatorname{PolyRing}(6, R)$ such that $\operatorname{Subst}(q, 0, Y_4) = \sum S$ and $\operatorname{len} S_{15} = \operatorname{len} S$ and for every i such that $i \in \operatorname{dom} S$ holds $S(i) = q(S_{15/i}) \cdot (\operatorname{Subst}(S_{15/i}, 0, Y_4))$. Set $E_1 = \operatorname{EmptyBag} 6$. Set $M_1 = \operatorname{EmptyBag} 4 +\cdot (0, 8)$. Set $M_2 = E_1 +\cdot (0, 8)$. $2 \cdot M_1 +\cdot (0, M_1(0)) = M_1$. For every x such that $x \in 4$ holds $(M_2{\restriction}4)(x) = M_1(x)$. For every i such that $i \geqslant 4$ holds $M_2(i) = 0$. Consider I being an object such that $I \in \operatorname{dom} S_{15}$ and $S_{15}(I) = M_2$. Define $\mathcal{P}[\text{natural number}] \equiv ({Y_4}^{\$_1})(E_1 +\cdot (4, \$_1)) = 1_R$. ${Y_4}^0 = 1\_(6, R)$. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. Set $Z_8 = E_1 +\cdot (4, 8)$. $(\operatorname{Subst}(S_{15/I}, 0, Y_4))(Z_8) = ({Y_4}^{M_2(0)})(Z_8)$. For every i such that $i \in \operatorname{dom} S$ for every bag b of 6 such that $b \in \operatorname{Support} q(S_{15/i}) \cdot (\operatorname{Subst}(S_{15/i}, 0, Y_4))$ and $b(4) \geqslant 8$ holds $i = I$ and $b = Z_8$.

For every i such that $i \in \operatorname{dom} S$ for every bag b of 6 such that $b \in \operatorname{Support} q(S_{15/i}) \cdot (\operatorname{Subst}(S_{15/i}, 0, Y_4))$ holds $b(5) = 0$. Define $\mathcal{W}[\text{natural number}] \equiv$ for every natural number i such that $\$_1 = i$ and $i \leqslant \operatorname{len} S$ for every polynomial w of 6,R such that $w = \sum(S{\restriction}i)$ holds if $I \leqslant i$, then $w(Z_8) = \mathbf{1}_R$ and if $i < I$, then $w(Z_8) = 0_R$ and for every bag b of 6 such that $b \in \operatorname{Support} w$ and $b \neq Z_8$ holds $b(4) < 8$ and for every bag b of 6 such that $b \in \operatorname{Support} w$ holds $b(5) = 0$. $\mathcal{W}[0]$. If $\mathcal{W}[n]$, then $\mathcal{W}[n+1]$. Set $S_9 = \operatorname{Subst}(q, 0, Y_4)$. $\mathcal{W}[n]$. Define $\mathcal{J}[\text{bag of } 6, \text{element of } R] \equiv$ if $\$_1(4) + \$_1(5) = 8$, then $\$_2 = S_9(\$_1 +\cdot (5, 0))$ and if $\$_1(4) + \$_1(5) \neq 8$, then $\$_2 = 0_R$. For every element x of Bags 6, there exists an element y of R such that $\mathcal{J}[x, y]$. Consider W being a function from Bags 6 into R such that for every element x of Bags 6, $\mathcal{J}[x, W(x)]$. Set $S_7 = \operatorname{SgmX}(\operatorname{BagOrder} 6, \operatorname{Support} S_9)$. Define $\mathcal{O}(\text{object}) = S_{7/\$_1} +\cdot (5, 8 -' (S_{7/\$_1})(4))$.

Consider S_{10} being a finite sequence such that $\operatorname{len} S_{10} = \operatorname{len} S_7$ and for every k such that $k \in \operatorname{dom} S_{10}$ holds $S_{10}(k) = \mathcal{O}(k)$. $\operatorname{rng} S_{10} \subseteq \operatorname{Support} W$. $\operatorname{Support} W \subseteq \operatorname{rng} S_{10}$. S_{10} is one-to-one. Reconsider $R_1 = R$ as a field. $\operatorname{Monom}(-1_{R_1}, Y_5) = -\operatorname{Monom}(1_{R_1}, Y_5)$. $\operatorname{rng} W \subseteq \mathbb{Z}$. Reconsider $S_8 = S_9$, $J = W$ as a polynomial of 6,R_1. For every function f from 6 into $\mathbb{R}_{\mathrm{F}}$ and for every element d of $\mathbb{R}_{\mathrm{F}}$ such that $f(5) \neq 0$ and $d = \frac{f(4)}{f(5)}$ holds $\operatorname{eval}(W, f) = \operatorname{power}_{\mathbb{R}_{\mathrm{F}}}(f_{/5}, 8) \cdot (\operatorname{eval}(S_9, f +\cdot (4, d)))$. For every function f from 6 into $\mathbb{R}_{\mathrm{F}}$ such that $f(5) \neq 0$ holds $\operatorname{eval}(W, f) = \operatorname{power}_R(f_{/5}, 8) \cdot (\operatorname{eval}(\mathrm{J}^{\sqrt{\mathbb{C}}}(M), {}^{@}\langle -f(0) + \frac{f(4)}{f(5)}, f(1), f(2), f(3) \rangle))$. Set $N = \gcd(f(5), f(4))$.

Consider g_5, g_4 being integers such that $f(5) = N \cdot g_5$ and $f(4) = N \cdot g_4$ and g_5 and g_4 are relatively prime. Reconsider $N_5 = N$, $g_2 = g_5$, $g_3 = g_4$ as an element of R. Set $g = (f +\cdot (4, g_3)) +\cdot (5, g_2)$.

Reconsider $g_1 = g$ as a function from 6 into R_1. $\operatorname{rng} g \subseteq \mathbb{Z}$. $\operatorname{power}_{\mathbb{R}_{\mathrm{F}}}(N_5, 8) \neq 0_R$. Set $R_8 = E_1 +\cdot (4, 8)$. Set $M_5 = \operatorname{Monom}(1_{R_1}, R_8)$. Set $S = \operatorname{SgmX}(\operatorname{BagOrder} 6, \operatorname{Support}(J - M_5))$. Consider R_4 being a finite sequence of elements of R_1 such that $\operatorname{len} R_4 = \operatorname{len} S$ and $\operatorname{eval}(J - M_5, g_1) = \sum R_4$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} R_4$ holds $R_{4/i} = (J - M_5) \cdot S_{/i} \cdot (\operatorname{eval}(S_{/i}, g_1))$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every natural number i such that $i = \$_1 \leqslant \operatorname{len} S$ there exists an integer s such that $s \cdot g(5) = \sum(R_4 \restriction i)$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. Consider s being an integer such that $s \cdot g(5) = \sum(R_4 \restriction \operatorname{len} R_4)$. $\operatorname{eval}(R_8, g) = \operatorname{power}_R(g(4), 8)$. Define $\mathcal{H}[\text{natural number}] \equiv$ if $g_5 \mid {g_4}^{\$_1}$, then $g_5 \mid g_4$. $\mathcal{H}[0]$. If $\mathcal{H}[j]$, then $\mathcal{H}[j+1]$. $\mathcal{H}[j]$. $\square$

Let x be an integer. One can verify that $\langle x \rangle$ is $\mathbb{Z}$-valued. Let x, y, z, t be integers. Let us observe that $\langle x, y, z, t \rangle$ is $\mathbb{Z}$-valued.

Now we state the propositions:

(77) There exists a $\mathbb{Z}$-valued polynomial K_3 of 8,$\mathbb{R}_{\mathrm{F}}$ such that for every natural numbers x_1, x_2, x_3, P, R, N for every integer V such that x_1 is odd and x_2 is odd and $P > 0$ and $N > \sqrt{x_1} + 2 \cdot \sqrt{x_2} + 4 \cdot \sqrt{x_3} + R$ holds x_1 is a square and x_2 is a square and x_3 is a square and $P \mid R$ and $V \geqslant 0$ iff there exists a natural number z such that for every function f from 8 into $\mathbb{R}_{\mathrm{F}}$ such that $f = \langle z, x_1, 4 \cdot x_2, 16 \cdot x_3 \rangle ^\frown \langle R, P, N, V \rangle$ holds $\operatorname{eval}(K_3, f) = 0$.
PROOF: Set $M =$ the $\mathrm{J}_{\mathrm{poly}}$ of 4, $\mathbb{C}_{\mathrm{F}}$. Set $R_3 = \mathbb{R}_{\mathrm{F}}$. Reconsider $R_1 = R_3$ as a field. Consider K_2 being a $\mathbb{Z}$-valued polynomial of 6,$\mathbb{R}_{\mathrm{F}}$ such that for every function f from 6 into $\mathbb{R}_{\mathrm{F}}$ such that $f(5) \neq 0$ holds $\operatorname{eval}(K_2, f) = \operatorname{power}_{\mathbb{R}_{\mathrm{F}}}(f_{/5}, 8) \cdot (\operatorname{eval}(\mathrm{J}^{\sqrt{\mathbb{C}}}(M), {}^{@}\langle -f(0) + \frac{f(4)}{f(5)}, f(1), f(2), f(3) \rangle))$ and for every $\mathbb{Z}$-valued function f from 6 into $\mathbb{R}_{\mathrm{F}}$ such that $f(5) \neq 0$ and $\operatorname{eval}(K_2, f) = 0$ holds $f(5) \mid f(4)$. Consider K_{28} being a polynomial of $6+2$,R_3 such that $\operatorname{rng} K_{28} \subseteq \operatorname{rng} K_2 \cup \{0_{R_3}\}$ and for every bag b of $6+2$, $b \in \operatorname{Support} K_{28}$ iff $b \restriction 6 \in \operatorname{Support} K_2$ and for every i such that $i \geqslant 6$ holds $b(i) = 0$ and for every bag b of $6+2$ such that $b \in \operatorname{Support} K_{28}$ holds $K_{28}(b) = K_2(b \restriction 6)$ and for every function x from 6 into R_3 and for every function y from $6+2$ into R_3 such that $y \restriction 6 = x$ holds $\operatorname{eval}(K_2, x) = \operatorname{eval}(K_{28}, y)$. Set $n_1 = \operatorname{EmptyBag} 8 +\cdot (6, 1)$. Set $n = \operatorname{Monom}(1_{R_3}, n_1)$. Set $v_1 = \operatorname{EmptyBag} 8 +\cdot (7, 1)$. Set $v = \operatorname{Monom}(-1_{R_3}, v_1)$. Set $z_3 = \operatorname{EmptyBag} 8 +\cdot (0, 1)$.

