Contents

Formaliz. Math. 30 (**3**)

Continued on inside back cover

FORMALIZED MATHEMATICS
Vol. 30, No. 3, Pages 159–168, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0012

sciendo.com/journal/forma

On Implicit and Inverse Function Theorems on Euclidean Spaces[1]

Kazuhisa Nakasho
Yamaguchi University
Yamaguchi, Japan

Yasunari Shidama
Karuizawa Hotch 244-1
Nagano, Japan

Summary. Previous Mizar articles [7, 6, 5] formalized the implicit and inverse function theorems for Frechet continuously differentiable maps on Banach spaces. In this paper, using the Mizar system [1], [2], we formalize these theorems on Euclidean spaces by specializing them. We referred to [4], [12], [10], [11] in this formalization.

MSC: 26B10 47J07 68V20

Keywords: implicit function theorem; inverse function theorem; continuously differentiable function

MML identifier: NDIFF11, version: 8.1.12 5.71.1431

1. Matrix and Linear Transformation on Euclidean Spaces

Let n be a natural number. One can check that $\langle \mathcal{E}^n, \|\cdot\| \rangle$ is finite dimensional. Now we state the propositions:

(1) Let us consider a non zero natural number n, and a real normed space X. Then every linear operator from $\langle \mathcal{E}^n, \|\cdot\| \rangle$ into X is Lipschitzian.

(2) Let us consider a non zero natural number m, and finite sequences s, t of elements of $\mathcal{R}^m$. Suppose $1 \leqslant \operatorname{len} s$ and $s = t \restriction \operatorname{len} s$. Let us consider a natural number i. If $1 \leqslant i \leqslant \operatorname{len} s$, then $(\operatorname{accum} t)(i) = (\operatorname{accum} s)(i)$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if $1 \leqslant \$_1 \leqslant \operatorname{len} s$, then $(\operatorname{accum} t)(\$_1) = (\operatorname{accum} s)(\$_1)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

[1] This work was supported by JSPS KAKENHI Grant Number JP20K19863.

(3) Let us consider a non zero natural number m, finite sequences s, s_1 of elements of $\mathcal{R}^m$, and an element s_0 of $\mathcal{R}^m$. If $s_1 = s \frown \langle s_0 \rangle$, then $\sum s_1 = \sum s + s_0$. The theorem is a consequence of (2).

(4) Let us consider a non zero natural number m, a finite sequence s of elements of $\mathcal{R}^m$, and a natural number j. Suppose $1 \leqslant j \leqslant m$. Then there exists a finite sequence t of elements of $\mathbb{R}$ such that

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

(ii) for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} s$ there exists an element s_2 of $\mathcal{R}^m$ such that $s_2 = s(i)$ and $t(i) = s_2(j)$, and

(iii) $(\sum s)(j) = \sum t$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence s of elements of $\mathcal{R}^m$ for every natural number j such that $\operatorname{len} s = \$_1$ and $1 \leqslant j \leqslant m$ there exists a finite sequence t of elements of $\mathbb{R}$ such that $\operatorname{len} t = \operatorname{len} s$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} s$ there exists an element s_2 of $\mathcal{R}^m$ such that $s_2 = s(i)$ and $t(i) = s_2(j)$ and $(\sum s)(j) = \sum t$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(5) Let us consider a non zero natural number m, and an element x of $\mathcal{R}^m$. Then there exists a finite sequence s of elements of $\mathcal{R}^m$ such that

(i) $\operatorname{dom} s = \operatorname{Seg} m$, and

(ii) for every natural number i such that $1 \leqslant i \leqslant m$ there exists an element e of $\mathcal{R}^m$ such that $e = (\operatorname{reproj}(i, \langle \underbrace{0, \ldots, 0}_{m} \rangle))(1)$ and $s(i) = (\operatorname{proj}(i, m))(x) \cdot e$, and

(iii) $\sum s = x$.

