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 $i = -k$. □

(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 $\overline{\overline{2^{(\operatorname{Seg} m) \setminus \{1\}}}} = 2^{m -' 1}$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \overline{\overline{2^{(\operatorname{Seg}(1+\$_1)) \setminus \{1\}}}} = 2^{\$_1}$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

(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 $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. □

2. More on Bags

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

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

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

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

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 $\mathcal{P}[j+1]$. $\mathcal{P}[j]$. □

(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 $b(y) = (b_5 + E_6)(y)$. □

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

(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 $y_{/i} = \mathrm{power}_L(f \cdot S_{/i}, b \cdot S_{/i})$. □

(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 $\operatorname{support}(2 \cdot b +\cdot (0, b(0))) = \operatorname{support} b$.

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

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

Proof: Set $E_3 = \operatorname{EmptyBag} X$. 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 $\operatorname{Monom}(-a, b) = -\operatorname{Monom}(a, b)$.

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

(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 $\operatorname{Monom}(a_1, b) + \operatorname{Monom}(a_2, b) = \operatorname{Monom}(a_1 + a_2, b)$.

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

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

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

(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 $\operatorname{Support}(p - \operatorname{Monom}(p(b), b)) = (\operatorname{Support} p) \setminus \{b\}$. 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 $\mathbb{R}_F$, and a function x from n into $\mathbb{R}_F$. Then $\operatorname{eval}(\operatorname{Monom}(i, \operatorname{EmptyBag} n +\cdot (p, 1)), x) = i \cdot (x_{/p})$. 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 $\mathbb{R}_F$. One can check that $\operatorname{Monom}(i, b)$ 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 $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

(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 $f(j) = \mathrm{eval}(q,x)$. □

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 $b \in$ 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 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 vars$(p) = \bigcup\{$support b, where b is an element of Bags $X : b \in$ 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 $b \in$ Support p, then support $b \subseteq$ 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 vars$(p + q) \subseteq$ vars$(p) \cup$ 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 vars$(p) =$ vars$(-p)$.

Proof: vars$(p) \subseteq$ vars$(-p)$. Consider b being a bag of X such that $b \in$ 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 vars$(p * q) \subseteq$ vars$(p) \cup$ 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 vars$(a \cdot p) \subseteq$ 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 vars$(p^k) \subseteq$ vars(p).

Proof: Define $\mathcal{P}$[natural number] $\equiv$ vars$(p^{\$_1}) \subseteq$ vars(p). $p^0 = 1\_(X, S)$. 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 $\mathcal{P}[n + 1]$. $\mathcal{P}[n]$. $\square$

(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, $it(b) = p(b \text{ extended by } 0)$.

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)]. $\square$

(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). $\square$

(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 $y(i) = y_3(i)$. □

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 $s_1(x) = (s + (E +\cdot (i, 1)))(x)$. □

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 $\mathrm{Sgn}_{L,E}(\emptyset) = 1_L$.

(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 $\mathrm{Sgn}_{L,(e \frown \langle E \rangle)}(f \frown \langle x \rangle) = \mathrm{Sgn}_{L,e}(f)$.
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 $f(x) \in e(x)\}$. $X \subseteq \operatorname{dom} f$. $X = X_1$. □

(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 $\mathrm{Sgn}_{L,(e \frown \langle E \rangle)}(f \frown \langle x \rangle) = -\mathrm{Sgn}_{L,e}(f)$.
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 $f(x) \in e(x)\}$. $X \subseteq X_1$. $X_1 \subseteq \operatorname{dom} f_5$. $\operatorname{len} f + 1 \notin X$. $X_1 \subseteq X \cup \{\operatorname{len} f + 1\}$. □

(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 $x_6 = \mathrm{FS2XFS}(f)$.

Let us consider a finite set F, an enumeration E of F, and a finite sequence d. Suppose $d \in \operatorname{dom}_\kappa(\mathrm{SignGenOp}(f, (\text{the addition of } L), F)) \cdot E(\kappa)$. Then $(\text{the multiplication of } L) \odot (\mathrm{App}((\mathrm{SignGenOp}(f, (\text{the addition of } L), F)) \cdot E))(d) = \mathrm{eval}(\mathrm{Monom}(\mathrm{Sgn}_{L,E}(d), \mathrm{count\_reps}(d, n)), x_6)$.
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 $d \in \operatorname{dom}_\kappa(\mathrm{SignGenOp}(f, A, F)) \cdot E(\kappa)$ holds $M \odot (\mathrm{App}((\mathrm{SignGenOp}(f, A, F)) \cdot E))(d) = \mathrm{eval}(\mathrm{Monom}(\mathrm{Sgn}_{L,E}(d), \mathrm{count\_reps}(d, n)), x_6)$. $\mathcal{P}[0]$. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. □

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

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

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

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

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

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

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

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

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

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

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 $\mathrm{J_{poly}}$ of m, L is a polynomial of m,L defined by

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

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

(Def. 11) $\mathrm{len}\, it = \mathrm{len}\, f$ and $it(1) = f(1)$ and for every natural number i such that $i \in \mathrm{dom}\, f$ 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 $\mathrm{J}^{\sqrt{\cdot}}(P)$ 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 $\mathrm{J}^{\sqrt{\cdot}}(P)$ 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 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 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 $x_6 = \mathrm{FS2XFS}(f)$ and $c_2 = \mathrm{FS2XFS}(\sqrt[\mathbb{C}]{f})$. 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 $C_2 = \mathrm{SgmX}(\mathrm{BagOrder}\, m, \operatorname{Support} C)$. 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 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 $\mathbb{C}_{\mathrm{F}}) \odot \mathrm{SignGen}(\sqrt[\mathbb{C}]{\mathrm{XFS2FS}(^{@}f)}$, (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 $\mathrm{Fin}\,\mathrm{dom}\, C_1$ such that $X = \$_1$