Set $z = \operatorname{Monom}(1_{R_3}, z_3)$. $\operatorname{Monom}(-1_{R_1}, v_1) = -\operatorname{Monom}(1_{R_1}, v_1)$. Set $z_4 = z + n * v$. Reconsider $K_3 = \operatorname{Subst}(K_{28}, 0, z_4)$ as a $\mathbb{Z}$-valued polynomial of 8,R_3. If x_1 is a square and x_2 is a square and x_3 is a square and $P \mid R$ and $V \geqslant 0$, then there exists a natural number z such that for every function f from 8 into $\mathbb{R}_{\mathrm{F}}$ such that $f = \langle z, x_1, 4 \cdot x_2, 16 \cdot x_3\rangle \frown \langle R, P, N, V\rangle$ holds $\mathrm{eval}(K_3, f) = 0$. Reconsider $f = \langle zz, x_1, 4 \cdot x_2, 16 \cdot x_3\rangle \frown \langle R, P, N, V\rangle$ as a $\mathbb{Z}$-valued function from 8 into $\mathbb{R}_{\mathrm{F}}$. $\mathrm{eval}(K_3, f) = \mathrm{eval}(K_{28}, f {+\cdot} (0, \mathrm{eval}(z_4, f)))$. Set $y = -N \cdot V + zz$. Reconsider $Y = y$, $z_5 = zz$, $N_4 = N$, $V_5 = V$ as an element of R_3. $\mathrm{eval}(z_3, f) = \mathrm{power}_{R_3}(f(0), 1)$. $\mathrm{eval}(v_1, f) = \mathrm{power}_{R_3}(f(7), 1)$. $\mathrm{eval}(n_1, f) = \mathrm{power}_{R_3}(f(6), 1)$. Set $f_6 = (f {+\cdot} (0, Y))\restriction 6$. Consider d being a natural number such that $P \cdot d = R$. $\mathrm{power}_{R_3}(f_{6/5}, 8) \neq 0$. x_1 is a square and x_2 is a square and x_3 is a square and $-(-y + d) \leqslant \sqrt{x_1} + 2 \cdot \sqrt{x_2} + 4 \cdot \sqrt{x_3}$. $\square$

(78) Let us consider a set X, a right zeroed, non empty additive loop structure S, series p, q of X, S, and a set V. Suppose $\mathrm{vars}(p) \subseteq V$ and $\mathrm{vars}(q) \subseteq V$. Then $\mathrm{vars}(p + q) \subseteq V$. The theorem is a consequence of (41).

(79) Let us consider an ordinal number X, an add-associative, right complementable, right zeroed, right unital, distributive, non empty double loop structure S, polynomials p, q of X,S, and a set V. Suppose $\mathrm{vars}(p) \subseteq V$ and $\mathrm{vars}(q) \subseteq V$. Then $\mathrm{vars}(p * q) \subseteq V$. The theorem is a consequence of (43).

(80) Let us consider a set X, an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure S, a series p of X, S, an element a of S, and a set V. If $\mathrm{vars}(p) \subseteq V$, then $\mathrm{vars}(a \cdot p) \subseteq V$. The theorem is a consequence of (44).

(81) Let us consider a set X, an add-associative, right zeroed, right complementable, non empty additive loop structure S, series p, q of X, S, and a set V. Suppose $\mathrm{vars}(p) \subseteq V$ and $\mathrm{vars}(q) \subseteq V$. Then $\mathrm{vars}(p - q) \subseteq V$. The theorem is a consequence of (42) and (41).

(82) There exists a $\mathbb{Z}$-valued polynomial Z of 17,$\mathbb{R}_{\mathrm{F}}$ such that

   (i) $\mathrm{vars}(Z) \subseteq \{0\} \cup 17 \setminus 8$, and

   (ii) for every natural number x_8 such that $x_8 > 0$ holds $x_8 + 1$ is prime iff there exists a $\mathbb{Z}$-valued function x from 17 into $\mathbb{R}_{\mathrm{F}}$ such that $x_{/8} = x_8$ and $x_{/9}$ is a positive natural number and $x_{/10}$ is a positive natural number and $x_{/11}$ is a positive natural number and $x_{/12}$ is a positive natural number and $x_{/13}$ is a positive natural number and $x_{/14}$ is a natural number and $x_{/15}$ is a natural number and $x_{/16}$ is a natural number and $x_{/0}$ is a natural number and $\mathrm{eval}(Z, x) = 0_{\mathbb{R}_{\mathrm{F}}}$.

PROOF: Set $N = 17$. Set $E_2 = \mathrm{EmptyBag}\, N$. Set $V_4 = N \setminus 8$. $n \in V_4$ iff $8 \leqslant n < N$. Set $k = 8$. Set $P_{11} = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (k, 1))$. $\mathrm{vars}(P_{11}) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(P_{11}, x) = x_{/k}$. Set $f = 9$. Set $P_9 = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (f, 1))$. $\mathrm{vars}(P_9) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(P_9, x) = x_{/f}$. Set $i = 10$. Set $\Pi = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (i, 1))$.

$\mathrm{vars}(\Pi) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(\Pi, x) = x_{/i}$. Set $j = 11$. Set $P_{10} = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 +\cdot (j, 1))$. $\mathrm{vars}(P_{10}) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(P_{10}, x) = x_{/j}$. Set $m = 12$. Set $P_{12} = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 +\cdot (m, 1))$. $\mathrm{vars}(P_{12}) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(P_{12}, x) = x_{/m}$. Set $u = 13$. Set $P_{17} = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 +\cdot (u, 1))$. $\mathrm{vars}(P_{17}) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(P_{17}, x) = x_{/u}$. Set $r = 14$. Set $P_{14} = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 +\cdot (r, 1))$. $\mathrm{vars}(P_{14}) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(P_{14}, x) = x_{/r}$.

Set $s = 15$. Set $P_{15} = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 +\cdot (s, 1))$. $\mathrm{vars}(P_{15}) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(P_{15}, x) = x_{/s}$. Set $t = 16$. Set $P_{16} = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 +\cdot (t, 1))$. $\mathrm{vars}(P_{16}) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(P_{16}, x) = x_{/t}$. Reconsider $H_1 = 100$ as an integer element of $\mathbb{R}_{\mathrm{F}}$. Set $O = 1\_(N, \mathbb{R}_{\mathrm{F}})$. $\mathrm{vars}(O) \subseteq V_4$. Reconsider $W = H_1 \cdot ((P_9 * P_{11}) * (P_{11} + O))$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(W) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(W, x) = H_1 \cdot (x_{/f}) \cdot (x_{/k}) \cdot (x_{/k} + 1_{\mathbb{R}_{\mathrm{F}}})$. Reconsider $U = H_1 \cdot (((P_{17} * P_{17}) * P_{17}) * ((W * W) * W)) + O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(U) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(U, x) = H_1 \cdot (x_{/u})^3 \cdot (\mathrm{eval}(W, x))^3 + 1_{\mathbb{R}_{\mathrm{F}}}$. Reconsider $M = H_1 \cdot ((P_{12} * U) * W) + O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(M) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(M, x) = H_1 \cdot (x_{/m}) \cdot (\mathrm{eval}(U, x)) \cdot (\mathrm{eval}(W, x)) + 1_{\mathbb{R}_{\mathrm{F}}}$. Reconsider $S = (M - O) * P_{15} + P_{11} + O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(S) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(S, x) = (\mathrm{eval}(M, x) - 1_{\mathbb{R}_{\mathrm{F}}}) \cdot (x_{/s}) + x_{/k} + 1_{\mathbb{R}_{\mathrm{F}}}$.

Reconsider $T = (M * U - O) * P_{16} + W - P_{11} + O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(T) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(T, x) = ((\mathrm{eval}(M, x)) \cdot (\mathrm{eval}(U, x)) - 1_{\mathbb{R}_{\mathrm{F}}}) \cdot (x_{/t}) + \mathrm{eval}(W, x) - x_{/k} + 1_{\mathbb{R}_{\mathrm{F}}}$. Reconsider $T_2 = 2$ as an integer element of $\mathbb{R}_{\mathrm{F}}$. Reconsider $Q = T_2 \cdot (M * W) - W * W - O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(Q) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(Q, x) = T_2 \cdot (\mathrm{eval}(M, x)) \cdot (\mathrm{eval}(W, x)) - (\mathrm{eval}(W, x))^{\mathbf{2}} - 1_{\mathbb{R}_{\mathrm{F}}}$. Reconsider $L = (P_{11} + O) * Q$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(L) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(L, x) = (x_{/k} + 1_{\mathbb{R}_{\mathrm{F}}}) \cdot (\mathrm{eval}(Q, x))$. Reconsider $A = M * (U + O)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(A) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(A, x) = (\mathrm{eval}(M, x)) \cdot (\mathrm{eval}(U, x) + 1_{\mathbb{R}_{\mathrm{F}}})$. Reconsider $B = W + O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(B) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(B, x) = \mathrm{eval}(W, x) + 1_{\mathbb{R}_{\mathrm{F}}}$. Reconsider $C = P_{14} + W + O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(C) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(C, x) = x_{/r} + \mathrm{eval}(W, x) + 1_{\mathbb{R}_{\mathrm{F}}}$.

Reconsider $D = (A * A - O) * (C * C) + O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(D) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(D, x) =$

$((\mathrm{eval}(A,x))^{\mathbf{2}} - 1_{\mathbb{R}_\mathrm{F}}) \cdot (\mathrm{eval}(C,x))^{\mathbf{2}} + 1_{\mathbb{R}_\mathrm{F}}$. Reconsider $E = T_2 \cdot ((((\Pi * C) * C) * L) * D)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(E) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(E,x) = T_2 \cdot (x_{/i}) \cdot (\mathrm{eval}(C,x))^{\mathbf{2}} \cdot (\mathrm{eval}(L,x)) \cdot (\mathrm{eval}(D,x))$. Reconsider $F = (A*A-O)*(E*E)+O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(F) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(F,x) = ((\mathrm{eval}(A,x))^{\mathbf{2}} - 1_{\mathbb{R}_\mathrm{F}}) \cdot (\mathrm{eval}(E,x))^{\mathbf{2}} + 1_{\mathbb{R}_\mathrm{F}}$. Reconsider $G = A + F * (F - A)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(G) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(G,x) = \mathrm{eval}(A,x) + (\mathrm{eval}(F,x)) \cdot (\mathrm{eval}(F,x) - \mathrm{eval}(A,x))$. Reconsider $H = B + T_2 \cdot ((P_{10} - O) * C)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(H) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(H,x) = \mathrm{eval}(B,x) + T_2 \cdot (x_{/j} - 1_{\mathbb{R}_\mathrm{F}}) \cdot (\mathrm{eval}(C,x))$. Reconsider $I = (G*G-O)*(H*H)+O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(I) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(I,x) = ((\mathrm{eval}(G,x))^{\mathbf{2}} - 1_{\mathbb{R}_\mathrm{F}}) \cdot (\mathrm{eval}(H,x))^{\mathbf{2}} + 1_{\mathbb{R}_\mathrm{F}}$.