Proof: Define $\mathcal{P}[\text{natural number}, \text{object}] \equiv$ there exists an element e of $\mathcal{R}^m$ such that $e = (\operatorname{reproj}(\$_1, \langle \underbrace{0, \ldots, 0}_{m} \rangle))(1)$ and $\$_2 = (\operatorname{proj}(\$_1, m))(x) \cdot e$. For every natural number i such that $i \in \operatorname{Seg} m$ there exists an element y of $\mathcal{R}^m$ such that $\mathcal{P}[i, y]$. Consider s being a finite sequence of elements of $\mathcal{R}^m$ such that $\operatorname{dom} s = \operatorname{Seg} m$ and for every natural number i such that $i \in \operatorname{Seg} m$ holds $\mathcal{P}[i, s(i)]$. For every natural number i such that $1 \leqslant i \leqslant m$ there exists an element e of $\mathcal{R}^m$ such that $e = (\operatorname{reproj}(i, \langle \underbrace{0, \ldots, 0}_{m} \rangle))(1)$ and $s(i) = (\operatorname{proj}(i, m))(x) \cdot e$. For every natural number i such that $1 \leqslant i \leqslant \operatorname{len} \sum s$ holds $(\sum s)(i) = x(i)$. □

(6) Let us consider non zero elements m, n of $\mathbb{N}$, and a matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $m \times n$. Then $\operatorname{Mx2Tran}(M)$ is a Lipschitzian linear operator from $\langle \mathcal{E}^m, \| \cdot \| \rangle$ into $\langle \mathcal{E}^n, \| \cdot \| \rangle$.

Proof: Reconsider $f = \mathrm{Mx2Tran}(M)$ as a function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ into $\langle \mathcal{E}^n, \|\cdot\| \rangle$. For every elements x, y of $\langle \mathcal{E}^m, \|\cdot\| \rangle$, $f(x+y) = f(x) + f(y)$. For every vector x of $\langle \mathcal{E}^m, \|\cdot\| \rangle$ and for every real number a, $f(a \cdot x) = a \cdot f(x)$ by [8, (4),(8)]. □

Let us consider a non zero element m of $\mathbb{N}$ and a linear operator f from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ into $\langle \mathcal{E}^m, \|\cdot\| \rangle$. Now we state the propositions:

(7) Suppose f is bijective. Then there exists a Lipschitzian linear operator g from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ into $\langle \mathcal{E}^m, \|\cdot\| \rangle$ such that

(i) $g = f^{-1}$, and

(ii) g is one-to-one and onto.

(8) Suppose f is bijective. Then there exists a point g of the real norm space of bounded linear operators from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ into $\langle \mathcal{E}^m, \|\cdot\| \rangle$ such that

(i) $g = f$, and

(ii) g is invertible.

The theorem is a consequence of (7).

Let us consider non zero elements m, n of $\mathbb{N}$ and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension m. Now we state the propositions:

(9) $\mathrm{Mx2Tran}(M)$ is bijective if and only if $\mathrm{Det}\, M \neq 0_{\mathbb{R}_{\mathrm{F}}}$.

(10) $\mathrm{Mx2Tran}(M)$ is bijective if and only if M is invertible.

(11) Let us consider a non zero element m of $\mathbb{N}$, and a point f of the real norm space of bounded linear operators from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ into $\langle \mathcal{E}^m, \|\cdot\| \rangle$. Suppose f is one-to-one and $\mathrm{rng}\, f =$ the carrier of $\langle \mathcal{E}^m, \|\cdot\| \rangle$. Then f is invertible. The theorem is a consequence of (8).

Let us consider a non zero element m of $\mathbb{N}$, a point f of the real norm space of bounded linear operators from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ into $\langle \mathcal{E}^m, \|\cdot\| \rangle$, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension m. Now we state the propositions:

(12) If $f = \mathrm{Mx2Tran}(M)$, then f is invertible iff M is invertible. The theorem is a consequence of (10) and (11).

(13) If $f = \mathrm{Mx2Tran}(M)$, then f is invertible iff $\mathrm{Det}\, M \neq 0_{\mathbb{R}_{\mathrm{F}}}$. The theorem is a consequence of (12).

Let us consider non zero elements m, n of $\mathbb{N}$. Now we state the propositions:

(14) There exists a function f from $\mathcal{R}^m \times \mathcal{R}^n$ into $\mathcal{R}^{m+n}$ such that

(i) for every element x of $\mathcal{R}^m$ and for every element y of $\mathcal{R}^n$, $f(x, y) = x \frown y$, and

(ii) f is one-to-one and onto.