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

For every element B_9 of Fin dom C_1 and for every element b of 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 Fin 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 $t_1(x) = A$. □

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 $\mathbb{C}_F$, and a set A. Then there exists an integer i such that

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

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

9. Prime Representing Polynomial Construction

Now we state the propositions:

(73) Let us consider a $\mathrm{J}_{\mathrm{poly}}$ of 4, $\mathbb{C}_F$, 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 $\mathbb{C}_F$. 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 $\mathrm{J}_{\mathrm{poly}}$ 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 $\mathcal{P}$[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 $\mathrm{J}_{\mathrm{poly}}$ 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 $\operatorname{Bags} 6$, there exists an element y of R such that $\mathcal{J}[x, y]$. Consider W being a function from $\operatorname{Bags} 6$ into R such that for every element x of $\operatorname{Bags} 6$, $\mathcal{J}[x, W(x)]$. 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 $\mathcal{H}[j+1]$. $\mathcal{H}[j]$. □

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 $-(-y + d) \leqslant \sqrt{x_1} + 2 \cdot \sqrt{x_2} + 4 \cdot \sqrt{x_3}$. □

(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 $\mathbb{R}_{\rm F}$ 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 $\mathrm{eval}(Z_7, x) = 0_{\mathbb{R}_{\rm F}}$ by [7, (23)]. $\mathrm{vars}(Z) \subseteq 8$. $\mathrm{vars}(Z_1) \subseteq (\mathrm{vars}(Z)) \setminus \{1\} \cup \mathrm{vars}(X_1)$. $\mathrm{vars}(F_4 \cdot X_2) \subseteq V_4$. $\mathrm{vars}(Z_2) \subseteq (\mathrm{vars}(Z_1)) \setminus \{2\} \cup \mathrm{vars}(F_4 \cdot X_2)$. $\mathrm{vars}(F_4 \cdot F_4 \cdot X_3) \subseteq V_4$. $\mathrm{vars}(Z_3) \subseteq (\mathrm{vars}(Z_2)) \setminus \{3\} \cup \mathrm{vars}(F_4 \cdot F_4 \cdot X_3)$. $\mathrm{vars}(Z_4) \subseteq (\mathrm{vars}(Z_3)) \setminus \{4\} \cup \mathrm{vars}(R)$. $\mathrm{vars}(Z_5) \subseteq (\mathrm{vars}(Z_4)) \setminus \{5\} \cup \mathrm{vars}(P)$. $\mathrm{vars}(Z_6) \subseteq (\mathrm{vars}(Z_5)) \setminus \{6\} \cup \mathrm{vars}(N_3)$. $\mathrm{vars}(Z_7) \subseteq (\mathrm{vars}(Z_6)) \setminus \{7\} \cup \mathrm{vars}(V)$. □

(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 $\mathcal{P}$[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 $\mathcal{P}[n]$. $\mathcal{P}[0]$. □

(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,$\mathbb{R}_{\rm F}$ such that for every positive natural number k, $k + 1$ is prime iff there exists a natural-valued function v from 10 into $\mathbb{R}_{\rm F}$ such that $v(1) = k$ and $\mathrm{eval}(P_{13}, v) = 0_{\mathbb{R}_{\rm F}}$.

Proof: Consider p_1 being a $\mathbb{Z}$-valued polynomial of $17,\mathbb{R}_{\rm F}$ 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 $\mathbb{R}_{\rm F}$ 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 $\mathrm{eval}(p_1, x) = 0_{\mathbb{R}_{\rm F}}$. 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 $10+7,\mathbb{R}_{\rm F}$. $\mathrm{vars}(p_2) \subseteq R_2{}^\circ(\mathrm{vars}(p_1))$.

Consider p_3 being a polynomial of $10,\mathbb{R}_{\rm F}$ 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 $\mathbb{R}_{\rm F}$ and for every function y from 10 into $\mathbb{R}_{\rm F}$ 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 $\mathbb{R}_{\rm F}$ 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 $\mathrm{eval}(p_3, x) = 0_{\mathbb{R}_{\rm F}}$. Set $E_2 = \mathrm{EmptyBag}\,10$. Set $O = 1\_(10, \mathbb{R}_{\rm F})$. Set $P_2 = \mathrm{Monom}(1_{\mathbb{R}_{\rm F}}, E_2 {+\cdot} (2, 1)) + O$. Set $P_3 = \mathrm{Monom}(1_{\mathbb{R}_{\rm F}}, E_2 {+\cdot} (3, 1)) + O$. Set $P_4 = \mathrm{Monom}(1_{\mathbb{R}_{\rm F}}, E_2 {+\cdot} (4, 1)) + O$. Set $P_5 = \mathrm{Monom}(1_{\mathbb{R}_{\rm F}}, E_2 {+\cdot} (5, 1)) + O$. Set $P_6 = \mathrm{Monom}(1_{\mathbb{R}_{\rm F}}, E_2 {+\cdot} (6, 1)) + O$.

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

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