Reconsider $X_1 = (M*M-O)*(S*S)+O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(X_1) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(X_1,x) = ((\mathrm{eval}(M,x))^{\mathbf{2}} - 1_{\mathbb{R}_\mathrm{F}}) \cdot (\mathrm{eval}(S,x))^{\mathbf{2}} + 1_{\mathbb{R}_\mathrm{F}}$. Reconsider $X_2 = ((M*U)*(M*U)-O)*(T*T)+O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(X_2) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(X_2,x) = (((\mathrm{eval}(M,x)) \cdot (\mathrm{eval}(U,x)))^{\mathbf{2}} - 1_{\mathbb{R}_\mathrm{F}}) \cdot (\mathrm{eval}(T,x))^{\mathbf{2}} + 1_{\mathbb{R}_\mathrm{F}}$. Reconsider $X_3 = (D * F) * I$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(X_3) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(X_3,x) = (\mathrm{eval}(D,x)) \cdot (\mathrm{eval}(F,x)) \cdot (\mathrm{eval}(I,x))$. Reconsider $P = F * L$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(P) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(P,x) = (\mathrm{eval}(F,x)) \cdot (\mathrm{eval}(L,x))$. Reconsider $R = (H - C) * L + (F * (P_9 + O)) * Q + (F * (P_{11} + O)) * (((W * W - O) * S) * P_{17} - (W * W) * (P_{17} * P_{17}) + O)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(R) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(R,x) = (\mathrm{eval}(H,x) - \mathrm{eval}(C,x)) \cdot (\mathrm{eval}(L,x)) + (\mathrm{eval}(F,x)) \cdot (x_{/f} + 1_{\mathbb{R}_\mathrm{F}}) \cdot (\mathrm{eval}(Q,x)) + (\mathrm{eval}(F,x)) \cdot (x_{/k} + 1_{\mathbb{R}_\mathrm{F}}) \cdot (((\mathrm{eval}(W,x))^{\mathbf{2}} - 1_{\mathbb{R}_\mathrm{F}}) \cdot (\mathrm{eval}(S,x)) \cdot (x_{/u}) - (\mathrm{eval}(W,x))^{\mathbf{2}} \cdot (x_{/u})^{\mathbf{2}} + 1_{\mathbb{R}_\mathrm{F}})$.

Reconsider $E_4 = 8$ as an integer element of $\mathbb{R}_\mathrm{F}$. Reconsider $V_1 = E_4 \cdot ((((P_9 * P_{17}) * S) * T) * (P_{14} - ((P_{12} * S) * T) * U))$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(V_1) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(V_1,x) = E_4 \cdot (x_{/f} \cdot (x_{/u}) \cdot (\mathrm{eval}(S,x)) \cdot (\mathrm{eval}(T,x)) \cdot (x_{/r} - x_{/m} \cdot (\mathrm{eval}(S,x)) \cdot (\mathrm{eval}(T,x)) \cdot (\mathrm{eval}(U,x))))$. Reconsider $F_4 = 4$ as an integer element of $\mathbb{R}_\mathrm{F}$. Reconsider $V_2 = F_4 \cdot (((P_{17} * P_{17}) * (S * S)) * (T * T))$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(V_2) \subseteq V_4$. For every function x from N into $\mathbb{R}_\mathrm{F}$, $\mathrm{eval}(V_2,x) = F_4 \cdot (x_{/u})^{\mathbf{2}} \cdot (\mathrm{eval}(S,x))^{\mathbf{2}} \cdot (\mathrm{eval}(T,x))^{\mathbf{2}}$. Reconsider $V_3 = (F_4 \cdot (P_9 * P_9) - O) * ((P_{14} - ((P_{12} * S) * T) * U) * (P_{14} - ((P_{12} * S) * T) * U))$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_\mathrm{F}$. $\mathrm{vars}(V_3) \subseteq V_4$. For every function x

from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(V_3, x) = (F_4 \cdot (x_{/f})^{\mathbf{2}} - 1_{\mathbb{R}_{\mathrm{F}}}) \cdot (x_{/r} - x_{/m} \cdot (\mathrm{eval}(S, x)) \cdot (\mathrm{eval}(T, x)) \cdot (\mathrm{eval}(U, x)))^{\mathbf{2}}$. Reconsider $N_1 = M * S + T_2 \cdot ((M * U) * T)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(N_1) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(N_1, x) = (\mathrm{eval}(M, x)) \cdot (\mathrm{eval}(S, x)) + T_2 \cdot (\mathrm{eval}(M, x)) \cdot (\mathrm{eval}(U, x)) \cdot (\mathrm{eval}(T, x))$.

Reconsider $N_2 = F_4 \cdot (((((A * A) * C) * E) * G) * H)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(N_2) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$, $\mathrm{eval}(N_2, x) = F_4 \cdot ((\mathrm{eval}(A, x)) \cdot (\mathrm{eval}(A, x)) \cdot (\mathrm{eval}(C, x)) \cdot (\mathrm{eval}(E, x)) \cdot (\mathrm{eval}(G, x)) \cdot (\mathrm{eval}(H, x)))$. Reconsider $V = V_1 - V_2 - V_3 - O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. Reconsider $N_3 = N_1 + N_2 + R + O$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(V) \subseteq V_4$. $\mathrm{vars}(N_3) \subseteq V_4$. For every function x from N into $\mathbb{R}_{\mathrm{F}}$ such that $x_{/k}$ is a positive natural number and $x_{/f}$ is a positive natural number and $x_{/i}$ is a positive natural number and $x_{/j}$ is a positive natural number and $x_{/m}$ is a positive natural number and $x_{/u}$ is a positive natural number and $x_{/r}$ is a natural number and $x_{/s}$ is a natural number and $x_{/t}$ is a natural number holds $\mathrm{eval}(X_1, x)$ is an odd natural number and $\mathrm{eval}(X_2, x)$ is an odd natural number and $\mathrm{eval}(X_3, x)$ is a natural number and $\mathrm{eval}(P, x)$ is a positive natural number and $\mathrm{eval}(R, x)$ is a natural number and $\mathrm{eval}(N_3, x)$ is a natural number and $\mathrm{eval}(N_3, x) > \sqrt{\mathrm{eval}(X_1, x)} + 2 \cdot \sqrt{\mathrm{eval}(X_2, x)} + 4 \cdot \sqrt{\mathrm{eval}(X_3, x)} + \mathrm{eval}(R, x)$.

Consider K_3 being a $\mathbb{Z}$-valued polynomial of 8,$\mathbb{R}_{\mathrm{F}}$ such that for every natural numbers x_1, x_2, x_3, P, R, N and for every integer V such that x_1 is odd and x_2 is odd and $P > 0$ and $N > \sqrt{x_1} + 2 \cdot \sqrt{x_2} + 4 \cdot \sqrt{x_3} + R$ holds x_1 is a square and x_2 is a square and x_3 is a square and $P \mid R$ and $V \geqslant 0$ iff there exists a natural number z such that for every function f from 8 into $\mathbb{R}_{\mathrm{F}}$ such that $f = \langle z, x_1, 4 \cdot x_2, 16 \cdot x_3 \rangle \frown \langle R, P, N, V \rangle$ holds $\mathrm{eval}(K_3, f) = 0$. Consider Z being a polynomial of $8 + 9$,$\mathbb{R}_{\mathrm{F}}$ such that $\mathrm{rng}\, Z \subseteq \mathrm{rng}\, K_3 \cup \{0_{\mathbb{R}_{\mathrm{F}}}\}$ and for every bag b of $8 + 9$, $b \in \mathrm{Support}\, Z$ iff $b \restriction 8 \in \mathrm{Support}\, K_3$ and for every i such that $i \geqslant 8$ holds $b(i) = 0$ and for every bag b of $8 + 9$ such that $b \in \mathrm{Support}\, Z$ holds $Z(b) = K_3(b \restriction 8)$ and for every function x from 8 into $\mathbb{R}_{\mathrm{F}}$ and for every function y from $8 + 9$ into $\mathbb{R}_{\mathrm{F}}$ such that $y \restriction 8 = x$ holds $\mathrm{eval}(K_3, x) = \mathrm{eval}(Z, y)$. Reconsider $Z_1 = \mathrm{Subst}(Z, 1, X_1)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. Reconsider $Z_2 = \mathrm{Subst}(Z_1, 2, F_4 \cdot X_2)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. Reconsider $Z_3 = \mathrm{Subst}(Z_2, 3, F_4 \cdot F_4 \cdot X_3)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. Reconsider $Z_4 = \mathrm{Subst}(Z_3, 4, R)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. Reconsider $Z_5 = \mathrm{Subst}(Z_4, 5, P)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. Reconsider $Z_6 = \mathrm{Subst}(Z_5, 6, N_3)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$. Reconsider $Z_7 = \mathrm{Subst}(Z_6, 7, V)$ as a $\mathbb{Z}$-valued polynomial of N,$\mathbb{R}_{\mathrm{F}}$.

For every natural number x_8 such that $x_8 > 0$ holds $x_8 + 1$ is prime iff there exists a $\mathbb{Z}$-valued function x from N into $\mathbb{R}_{\mathrm{F}}$ such that $x_{/k} = x_8$ and $x_{/f}$ is a positive natural number and $x_{/i}$ is a positive natural number and $x_{/j}$ is a positive natural number and $x_{/m}$ is a positive natural number and $x_{/u}$ is a positive natural number and $x_{/r}$ is a natural number and $x_{/s}$ is a natural number and $x_{/t}$ is a natural number and $x_{/0}$ is a natural number and $\mathrm{eval}(Z_7, x) = 0_{\mathbb{R}_{\mathrm{F}}}$ by [7, (23)]. $\mathrm{vars}(Z) \subseteq 8$. $\mathrm{vars}(Z_1) \subseteq (\mathrm{vars}(Z)) \setminus \{1\} \cup \mathrm{vars}(X_1)$. $\mathrm{vars}(F_4 \cdot X_2) \subseteq V_4$. $\mathrm{vars}(Z_2) \subseteq (\mathrm{vars}(Z_1)) \setminus \{2\} \cup \mathrm{vars}(F_4 \cdot X_2)$. $\mathrm{vars}(F_4 \cdot F_4 \cdot X_3) \subseteq V_4$. $\mathrm{vars}(Z_3) \subseteq (\mathrm{vars}(Z_2)) \setminus \{3\} \cup \mathrm{vars}(F_4 \cdot F_4 \cdot X_3)$. $\mathrm{vars}(Z_4) \subseteq (\mathrm{vars}(Z_3)) \setminus \{4\} \cup \mathrm{vars}(R)$. $\mathrm{vars}(Z_5) \subseteq (\mathrm{vars}(Z_4)) \setminus \{5\} \cup \mathrm{vars}(P)$. $\mathrm{vars}(Z_6) \subseteq (\mathrm{vars}(Z_5)) \setminus \{6\} \cup \mathrm{vars}(N_3)$. $\mathrm{vars}(Z_7) \subseteq (\mathrm{vars}(Z_6)) \setminus \{7\} \cup \mathrm{vars}(V)$. $\square$