Proof: Define $\mathcal{S}[\text{object}, \text{object}, \text{object}] \equiv$ there exists an element x of $\mathcal{R}^m$ and there exists an element y of $\mathcal{R}^n$ such that $x = \$_1$ and $y = \$_2$ and $\$_3 = x \frown y$. For every objects x, y such that $x \in \mathcal{R}^m$ and $y \in \mathcal{R}^n$ there exists an object z such that $z \in \mathcal{R}^{m+n}$ and $\mathcal{S}[x, y, z]$. Consider f being a function from $\mathcal{R}^m \times \mathcal{R}^n$ into $\mathcal{R}^{m+n}$ such that for every objects x, y such that $x \in \mathcal{R}^m$ and $y \in \mathcal{R}^n$ holds $\mathcal{S}[x, y, f(x, y)]$. For every element x of $\mathcal{R}^m$ and for every element y of $\mathcal{R}^n$, $f(x, y) = x \frown y$. □

(15) There exists a function f from $\langle \mathcal{E}^m, \|\cdot\| \rangle \times \langle \mathcal{E}^n, \|\cdot\| \rangle$ into $\langle \mathcal{E}^{m+n}, \|\cdot\| \rangle$ such that

(i) f is one-to-one and onto, and

(ii) for every element x of $\mathcal{R}^m$ and for every element y of $\mathcal{R}^n$, $f(x, y) = x \frown y$, and

(iii) for every points u, v of $\langle \mathcal{E}^m, \|\cdot\| \rangle \times \langle \mathcal{E}^n, \|\cdot\| \rangle$, $f(u + v) = f(u) + f(v)$, and

(iv) for every point u of $\langle \mathcal{E}^m, \|\cdot\| \rangle \times \langle \mathcal{E}^n, \|\cdot\| \rangle$ and for every real number r, $f(r \cdot u) = r \cdot f(u)$, and

(v) $f(0_{\langle \mathcal{E}^m, \|\cdot\| \rangle \times \langle \mathcal{E}^n, \|\cdot\| \rangle}) = 0_{\langle \mathcal{E}^{m+n}, \|\cdot\| \rangle}$, and

(vi) for every point u of $\langle \mathcal{E}^m, \|\cdot\| \rangle \times \langle \mathcal{E}^n, \|\cdot\| \rangle$, $\|f(u)\| = \|u\|$.

Proof: Consider f being a function from $\mathcal{R}^m \times \mathcal{R}^n$ into $\mathcal{R}^{m+n}$ such that for every element x of $\mathcal{R}^m$ and for every element y of $\mathcal{R}^n$, $f(x, y) = x \frown y$ and f is one-to-one and onto. For every points u, v of $\langle \mathcal{E}^m, \|\cdot\| \rangle \times \langle \mathcal{E}^n, \|\cdot\| \rangle$, $f(u + v) = f(u) + f(v)$. For every point u of $\langle \mathcal{E}^m, \|\cdot\| \rangle \times \langle \mathcal{E}^n, \|\cdot\| \rangle$ and for every real number r, $f(r \cdot u) = r \cdot f(u)$. For every point u of $\langle \mathcal{E}^m, \|\cdot\| \rangle \times \langle \mathcal{E}^n, \|\cdot\| \rangle$, $\|f(u)\| = \|u\|$ by [9, (18)]. □

2. Total Derivative and Partial Derivative

Now we state the propositions:

(16) Let us consider real normed spaces X, Y, a point x of X, and a Lipschitzian linear operator f from X into Y. Then

(i) f is differentiable in x, and

(ii) $f = f'(x)$.

Proof: Set $C = \Omega_X$. Reconsider $g = (\text{the carrier of } X) \longmapsto 0_Y$ as a partial function from X to Y. Reconsider $f_0 = f$ as an element of $\mathrm{BdLinOps}(X, Y)$. For every (0_X)-convergent sequence h of X such that h is non-zero holds $\|h\|^{-1} \cdot (g_* h)$ is convergent and $\lim(\|h\|^{-1} \cdot (g_* h)) = 0_Y$. For every point x_0 of X such that $x_0 \in C$ holds $f_{/x_0} - f_{/x} = f_0(x_0 - x) + g_{/x_0 - x}$. □

(17) Let us consider a non zero natural number n, a natural number i, and a point x of $\langle \mathcal{E}^n, \| \cdot \| \rangle$. Suppose $1 \leqslant i \leqslant n$. Then

(i) $\mathrm{Proj}(i, n)$ is differentiable in x, and

(ii) $(\mathrm{Proj}(i, n))'(x) = \mathrm{Proj}(i, n)$.