(83) Let us consider a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure L, and a polynomial p of $n+m$,L. Suppose $\mathrm{vars}(p) \subseteq n$. Then there exists a polynomial q of n,L such that

(i) $\mathrm{vars}(q) \subseteq n$, and

(ii) $\mathrm{rng}\, q \subseteq \mathrm{rng}\, p$, and

(iii) for every bag b of $n+m$, $b \restriction n \in \mathrm{Support}\, q$ and for every i such that $i \geqslant n$ holds $b(i) = 0$ iff $b \in \mathrm{Support}\, p$, and

(iv) for every bag b of $n+m$ such that $b \in \mathrm{Support}\, p$ holds $q(b \restriction n) = p(b)$, and

(v) for every function x from $n+m$ into L and for every function y from n into L such that $x \restriction n = y$ holds $\mathrm{eval}(p, x) = \mathrm{eval}(q, y)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \$_1 \leqslant m$ and there exists a polynomial q of $n + \$_1$,$L$ such that $\mathrm{vars}(q) \subseteq n$ and $\mathrm{rng}\, q \subseteq \mathrm{rng}\, p$ and for every bag b of $n+m$, $b \restriction (n + \$_1) \in \mathrm{Support}\, q$ and for every i such that $i \geqslant n + \$_1$ holds $b(i) = 0$ iff $b \in \mathrm{Support}\, p$ and for every bag b of $n+m$ such that $b \in \mathrm{Support}\, p$ holds $q(b \restriction (n + \$_1)) = p(b)$ and for every function x from $n+m$ into L and for every function y from $n + \$_1$ into L such that $x \restriction (n + \$_1) = y$ holds $\mathrm{eval}(p, x) = \mathrm{eval}(q, y)$. There exists k such that $\mathcal{P}[k]$. For every natural number k such that $k \neq 0$ and $\mathcal{P}[k]$ there exists a natural number n such that $n < k$ and $\mathcal{P}[n]$. $\mathcal{P}[0]$. $\square$

(84) Let us consider an ordinal number X, a non empty zero structure L, a series s of X, L, and a permutation p_4 of X. Then vars(the s permuted by p_4) $\subseteq p_4{}^{\circ}(\mathrm{vars}(s))$.

(85) Prime Representing Polynomial with 10 Variables:
There exists a $\mathbb{Z}$-valued polynomial P_{13} of 10,$\mathbb{R}_{\mathrm{F}}$ such that for every positive natural number k, $k+1$ is prime iff there exists a natural-valued function v from 10 into $\mathbb{R}_{\mathrm{F}}$ such that $v(1) = k$ and $\mathrm{eval}(P_{13}, v) = 0_{\mathbb{R}_{\mathrm{F}}}$.

Proof: Consider p_1 being a $\mathbb{Z}$-valued polynomial of $17,\mathbb{R}_{\mathrm{F}}$ such that $\mathrm{vars}(p_1) \subseteq \{0\} \cup 17 \setminus 8$ and for every natural number x_8 such that $x_8 > 0$ holds x_8+1 is prime iff there exists a $\mathbb{Z}$-valued function x from 17 into $\mathbb{R}_{\mathrm{F}}$ such that $x_{/8} = x_8$ and $x_{/9}$ is a positive natural number and $x_{/10}$ is a positive natural number and $x_{/11}$ is a positive natural number and $x_{/12}$ is a positive natural number and $x_{/13}$ is a positive natural number and $x_{/14}$ is a natural number and $x_{/15}$ is a natural number and $x_{/16}$ is a natural number and $x_{/0}$ is a natural number and $\mathrm{eval}(p_1, x) = 0_{\mathbb{R}_{\mathrm{F}}}$. Set $N = 16$. Set $I_2 = \mathrm{idseq}(N)$. Set $E = 9$. Set $I_1 = \mathrm{idseq}(E)$. Consider f being a finite sequence such that $I_2 = I_1 {}^\frown f$. Set $R = f {}^\frown I_1$. Set $Z = \mathrm{id}_{\{0\}}$. Set $R_2 = R {+\cdot} Z$. $\mathbb{Z}_{17} \setminus (\mathrm{rng}\, f) \subseteq \mathbb{Z}_{10}$. For every i such that $1 \leqslant i \leqslant 9$ holds $(R_2{}^{-1})(i) = i+7$ and $R_2(i+7) = i$. Set $P_2 =$ the p_1 permuted by R_2. Reconsider $p_2 = P_2$ as a $\mathbb{Z}$-valued polynomial of $10+7,\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(p_2) \subseteq R_2{}^\circ(\mathrm{vars}(p_1))$.

Consider p_3 being a polynomial of $10,\mathbb{R}_{\mathrm{F}}$ such that $\mathrm{vars}(p_3) \subseteq 10$ and $\mathrm{rng}\, p_3 \subseteq \mathrm{rng}\, p_2$ and for every bag b of $10+7$, $b{\restriction}10 \in \mathrm{Support}\, p_3$ and for every i such that $i \geqslant 10$ holds $b(i) = 0$ iff $b \in \mathrm{Support}\, p_2$ and for every bag b of $10+7$ such that $b \in \mathrm{Support}\, p_2$ holds $p_3(b{\restriction}10) = p_2(b)$ and for every function x from $10+7$ into $\mathbb{R}_{\mathrm{F}}$ and for every function y from 10 into $\mathbb{R}_{\mathrm{F}}$ such that $x{\restriction}10 = y$ holds $\mathrm{eval}(p_2, x) = \mathrm{eval}(p_3, y)$. For every natural number x_8 such that $x_8 > 0$ holds x_8+1 is prime iff there exists a $\mathbb{Z}$-valued function x from 10 into $\mathbb{R}_{\mathrm{F}}$ such that $x(0)$ is a natural number and $x(1) = x_8$ and $x(2)$ is a positive natural number and $x(3)$ is a positive natural number and $x(4)$ is a positive natural number and $x(5)$ is a positive natural number and $x(6)$ is a positive natural number and $x(7)$ is a natural number and $x(8)$ is a natural number and $x(9)$ is a natural number and $\mathrm{eval}(p_3, x) = 0_{\mathbb{R}_{\mathrm{F}}}$. Set $E_2 = \mathrm{EmptyBag}\, 10$. Set $O = 1\_(10, \mathbb{R}_{\mathrm{F}})$. Set $P_2 = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (2,1)) + O$. Set $P_3 = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (3,1)) + O$. Set $P_4 = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (4,1)) + O$. Set $P_5 = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (5,1)) + O$. Set $P_6 = \mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (6,1)) + O$.

Reconsider $Z_2 = \mathrm{Subst}(p_3, 2, P_2)$ as a $\mathbb{Z}$-valued polynomial of $10,\mathbb{R}_{\mathrm{F}}$. Reconsider $Z_3 = \mathrm{Subst}(Z_2, 3, P_3)$ as a $\mathbb{Z}$-valued polynomial of $10,\mathbb{R}_{\mathrm{F}}$. Reconsider $Z_4 = \mathrm{Subst}(Z_3, 4, P_4)$ as a $\mathbb{Z}$-valued polynomial of $10,\mathbb{R}_{\mathrm{F}}$. Reconsider $Z_5 = \mathrm{Subst}(Z_4, 5, P_5)$ as a $\mathbb{Z}$-valued polynomial of $10,\mathbb{R}_{\mathrm{F}}$. Reconsider $Z_6 = \mathrm{Subst}(Z_5, 6, P_6)$ as a $\mathbb{Z}$-valued polynomial of $10,\mathbb{R}_{\mathrm{F}}$. $\mathrm{vars}(O) = \emptyset$. $\mathrm{vars}(\mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (5,1))) \cup \mathrm{vars}(O) \subseteq \{5\} \cup \emptyset$. $\mathrm{vars}(P_5) \subseteq \mathrm{vars}(\mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (5,1))) \cup \mathrm{vars}(O)$. $\mathrm{vars}(\mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (4,1))) \cup \mathrm{vars}(O) \subseteq \{4\} \cup \emptyset$. $\mathrm{vars}(P_4) \subseteq \mathrm{vars}(\mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (4,1))) \cup \mathrm{vars}(O)$. $\mathrm{vars}(\mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (3,1))) \cup \mathrm{vars}(O) \subseteq \{3\} \cup \emptyset$. $\mathrm{vars}(P_3) \subseteq \mathrm{vars}(\mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (3,1))) \cup \mathrm{vars}(O)$. $\mathrm{vars}(\mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (2,1))) \cup \mathrm{vars}(O) \subseteq \{2\} \cup \emptyset$. $\mathrm{vars}(P_2) \subseteq \mathrm{vars}(\mathrm{Monom}(1_{\mathbb{R}_{\mathrm{F}}}, E_2 {+\cdot} (2,1))) \cup \mathrm{vars}(O)$.

If $k+1$ is prime, then there exists a natural-valued function v from 10 into $\mathbb{R}_{\mathrm{F}}$ such that $v(1)=k$ and $\mathrm{eval}(Z_6,v)=0_{\mathbb{R}_{\mathrm{F}}}$. Set $V_{10}=VV+\cdot(6,\mathrm{eval}(P_6,VV))$. $\mathrm{eval}(Z_6,VV)=\mathrm{eval}(Z_5,V_{10})$. Set $V_9=V_{10}+\cdot(5,\mathrm{eval}(P_5,VV))$. $\mathrm{eval}(P_5,V_{10})=\mathrm{eval}(P_5,VV)$. $\mathrm{eval}(Z_5,V_{10})=\mathrm{eval}(Z_4,V_9)$. Set $V_8=V_9+\cdot(4,\mathrm{eval}(P_4,VV))$. $\mathrm{eval}(P_4,V_9)=\mathrm{eval}(P_4,V_{10})$. $\mathrm{eval}(Z_4,V_9)=\mathrm{eval}(Z_3,V_8)$.Set $V_7=V_8+\cdot(3,\mathrm{eval}(P_3,VV))$. $\mathrm{eval}(P_3,V_8)=\mathrm{eval}(P_3,V_9)$. $\mathrm{eval}(Z_3,V_8)=\mathrm{eval}(Z_2,V_7)$. Set $V_6=V_7+\cdot(2,\mathrm{eval}(P_2,VV))$. $\mathrm{eval}(P_2,V_7)=\mathrm{eval}(P_2,V_8)$. $\mathrm{eval}(Z_2,V_7)=\mathrm{eval}(p_3,V_6)$. For every natural number y such that $y=0$ or $y=1$ or $y=7$ or $y=8$ or $y=9$ holds $V_6(y)=VV(y)$. $\square$

References

[1] 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.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Artur Korniłowicz and Adam Naumowicz. Niven's theorem. *Formalized Mathematics*, 24 (**4**):301–308, 2016. doi:10.1515/forma-2016-0026.

[4] Yuri Matiyasevich. Primes are nonnegative values of a polynomial in 10 variables. *Journal of Soviet Mathematics*, 15:33–44, 1981. doi:10.1007/BF01404106.

[5] Karol Pąk. Diophantine sets. Preliminaries. *Formalized Mathematics*, 26(**1**):81–90, 2018. doi:10.2478/forma-2018-0007.

[6] Karol Pąk. Prime representing polynomial with 10 unknowns – Introduction. *Formalized Mathematics*, 30(**3**):169–198, 2022. doi:10.2478/forma-2022-0013.

[7] Karol Pąk. Prime representing polynomial with 10 unknowns – Introduction. Part II. *Formalized Mathematics*, 30(**4**):245–253, 2022. doi:10.2478/forma-2022-0020.

[8] Karol Pąk and Cezary Kaliszyk. Formalizing a diophantine representation of the set of prime numbers. In June Andronick and Leonardo de Moura, editors, *13th International Conference on Interactive Theorem Proving, ITP 2022, August 7-10, 2022, Haifa, Israel*, volume 237 of *LIPIcs*, pages 26:1–26:8. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. doi:10.4230/LIPIcs.ITP.2022.26.

[9] Christoph Schwarzweller and Artur Korniłowicz. Characteristic of rings. Prime fields. *Formalized Mathematics*, 23(**4**):333–349, 2015. doi:10.1515/forma-2015-0027.

Accepted December 27, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 4, Pages 281–294, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0022

sciendo
sciendo.com/journal/forma

Existence and Uniqueness of Algebraic Closures

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. This is the second part of a two-part article formalizing existence and uniqueness of algebraic closures, using the Mizar [2], [1] formalism. Our proof follows Artin's classical one as presented by Lang in [3]. In the first part we proved that for a given field F there exists a field extension E such that every non-constant polynomial $p \in F[X]$ has a root in E. Artin's proof applies Kronecker's construction to each polynomial $p \in F[X] \backslash F$ simultaneously. To do so we needed the polynomial ring $F[X_1, X_2, ...]$ with infinitely many variables, one for each polynomal $p \in F[X] \backslash F$. The desired field extension E then is $F[X_1, X_2, ...] \backslash I$, where I is a maximal ideal generated by all non-constant polynomials $p \in F[X]$. Note, that to show that I is maximal Zorn's lemma has to be applied.

In this second part this construction is iterated giving an infinite sequence of fields, whose union establishes a field extension A of F, in which every non-constant polynomial $p \in A[X]$ has a root. The field of algebraic elements of A then is an algebraic closure of F. To prove uniqueness of algebraic closures, e.g. that two algebraic closures of F are isomorphic over F, the technique of extending monomorphisms is applied: a monomorphism $F \longrightarrow A$, where A is an algebraic closure of F can be extended to a monomorphism $E \longrightarrow A$, where E is any algebraic extension of F. In case that E is algebraically closed this monomorphism is an isomorphism. Note that the existence of the extended monomorphism again relies on Zorn's lemma.

MSC: 12F05 68V20

Keywords: algebraic closures; polynomial rings with countably infinite number of variables; Emil Artin

MML identifier: FIELD_12, version: 8.1.12 5.72.1435

1. Preliminaries

Let L be a non empty double loop structure. One can verify that the double loop structure of L is non empty. Let L be a non trivial double loop structure. One can verify that the double loop structure of L is non trivial. Let L be a non degenerated double loop structure. One can verify that the double loop structure of L is non degenerated. Let L be an add-associative double loop structure. One can check that the double loop structure of L is add-associative.

Let L be a right zeroed double loop structure. Let us note that the double loop structure of L is right zeroed. Let L be a right complementable double loop structure. Observe that the double loop structure of L is right complementable. Let L be an Abelian double loop structure. Let us observe that the double loop structure of L is Abelian. Let L be an associative double loop structure. One can check that the double loop structure of L is associative.

Let L be a well unital, non empty double loop structure. Observe that the double loop structure of L is well unital. Let L be a left distributive, non empty double loop structure. One can check that the double loop structure of L is left distributive. Let L be a right distributive, non empty double loop structure. Observe that the double loop structure of L is right distributive. Let L be a commutative double loop structure. One can verify that the double loop structure of L is commutative.

Let L be an integral domain-like, non empty double loop structure. Let us note that the double loop structure of L is integral domain-like. Let L be an almost left invertible double loop structure. Observe that the double loop structure of L is almost left invertible. Now we state the proposition:

(1) Let us consider a field F. Then the double loop structure of $F \approx F$.

Let F be a field. Let us note that there exists an extension of F which is strict. Let L be an F-monomorphic field. Let us note that there exists an extension of L which is F-homomorphic and F-monomorphic and there exists an element of the carrier of $\mathrm{PolyRing}(F)$ which is monic and irreducible. Let F be a non algebraic closed field. Observe that there exists an element of the carrier of $\mathrm{PolyRing}(F)$ which is monic and non constant and has not roots. Now we state the propositions:

(2) Let us consider a field F_1, an F_1-monomorphic, F_1-homomorphic field F_2, a monomorphism h of F_1 and F_2, and an element p of the carrier of $\mathrm{PolyRing}(F_1)$. Then $(\mathrm{PolyHom}(h))(-p) = -(\mathrm{PolyHom}(h))(p)$.

(3) Let us consider a field F_1, an F_1-monomorphic, F_1-homomorphic field F_2, a monomorphism h of F_1 and F_2, and elements p, q of the carrier of $\mathrm{PolyRing}(F_1)$. If $p \mid q$, then $(\mathrm{PolyHom}(h))(p) \mid (\mathrm{PolyHom}(h))(q)$.

Let F_1 be a field, F_2 be an F_1-monomorphic, F_1-homomorphic field, h be a monomorphism of F_1 and F_2, and p be a non constant element of the carrier of PolyRing(F_1). Let us observe that (PolyHom(h))(p) is non constant as an element of the carrier of PolyRing(F_2).

Let R be a GCD domain and a, b be elements of R. We say that a and b are relatively prime if and only if

(Def. 1) 1_R is a GCD of a and b.

Let us consider a field F and elements p, q of the carrier of PolyRing(F). Now we state the propositions:

(4) p and q are relatively prime if and only if $\gcd(p, q) = \mathbf{1}.F$.

(5) If p and q are relatively prime, then p and q have no common roots.

(6) Let us consider a field F, and an element p of the carrier of PolyRing(F). Then there exists an extension E of F and there exists an F-algebraic element a of E such that $p = \mathrm{MinPoly}(a, F)$ if and only if p is monic and irreducible.

(7) Let us consider a field F, and an irreducible element p of the carrier of PolyRing(F). Then there exists an F-finite extension E of F such that

(i) $\deg(E, F) = \deg(p)$, and

(ii) p has a root in E.

The theorem is a consequence of (6).

(8) Let us consider a field F, and a non constant element p of the carrier of PolyRing(F). Then there exists an F-finite extension E of F such that

(i) p has a root in E, and

(ii) $\deg(E, F) \leqslant \deg(p)$.

The theorem is a consequence of (7).

(9) Let us consider a field F, an F-algebraic extension E of F, an E-extending extension K of F, and an element a of K. If a is E-algebraic, then a is F-algebraic.

(10) Let us consider fields F_1, F_2, L, an extension E_1 of F_1, a E_1-extending extension K_1 of F_1, a function h_1 from F_1 into L, a function h_2 from E_1 into L, and a function h_3 from K_1 into L. Suppose h_2 is h_1-extending and h_3 is h_2-extending. Then h_3 is h_1-extending.

Let F be a field. Let us observe that every extension of F is F-monomorphic and F-homomorphic.

Let E be an extension of F. Let us note that there exists a field which is E-homomorphic, E-monomorphic, F-homomorphic, and F-monomorphic.

2. Sequences of Fields

A sequence is a function defined by

(Def. 2) dom $it = \mathbb{N}$.

Let us observe that every sequence is $\mathbb{N}$-defined.

Let f be a binary relation. We say that f is field-yielding if and only if

(Def. 3) for every object x such that $x \in \operatorname{rng} f$ holds x is a field.

Observe that there exists a sequence which is field-yielding and every function which is field-yielding is also 1-sorted yielding.

Let f be a field-yielding sequence and i be an element of $\mathbb{N}$. One can check that the functor $f(i)$ yields a field. Let i be a natural number. Observe that the functor $f(i)$ yields a field.

The scheme *RecExField* deals with a field $\mathcal{A}$ and a ternary predicate $\mathcal{P}$ and states that

(Sch. 1) There exists a field-yielding sequence f such that $f(0) = \mathcal{A}$ and for every natural number n, $\mathcal{P}[n, f(n), f(n+1)]$

provided

- for every natural number n and for every field x, there exists a field y such that $\mathcal{P}[n, x, y]$.

Let f be a field-yielding sequence. We say that f is ascending if and only if

(Def. 4) for every element i of $\mathbb{N}$, $f(i+1)$ is an extension of $f(i)$.

Note that there exists a field-yielding sequence which is ascending.

Let f be a field-yielding sequence. The support of f yielding a non empty set is defined by the term

(Def. 5) $\bigcup$the set of all the carrier of $f(i)$ where i is an element of $\mathbb{N}$.

Now we state the propositions:

(11) Let us consider an ascending, field-yielding sequence f, elements i, j of $\mathbb{N}$, and an element a of $f(i)$. If $i \leqslant j$, then $a \in$ the carrier of $f(j)$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ there exists an element k of $\mathbb{N}$ such that $k = i + \$_1$ and $a \in$ the carrier of $f(k)$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $i + n = j$. □

(12) Let us consider an ascending, field-yielding sequence f, and elements i, j of $\mathbb{N}$. If $i \leqslant j$, then $f(j)$ is an extension of $f(i)$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ there exists an element k of $\mathbb{N}$ such that $k = i + \$_1$ and $f(k)$ is an extension of $f(i)$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $i + n = j$. □

(13) Let us consider an ascending, field-yielding sequence f, elements i, j of $\mathbb{N}$, elements x_2, y_2 of $f(i)$, and elements x_3, y_3 of $f(j)$. Suppose $x_2 = x_3$ and $y_2 = y_3$. Then

(i) $x_2 + y_2 = x_3 + y_3$, and

(ii) $x_2 \cdot y_2 = x_3 \cdot y_3$.

The theorem is a consequence of (12).