The theorem is a consequence of (16).

Let us consider non zero natural numbers m, n, a partial function f from $\mathcal{R}^m$ to $\mathcal{R}^n$, and an element x of $\mathcal{R}^m$. Now we state the propositions:

(18) f is differentiable in x if and only if for every natural number i such that $1 \leqslant i \leqslant n$ there exists a partial function f_1 from $\mathcal{R}^m$ to $\mathcal{R}^1$ such that $f_1 = (\mathrm{Proj}(i, n)) \cdot f$ and f_1 is differentiable in x.

(19) f is differentiable in x if and only if for every natural number i such that $1 \leqslant i \leqslant n$ there exists a partial function f_1 from $\mathcal{R}^m$ to $\mathbb{R}$ such that $f_1 = (\mathrm{proj}(i, n)) \cdot f$ and f_1 is differentiable in x.
Proof: For every natural number i, $\langle (\mathrm{proj}(i, n)) \cdot f \rangle = (\mathrm{Proj}(i, n)) \cdot f$ by [3, (11)]. For every natural number i such that $1 \leqslant i \leqslant n$ there exists a partial function F_1 from $\mathcal{R}^m$ to $\mathcal{R}^1$ such that $F_1 = (\mathrm{Proj}(i, n)) \cdot f$ and F_1 is differentiable in x. □

(20) Let us consider non zero natural numbers m, n, a partial function f from $\mathcal{R}^m$ to $\mathcal{R}^n$, and an element x of $\mathcal{R}^m$. Suppose f is differentiable in x. Let us consider a natural number i, and a partial function f_1 from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose $1 \leqslant i \leqslant n$ and $f_1 = (\mathrm{proj}(i, n)) \cdot f$. Then

(i) f_1 is differentiable in x, and

(ii) ${f_1}'(x) = (\mathrm{proj}(i, n)) \cdot (f'(x))$.

The theorem is a consequence of (19).

(21) Let us consider non zero natural numbers m, n, a partial function f from $\mathcal{R}^m$ to $\mathcal{R}^n$, and an element x of $\mathcal{R}^m$. Suppose f is differentiable in x. Let us consider natural numbers i, j. Suppose $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$. Then f is partially differentiable in x w.r.t. i and j. The theorem is a consequence of (19).

(22) Let us consider non zero natural numbers m, n, a partial function f from $\langle \mathcal{E}^m, \| \cdot \| \rangle$ to $\langle \mathcal{E}^n, \| \cdot \| \rangle$, and an element x of $\langle \mathcal{E}^m, \| \cdot \| \rangle$. Suppose f is differentiable in x. Let us consider natural numbers i, j. Suppose $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$. Then f is partially differentiable in x w.r.t. i and j.

(23) Let us consider a non zero natural number m, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, and an element x of $\mathcal{R}^m$. Suppose f is differentiable in x. Let us consider elements u, v of $\mathcal{R}^m$. Then $(f'(x))(u+v) = (f'(x))(u)+(f'(x))(v)$.

(24) Let us consider a non zero natural number m, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, and an element x of $\mathcal{R}^m$. Suppose f is differentiable in x. Let us consider an element u of $\mathcal{R}^m$, and a real number a. Then $(f'(x))(a \cdot u) = a \cdot (f'(x))(u)$.

(25) Let us consider a non zero natural number m, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, and an element x of $\mathcal{R}^m$. Suppose f is differentiable in x. Let us consider a finite sequence s of elements of $\mathcal{R}^m$, and a finite sequence t of elements of $\mathbb{R}$. Suppose $\operatorname{dom} s = \operatorname{dom} t$ and for every natural number i such that $i \in \operatorname{dom} s$ holds $t(i) = (f'(x))(s(i))$. Then $(f'(x))(\sum s) = \sum t$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence s of elements of $\mathcal{R}^m$ for every finite sequence t of elements of $\mathbb{R}$ such that $\operatorname{len} s = \$_1$ and $\operatorname{dom} s = \operatorname{dom} t$ and for every natural number i such that $i \in \operatorname{dom} s$ holds $t(i) = (f'(x))(s(i))$ holds $(f'(x))(\sum s) = \sum t$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(26) Let us consider a non zero natural number m, a partial function f from $\mathcal{R}^m$ to $\mathbb{R}$, and an element x of $\mathcal{R}^m$. Suppose f is differentiable in x. Let us consider an element d_1 of $\mathcal{R}^m$. Then there exists a finite sequence d_2 of elements of $\mathbb{R}$ such that