Let f be an ascending, field-yielding sequence. The functor addseq(f) yielding a binary operation on the support of f is defined by

(Def. 6) for every elements a, b of the support of f, there exists an element i of $\mathbb{N}$ and there exist elements x, y of $f(i)$ such that $x = a$ and $y = b$ and $it(a, b) = x + y$.

The functor multseq(f) yielding a binary operation on the support of f is defined by

(Def. 7) for every elements a, b of the support of f, there exists an element i of $\mathbb{N}$ and there exist elements x, y of $f(i)$ such that $x = a$ and $y = b$ and $it(a, b) = x \cdot y$.

The functor SeqField(f) yielding a strict double loop structure is defined by

(Def. 8) the carrier of it = the support of f and the addition of it = addseq(f) and the multiplication of it = multseq(f) and the one of $it = 1_{f(0)}$ and the zero of $it = 0_{f(0)}$.

Now we state the propositions:

(14) Let us consider an ascending, field-yielding sequence f, and an element i of $\mathbb{N}$. Then

(i) $1_{\mathrm{SeqField}(f)} = 1_{f(i)}$, and

(ii) $0_{\mathrm{SeqField}(f)} = 0_{f(i)}$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ there exists an element k of $\mathbb{N}$ such that $k = \$_1$ and $1_{f(k)} = 1_{f(0)}$ and $0_{f(k)} = 0_{f(0)}$. For every natural number k, $\mathcal{P}[k]$. $\square$

(15) Let us consider an ascending, field-yielding sequence f, elements a, b of SeqField(f), an element i of $\mathbb{N}$, and elements x, y of $f(i)$. If $x = a$ and $y = b$, then $a + b = x + y$ and $a \cdot b = x \cdot y$. The theorem is a consequence of (13).

Let f be an ascending, field-yielding sequence. Observe that SeqField(f) is non degenerated and SeqField(f) is Abelian, add-associative, right zeroed, and right complementable and SeqField(f) is commutative, associative, well unital, distributive, and almost left invertible. Now we state the propositions:

(16) Let us consider an ascending, field-yielding sequence f, and an element i of $\mathbb{N}$. Then $f(i)$ is a subfield of SeqField(f).
PROOF: Set $F = f(i)$. Set $K = \text{SeqField}(f)$. The addition of $F =$ (the addition of K) $\restriction$ (the carrier of F). The multiplication of $F =$ (the multiplication of K) $\restriction$ (the carrier of F). $1_F = 1_K$ and $0_F = 0_K$. $\square$

(17) Let us consider a field E, and an ascending, field-yielding sequence f. Suppose for every element i of $\mathbb{N}$, $f(i)$ is a subfield of E. Then SeqField(f) is a subfield of E.
PROOF: Set $F = \text{SeqField}(f)$. The carrier of $F \subseteq$ the carrier of K. The addition of $F =$ (the addition of K) $\restriction$ (the carrier of F). The multiplication of $F =$ (the multiplication of K) $\restriction$ (the carrier of F). $\square$

(18) Let us consider an ascending, field-yielding sequence f, and a finite subset X of SeqField(f). Then there exists an element i of $\mathbb{N}$ such that $X \subseteq$ the carrier of $f(i)$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset X of SeqField(f) such that $\overline{\overline{X}} = \$_1$ there exists an element i of $\mathbb{N}$ such that $X \subseteq$ the carrier of $f(i)$. $\mathcal{P}[0]$. $\mathcal{P}[1]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{X}} = n$. Consider i being an element of $\mathbb{N}$ such that $X \subseteq$ the carrier of $f(i)$. $\square$

3. Maximal Algebraic and Algebraic Closed Fields

Let F be a field. We say that F is maximal algebraic if and only if

(Def. 9) for every F-algebraic extension E of F, $E \approx F$.

Let us consider a field F. Now we state the propositions:

(19) F is maximal algebraic if and only if F is algebraic closed. The theorem is a consequence of (7).

(20) F is algebraic closed if and only if every non constant polynomial over F has roots.

(21) F is algebraic closed if and only if for every irreducible element p of the carrier of PolyRing(F), $\deg(p) = 1$.

(22) F is algebraic closed if and only if for every non constant polynomial p over F, p splits in F.

(23) F is algebraic closed if and only if every non constant, monic polynomial over F is a product of linear polynomials of F.

(24) F is algebraic closed if and only if for every elements p, q of the carrier of PolyRing(F), p and q are relatively prime iff p and q have no common roots. The theorem is a consequence of (4) and (5).

(25) F is algebraic closed if and only if for every F-algebraic extension E of F, $E \approx F$. The theorem is a consequence of (19).

(26) F is algebraic closed if and only if for every F-finite extension E of F, $E \approx F$. The theorem is a consequence of (19).

Let us note that every field which is algebraic closed is also infinite.

4. Existence of Algebraic Closures

Let F be a field. A closure sequence of F is an ascending, field-yielding sequence defined by

(Def. 10) $it(0) = F$ and for every element i of $\mathbb{N}$ and for every field K and for every extension E of K such that $K = it(i)$ and $E = it(i+1)$ for every non constant element p of the carrier of PolyRing(K), p has a root in E.

Now we state the proposition:

(27) Let us consider an ascending, field-yielding sequence f, and a polynomial p over SeqField(f). Then there exists an element i of $\mathbb{N}$ such that p is a polynomial over $f(i)$. The theorem is a consequence of (18) and (16).

Let F be a field and f be a closure sequence of F. Let us observe that SeqField(f) is F-extending and SeqField(f) is algebraic closed.

Now we state the proposition:

(28) Let us consider a field F. Then there exists an extension E of F such that E is algebraic closed.

Let F be a field. An algebraic closure of F is an extension of F defined by

(Def. 11) it is F-algebraic and algebraic closed.

Note that every algebraic closure of F is F-algebraic and algebraic closed and there exists an algebraic closed field which is F-homomorphic and F-monomorphic. Now we state the propositions:

(29) Let us consider a field F. Then there exists a field E such that E is an algebraic closure of F.

(30) Let us consider a field F, and an F-algebraic extension E of F. Then there exists an algebraic closure A of F such that E is a subfield of A.

Let F be a field and E be an F-algebraic extension of F. Let us observe that there exists an algebraic closure of F which is E-extending.

Now we state the propositions:

(31) Let us consider a field F, and an F-algebraic extension E of F. Then every algebraic closure of E is an algebraic closure of F.

(32) Let us consider a field F, an extension E of F, and an algebraic closure A of F. If A is E-extending, then A is an algebraic closure of E.

(33) Let us consider a field F, and algebraic closures A_1, A_2 of F. If A_1 is A_2-extending, then $A_2 \approx A_1$. The theorem is a consequence of (25).

5. Some More Preliminaries

Let R be a ring and S be an R-homomorphic ring. Observe that there exists a ring which is S-homomorphic and R-homomorphic.

Let T be an S-homomorphic ring, f be an additive function from R into S, and g be an additive function from S into T. Let us note that $g \cdot f$ is additive as a function from R into T.

Let f be a multiplicative function from R into S and g be a multiplicative function from S into T. Let us note that $g \cdot f$ is multiplicative as a function from R into T.

Let f be a unity-preserving function from R into S and g be a unity-preserving function from S into T. Let us note that $g \cdot f$ is unity-preserving as a function from R into T. Now we state the propositions:

(34) Let us consider a field F, and an extension E of F. Then id_F is a monomorphism of F and E.

Proof: Reconsider $f = \mathrm{id}_F$ as a function from F into E. f is additive, multiplicative, unity-preserving, and monomorphic. □

(35) Let us consider a ring R, an R-homomorphic ring S, an S-homomorphic, R-homomorphic ring T, an additive function f from R into S, and an additive function g from S into T. Then $\mathrm{PolyHom}(g \cdot f) = \mathrm{PolyHom}(g) \cdot \mathrm{PolyHom}(f)$.

(36) Let us consider a ring R, an R-homomorphic ring S, an R-homomorphic, S-homomorphic ring T, an additive function f from R into S, and an additive function g from S into T. Suppose $g \cdot f = \mathrm{id}_R$. Then $\mathrm{PolyHom}(g \cdot f) = \mathrm{id}_{\mathrm{PolyRing}(R)}$. The theorem is a consequence of (35).

(37) Let us consider fields F_1, F_2, and an extension E of F_1. If $F_1 \approx F_2$, then E is an extension of F_2.

(38) Let us consider fields F_1, F_2. Suppose $F_1 \approx F_2$. Then

(i) $\mathbf{0}.F_1 = \mathbf{0}.F_2$, and

(ii) $\mathbf{1}.F_1 = \mathbf{1}.F_2$.

(39) Let us consider fields F_1, F_2, and a polynomial p over F_1. If $F_1 \approx F_2$, then p is a polynomial over F_2.

(40) Let us consider fields F_1, F_2, and a non zero polynomial p over F_1. If $F_1 \approx F_2$, then p is a non zero polynomial over F_2. The theorem is a consequence of (39) and (38).

(41) Let us consider fields F_1, F_2, a polynomial p over F_1, a polynomial q over F_2, an element a of F_1, and an element b of F_2. Suppose $F_1 \approx F_2$ and $p = q$ and $a = b$. Then $\mathrm{eval}(p, a) = \mathrm{eval}(q, b)$.

(42) Let us consider fields F_1, F_2, an extension E_1 of F_1, an extension E_2 of F_2, a polynomial p over F_1, a polynomial q over F_2, an element a of E_1, and an element b of E_2. Suppose $F_1 \approx F_2$ and $E_1 \approx E_2$ and $p = q$ and $a = b$. Then $\mathrm{ExtEval}(p, a) = \mathrm{ExtEval}(q, b)$. The theorem is a consequence of (41).

(43) Let us consider fields F_1, F_2, and an F_1-algebraic extension E of F_1. If $F_1 \approx F_2$, then E is an F_2-algebraic extension of F_2. The theorem is a consequence of (37), (40), and (42).

(44) Let us consider fields F_1, F_2, and an algebraic closure E of F_1. If $F_1 \approx F_2$, then E is an algebraic closure of F_2. The theorem is a consequence of (43).

Let X be a set. We say that X is field-membered if and only if

(Def. 12) for every object x such that $x \in X$ holds x is a field.

Observe that there exists a set which is field-membered and non empty.

Let X be a non empty, field-membered set.

One can check that an element of X is a field. Let F be a field. The functor SubFields(F) yielding a set is defined by

(Def. 13) for every object o, $o \in it$ iff there exists a strict field K such that $o = K$ and K is a subfield of F.

One can check that SubFields(F) is non empty and field-membered. Now we state the proposition:

(45) Let us consider fields F, K. Then $K \in \mathrm{SubFields}(F)$ if and only if K is a strict subfield of F.

6. Uniqueness of Algebraic Closures

Let F be a field, E be an extension of F, L be an F-monomorphic field, and f be a monomorphism of F and L. The functor $\mathrm{ExtSet}(f, E)$ yielding a non empty set is defined by the term

(Def. 14) $\{\langle K, g\rangle$, where K is an element of SubFields(E), g is a function from K into L : there exists an extension K_1 of F and there exists a function g_1 from K_1 into L such that $K_1 = K$ and $g_1 = g$ and g_1 is monomorphic and f-extending$\}$.

Note that every element of $\mathrm{ExtSet}(f, E)$ is pair.

Let p be an element of $\mathrm{ExtSet}(f, E)$. One can verify that the functor $(p)_{\mathbf{1}}$ yields a strict extension of F. One can verify that the functor $(p)_{\mathbf{2}}$ yields a function from $(p)_{\mathbf{1}}$ into L. Now we state the proposition:

(46) Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, a strict extension K of F, and a function g from K into L. Suppose g is monomorphic. Then $\langle K, g\rangle \in \mathrm{ExtSet}(f, E)$ if and only if E is an extension of K and F is a subfield of K and g is f-extending. The theorem is a consequence of (45).

Let F be a field, E be an extension of F, L be an F-monomorphic field, f be a monomorphism of F and L, and p, q be elements of $\mathrm{ExtSet}(f, E)$. We say that $p \leqslant q$ if and only if

(Def. 15) $(q)_{\mathbf{1}}$ is an extension of $(p)_{\mathbf{1}}$ and for every extension K of $(p)_{\mathbf{1}}$ and for every function g from K into L such that $K = (q)_{\mathbf{1}}$ and $g = (q)_{\mathbf{2}}$ holds g is $(p)_{\mathbf{2}}$-extending.

Let S be a non empty subset of $\mathrm{ExtSet}(f, E)$. We say that S is ascending if and only if

(Def. 16) for every elements p, q of S, $p \leqslant q$ or $q \leqslant p$.

One can check that there exists a non empty subset of $\mathrm{ExtSet}(f, E)$ which is ascending. Now we state the propositions:

(47) Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, and an element p of $\mathrm{ExtSet}(f, E)$. Then $p \leqslant p$.

(48) Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, and elements p, q of $\mathrm{ExtSet}(f, E)$. If $p \leqslant q \leqslant p$, then $p = q$.

(49) Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, and elements p, q, r of $\mathrm{ExtSet}(f, E)$. If $p \leqslant q \leqslant r$, then $p \leqslant r$.

Let F be a field, E be an extension of F, L be an F-monomorphic field, f be a monomorphism of F and L, and S be a non empty subset of $\mathrm{ExtSet}(f, E)$. The functor unionCarrier(S, f, E) yielding a non empty set is defined by the term

(Def. 17) $\bigcup$the set of all the carrier of $(p)_{\mathbf{1}}$ where p is an element of S.

Let S be an ascending, non empty subset of $\mathrm{ExtSet}(f, E)$. The functors: unionAdd(S, f, E) and unionMult(S, f, E) yielding binary operations on union Carrier(S, f, E) are defined by conditions

(Def. 18) for every elements a, b of unionCarrier(S, f, E), there exists an element p of S and there exist elements x, y of $(p)_{\mathbf{1}}$ such that $x = a$ and $y = b$ and unionAdd$(S, f, E)(a, b) = x + y$,

(Def. 19) for every elements a, b of unionCarrier(S, f, E), there exists an element p of S and there exist elements x, y of $(p)_{\mathbf{1}}$ such that $x = a$ and $y = b$ and unionMult$(S, f, E)(a, b) = x \cdot y$,

respectively. The functors: unionOne(S, f, E) and unionZero(S, f, E) yielding elements of unionCarrier(S, f, E) are defined by conditions

(Def. 20) there exists an element p of S such that unionOne$(S, f, E) = 1_{(p)_{\mathbf{1}}}$,

(Def. 21) there exists an element p of S such that unionZero$(S, f, E) = 0_{(p)_{\mathbf{1}}}$,

respectively. The functor unionField(S, f, E) yielding a strict double loop structure is defined by

(Def. 22) the carrier of it = unionCarrier(S, f, E) and the addition of it = union Add(S, f, E) and the multiplication of it = unionMult(S, f, E) and the one of it = unionOne(S, f, E) and the zero of it = unionZero(S, f, E).

Now we state the propositions:

(50) Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, a non empty subset S of ExtSet(f, E), elements p, q of S, and an element a of $(p)_{\mathbf{1}}$. If $p \leqslant q$, then $a \in$ the carrier of $(q)_{\mathbf{1}}$.

(51) Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, an ascending, non empty subset S of ExtSet(f, E), and an element p of S. Then

  (i) $1_{\mathrm{unionField}(S,f,E)} = 1_{(p)_{\mathbf{1}}}$, and

  (ii) $0_{\mathrm{unionField}(S,f,E)} = 0_{(p)_{\mathbf{1}}}$.

(52) Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, an ascending, non empty subset S of ExtSet(f, E), elements a, b of unionField(S, f, E), an element p of S, and elements x, y of $(p)_{\mathbf{1}}$. If $x = a$ and $y = b$, then $a + b = x + y$ and $a \cdot b = x \cdot y$.

Let F be a field, E be an extension of F, L be an F-monomorphic field, f be a monomorphism of F and L, and S be an ascending, non empty subset of ExtSet(f, E). Let us observe that unionField(S, f, E) is non degenerated and unionField(S, f, E) is Abelian, add-associative, right zeroed, and right complementable and unionField(S, f, E) is commutative, associative, well unital, distributive, and almost left invertible. Now we state the proposition:

(53) Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, an ascending, non empty subset S of ExtSet(f, E), and an element p of S. Then $(p)_{\mathbf{1}}$ is a subfield of unionField(S, f, E).

Proof: Set $K = \mathrm{unionField}(S, f, E)$. The addition of $(p)_{\mathbf{1}}$ = (the addition of K) $\restriction$ (the carrier of $(p)_{\mathbf{1}}$). The multiplication of $(p)_{\mathbf{1}}$ = (the multiplication of K) $\restriction$ (the carrier of $(p)_{\mathbf{1}}$). $1_{(p)_{\mathbf{1}}} = 1_K$ and $0_K = 0_{(p)_{\mathbf{1}}}$. $\square$

Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, and an ascending, non empty subset S of $\mathrm{ExtSet}(f, E)$. Now we state the propositions:

(54) F is a subfield of $\mathrm{unionField}(S, f, E)$. The theorem is a consequence of (53).

(55) $\mathrm{unionField}(S, f, E)$ is a subfield of E.
Proof: Set $K = \mathrm{unionField}(S, f, E)$. The carrier of $K \subseteq$ the carrier of E. The addition of K = (the addition of E) $\restriction$ (the carrier of K). The multiplication of K = (the multiplication of E) $\restriction$ (the carrier of K). Set p = the element of S. Consider U being an element of $\mathrm{SubFields}(E)$, g being a function from U into L such that $p = \langle U, g\rangle$ and there exists an extension K_1 of F and there exists a function g_1 from K_1 into L such that $K_1 = U$ and $g_1 = g$ and g_1 is monomorphic and f-extending. $(p)_{\mathbf{1}}$ is a subfield of E. $1_K = 1_{(p)_{\mathbf{1}}}$. $0_K = 0_{(p)_{\mathbf{1}}}$. $\square$

Let F be a field, E be an extension of F, L be an F-monomorphic field, f be a monomorphism of F and L, and S be an ascending, non empty subset of $\mathrm{ExtSet}(f, E)$. Note that $\mathrm{unionField}(S, f, E)$ is F-extending.

The functor $\mathrm{unionExt}(S, f, E)$ yielding a function from $\mathrm{unionField}(S, f, E)$ into L is defined by

(Def. 23) for every element p of S, $it\restriction$(the carrier of $(p)_{\mathbf{1}}$) $= (p)_{\mathbf{2}}$.

Now we state the proposition:

(56) Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, and an ascending, non empty subset S of $\mathrm{ExtSet}(f, E)$. Then $\mathrm{unionExt}(S, f, E)$ is monomorphic and f-extending. The theorem is a consequence of (51) and (53).

Let F be a field, E be an extension of F, L be an F-monomorphic field, f be a monomorphism of F and L, and S be an ascending, non empty subset of $\mathrm{ExtSet}(f, E)$. The functor $\sup S$ yielding an element of $\mathrm{ExtSet}(f, E)$ is defined by the term

(Def. 24) $\langle \mathrm{unionField}(S, f, E), \mathrm{unionExt}(S, f, E)\rangle$.

Now we state the propositions:

(57) Let us consider a field F, an extension E of F, an F-monomorphic field L, a monomorphism f of F and L, an ascending, non empty subset S of $\mathrm{ExtSet}(f, E)$, and an element p of S. Then $p \leqslant \sup S$. The theorem is a consequence of (53).

(58) Let us consider a field F, an extension E of F, an F-algebraic element a of E, an F-monomorphic, algebraic closed field L, and a monomorphism f of F and L. Then there exists a function g from $\mathrm{FAdj}(F, \{a\})$ into L such that g is monomorphic and f-extending. The theorem is a consequence of (3) and (2).

(59) Let us consider a field F, an F-algebraic extension E of F, an F-monomorphic, algebraic closed field L, and a monomorphism f of F and L. Then there exists a function g from E into L such that g is monomorphic and f-extending. The theorem is a consequence of (47), (49), (48), (57), (45), (58), (10), and (1).

(60) Let us consider a field F, an extension E of F, an F-homomorphic, E-homomorphic field L, a homomorphism f from F to L, and a homomorphism g from E to L. Suppose g is f-extending. Then $\mathrm{Im}\, f$ is a subfield of $\mathrm{Im}\, g$.

(61) Let us consider a field F, an algebraic closure A of F, an A-monomorphic, A-homomorphic field L, and a monomorphism g of A and L. Then $\mathrm{Im}\, g$ is algebraic closed.

PROOF: Reconsider $f = g^{-1}$ as a function from $\mathrm{Im}\, g$ into A. f is additive, multiplicative, unity-preserving, and monomorphic. □

(62) Let us consider a field F, an F-monomorphic, F-homomorphic field L, an algebraic closure A of F, and a monomorphism f of F and L. Suppose L is an algebraic closure of $\mathrm{Im}\, f$. Let us consider a function g from A into L. If g is monomorphic and f-extending, then g is isomorphism. The theorem is a consequence of (61), (60), and (33).

(63) Let us consider a field F, and algebraic closures A_1, A_2 of F. Then A_1 and A_2 are isomorphic over F.

PROOF: Reconsider $L = A_2$ as an F-monomorphic, F-homomorphic, algebraic closed field. Reconsider $f = \mathrm{id}_F$ as a monomorphism of F and L. Consider g being a function from A_1 into L such that g is monomorphic and f-extending. The double loop structure of $F \approx F$. $\mathrm{Im}\, f =$ the double loop structure of F by [4, (7)]. L is an algebraic closure of $\mathrm{Im}\, f$. g is isomorphism. □

REFERENCES

[1] 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.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Serge Lang. *Algebra*. Springer Verlag, 2002 (Revised Third Edition).

[4] Christoph Schwarzweller. Field extensions and Kronecker's construction. *Formalized Mathematics*, 27(**3**):229–235, 2019. doi:10.2478/forma-2019-0022.

Accepted December 27, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 4, Pages 295–299, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0023

sciendo.com/journal/forma

Formalization of Orthogonal Decomposition for Hilbert Spaces

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In this article, we formalize the theorems about orthogonal decomposition of Hilbert spaces, using the Mizar system [1], [2]. For any subspace S of a Hilbert space H, any vector can be represented by the sum of a vector in S and a vector orthogonal to S. The formalization of orthogonal complements of Hilbert spaces has been stored in the Mizar Mathematical Library [4]. We referred to [5] and [6] in the formalization.

MSC: 46Bxx 68V20

Keywords: Hilbert space; orthogonal decomposition; topological space

MML identifier: `RUSUB_7`, version: `8.1.12 5.72.1435`

1. Preliminaries

From now on X denotes a real unitary space and x, y, y_1, y_2 denote points of X. Now we state the proposition:

(1) Let us consider a real unitary space X, points x, y of X, and points z, t of MetricSpaceNorm(the real normed space of X). If $x = z$ and $y = t$, then $\|x - y\| = \rho(z, t)$.

Let us consider a real unitary space X, an element z of MetricSpaceNorm(the real normed space of X), and a real number r. Now we state the propositions:

(2) There exists a point x of X such that

(i) $x = z$, and

(ii) $\mathrm{Ball}(z, r) = \{y$, where y is a point of $X : \|x - y\| < r\}$.

The theorem is a consequence of (1).

(3) There exists a point x of X such that

(i) $x = z$, and

(ii) $\overline{\mathrm{Ball}}(z, r) = \{y$, where y is a point of $X : \|x - y\| \leqslant r\}$.

The theorem is a consequence of (1).

(4) Let us consider a real unitary space X, a sequence S of X, a sequence S_1 of MetricSpaceNorm(the real normed space of X), a point x of X, and a point x_2 of MetricSpaceNorm(the real normed space of X). Suppose $S = S_1$ and $x = x_2$. Then S_1 is convergent to x_2 if and only if for every real number r such that $0 < r$ there exists a natural number m such that for every natural number n such that $m \leqslant n$ holds $\|S(n) - x\| < r$. The theorem is a consequence of (1).

Let us consider a real unitary space X, a sequence S of X, and a sequence S_1 of MetricSpaceNorm(the real normed space of X). Now we state the propositions:

(5) If $S = S_1$, then S_1 is convergent iff S is convergent. The theorem is a consequence of (4).

(6) If $S = S_1$ and S_1 is convergent, then $\lim S_1 = \lim S$. The theorem is a consequence of (5) and (4).

2. Topological Space Generated from Real Unitary Space

Now we state the proposition:

(7) Let us consider a real unitary space X, and a subset V of TopSpaceNorm (the real normed space of X). Then V is open if and only if for every point x of X such that $x \in V$ there exists a real number r such that $r > 0$ and $\{y$, where y is a point of $X : \|x - y\| < r\} \subseteq V$. The theorem is a consequence of (2).

Let us consider a real unitary space X, a point x of X, and a real number r. Now we state the propositions:

(8) $\{y$, where y is a point of $X : \|x - y\| < r\}$ is an open subset of TopSpaceNorm(the real normed space of X). The theorem is a consequence of (2).

(9) $\{y$, where y is a point of $X : \|x - y\| \leqslant r\}$ is a closed subset of TopSpaceNorm(the real normed space of X). The theorem is a consequence of (3).

(10) Let us consider a real unitary space M, a subset X of TopSpaceNorm(the real normed space of M), and an object x. Then $x \in \overline{X}$ if and only if there exists a sequence S of M such that for every natural number n, $S(n) \in X$ and S is convergent and $\lim S = x$. The theorem is a consequence of (5) and (6).

(11) Let us consider a real unitary space M, and a subset X of TopSpaceNorm (the real normed space of M). Then X is closed if and only if for every sequence S of M such that for every natural number n, $S(n) \in X$ and S is convergent holds $\lim S \in X$. The theorem is a consequence of (5) and (6).

(12) Let us consider a real unitary space S, and a subset X of S. Then X is a closed subset of TopSpaceNorm(the real normed space of S) if and only if for every sequence s_1 of S such that $\operatorname{rng} s_1 \subseteq X$ and s_1 is convergent holds $\lim s_1 \in X$. The theorem is a consequence of (11).

(13) Let us consider a real unitary space S, a point x of S, a point y of MetricSpaceNorm(the real normed space of S), and a real number r. If $x = y$, then $\mathrm{Ball}(x, r) = \mathrm{Ball}(y, r)$. The theorem is a consequence of (1).

(14) Let us consider a real unitary space S. Then TopSpaceNorm(the real normed space of S) = TopUnitSpace S. The theorem is a consequence of (13).

Let us consider a real unitary space S, a subset U of S, and a subset V of TopSpaceNorm(the real normed space of S). Now we state the propositions:

(15) If $U = V$, then U is closed iff V is closed.

(16) If $U = V$, then U is open iff V is open.

(17) Let us consider a real unitary space X, a subspace M of X, and points x, m_0 of X. Suppose $m_0 \in M$. Then for every point m of X such that $m \in M$ holds $\|x - m_0\| \leqslant \|x - m\|$ if and only if for every point m of X such that $m \in M$ holds $((x - m_0)|m) = 0$.

(18) Let us consider a real unitary space X, a subspace M of X, and points x, m_1, m_2 of X. Suppose $m_1, m_2 \in M$ and for every point m of X such that $m \in M$ holds $\|x - m_1\| \leqslant \|x - m\|$ and for every point m of X such that $m \in M$ holds $\|x - m_2\| \leqslant \|x - m\|$. Then $m_1 = m_2$.

(19) Let us consider a real Hilbert space of X, a subspace M of X, and a point x of X. Suppose the carrier of M is a closed subset of TopSpaceNorm(the real normed space of X). Then there exists a point m_0 of X such that

 (i) $m_0 \in M$, and

 (ii) for every point m of X such that $m \in M$ holds $\|x - m_0\| \leqslant \|x - m\|$.

The theorem is a consequence of (12).

Let X be a real unitary space and M be a subset of X. The functor OrtCompSet(M) yielding a non empty subset of X is defined by

(Def. 1) for every point x of X, $x \in it$ iff for every point y of X such that $y \in M$ holds $(y|x) = 0$.

Now we state the propositions:

(20) Let us consider a real unitary space X, and a subset M of X. Then OrtCompSet(M) is linearly closed.

PROOF: For every vectors v, u of X such that v, $u \in$ OrtCompSet(M) holds $v+u \in$ OrtCompSet(M). For every real number a and for every vector v of X such that $v \in$ OrtCompSet(M) holds $a \cdot v \in$ OrtCompSet(M). □

(21) Let us consider a real unitary space X, a non empty subset M of X, and a sequence s_2 of X. Suppose $\mathrm{rng}\, s_2 \subseteq$ the carrier of OrtComp(M) and s_2 is convergent. Then $\lim s_2 \in$ the carrier of OrtComp(M).

(22) Let us consider a real unitary space S, a non empty subset M of S, and a subset L of S. Suppose $L =$ the carrier of OrtComp(M). Then L is a closed subset of TopSpaceNorm(the real normed space of S). The theorem is a consequence of (21) and (12).

(23) Let us consider a real unitary space X. Then every non empty subset of X is a subset of OrtComp(OrtComp(M)).

(24) Let us consider a real unitary space X, and non empty subsets S, T of X. Suppose $S \subseteq T$. Then OrtComp(T) is a subspace of OrtComp(S).

(25) Let us consider a real Hilbert space of X, and a subspace M of X. Suppose X is strict and the carrier of M is a closed subset of TopSpaceNorm(the real normed space of X). Then X is the direct sum of M and OrtComp(M).

PROOF: For every object z, $z \in$ the carrier of $M +$ OrtComp(M) iff $z \in$ the carrier of X. For every object z, $z \in$ the carrier of $M \cap$ OrtComp(M) iff $z \in \{0_X\}$. □

(26) Let us consider a real Hilbert space of X, and a strict subspace M of X. Suppose X is strict and the carrier of M is a closed subset of TopSpaceNorm(the real normed space of X).

Then $M =$ OrtComp(OrtComp(M)).

PROOF: Reconsider $N =$ the carrier of M as a subset of X. N is a subset of OrtComp(OrtComp(N)). The carrier of OrtComp(OrtComp(M)) $\subseteq N$. □

(27) Let us consider a real unitary space X, a subspace M of X, a subset K of X, and a subset L of TopSpaceNorm(the real normed space of X). Suppose the carrier of $M = L$ and $K = \overline{L}$. Then K is linearly closed.

PROOF: For every vectors v, u of X such that $v, u \in K$ holds $v + u \in K$. For every real number a and for every vector v of X such that $v \in K$ holds $a \cdot v \in K$ by (10), [3, (15)]. □

(28) Let us consider a real Hilbert space of X, and a non empty subset M of X. Suppose X is strict. Then

(i) the carrier of OrtComp(OrtComp(M)) is a closed subset of TopSpaceNorm(the real normed space of X), and

(ii) there exists a subset L of TopSpaceNorm(the real normed space of X) such that L = the carrier of Lin(M) and the carrier of OrtComp(OrtComp(M)) $= \overline{L}$, and

(iii) Lin(M) is a subspace of OrtComp(OrtComp(M)).

(29) Let us consider a real Hilbert space of X, a strict subspace K of X, and a non empty subset M of X. Suppose X is strict and the carrier of K is a closed subset of TopSpaceNorm(the real normed space of X) and Lin(M) is a subspace of K. Then OrtComp(OrtComp(M)) is a subspace of K.

ACKNOWLEDGEMENT: The authors would also like to express our gratitude to Prof. Yasunari Shidama for his support and encouragement.

REFERENCES

[1] 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.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Noboru Endou, Takashi Mitsuishi, and Yasunari Shidama. Subspaces and cosets of subspace of real unitary space. *Formalized Mathematics*, 11(**1**):1–7, 2003.

[4] Noboru Endou, Takashi Mitsuishi, and Yasunari Shidama. Topology of real unitary space. *Formalized Mathematics*, 11(**1**):33–38, 2003.

[5] David G. Luenberger. *Optimization by Vector Space Methods*. John Wiley and Sons, 1969.

[6] Kôsaku Yosida. *Functional Analysis*. Springer, 1980.

Accepted December 27, 2022