(i) $\operatorname{dom} d_2 = \operatorname{Seg} m$, and

(ii) for every natural number i such that $1 \leqslant i \leqslant m$ holds $d_2(i) = (\operatorname{proj}(i,m))(d_1) \cdot (\operatorname{partdiff}(f,x,i))$, and

(iii) $(f'(x))(d_1) = \sum d_2$.

Proof: Consider s being a finite sequence of elements of $\mathcal{R}^m$ such that $\operatorname{dom} s = \operatorname{Seg} m$ and for every natural number i such that $1 \leqslant i \leqslant m$ there exists an element e of $\mathcal{R}^m$ such that $e = (\operatorname{reproj}(i, \langle \underbrace{0,\ldots,0}_{m} \rangle))(1)$ and $s(i) = (\operatorname{proj}(i,m))(d_1) \cdot e$ and $\sum s = d_1$. Define $\mathcal{F}$(natural number) $= (f'(x))(s(\$_1))(\in \mathbb{R})$. Consider d_2 being a finite sequence of elements of $\mathbb{R}$ such that $\operatorname{len} d_2 = m$ and for every natural number i such that $i \in \operatorname{dom} d_2$ holds $d_2(i) = \mathcal{F}(i)$. For every natural number i such that $i \in \operatorname{dom} d_2$ holds $d_2(i) = (f'(x))(s(i))$. For every natural number i such that $1 \leqslant i \leqslant m$ holds $d_2(i) = (\operatorname{proj}(i,m))(d_1) \cdot (\operatorname{partdiff}(f,x,i))$. □

(27) Let us consider non zero elements m, n of $\mathbb{N}$, a subset X of $\langle \mathcal{E}^m, \|\cdot\| \rangle$, and a partial function f from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose X is open and $X \subseteq \operatorname{dom} f$. Then f is differentiable on X and $f'_{\restriction X}$ is continuous on X if and only if for every natural numbers i, j such that $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$ holds $(\operatorname{Proj}(j,n)) \cdot f$ is partially differentiable on X w.r.t. i and $(\operatorname{Proj}(j,n)) \cdot f{\restriction}^i X$ is continuous on X.

Proof: For every natural number i such that $1 \leqslant i \leqslant m$ holds f is partially differentiable on X w.r.t. i and $f{\restriction}^{i}X$ is continuous on X. □

3. Jacobian Matrix

Let m, n be non zero natural numbers, f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$, and x be an element of $\mathcal{R}^m$. The functor Jacobian(f, x) yielding a matrix over $\mathbb{R}_{\rm F}$ of dimension $m{\times}n$ is defined by

(Def. 1) for every natural numbers i, j such that $i \in \operatorname{Seg} m$ and $j \in \operatorname{Seg} n$ holds $it_{i,j} = \operatorname{partdiff}(f, x, i, j)$.

Now we state the proposition:

(28) Let us consider non zero natural numbers m, n, a partial function f from $\mathcal{R}^m$ to $\mathcal{R}^n$, and an element x of $\mathcal{R}^m$. Suppose f is differentiable in x. Then $f'(x) = \text{Mx2Tran}(\text{Jacobian}(f, x))$.
Proof: For every element d_1 of $\mathcal{R}^m$, $(f'(x))(d_1) = (\text{Mx2Tran}(\text{Jacobian}(f, x)))(d_1)$. □

Let m, n be non zero natural numbers, f be a partial function from $\langle \mathcal{E}^m, \|\cdot\|\rangle$ to $\langle \mathcal{E}^n, \|\cdot\|\rangle$, and x be a point of $\langle \mathcal{E}^m, \|\cdot\|\rangle$. The functor Jacobian$(f, x)$ yielding a matrix over $\mathbb{R}_{\rm F}$ of dimension $m{\times}n$ is defined by

(Def. 2) there exists a partial function g from $\mathcal{R}^m$ to $\mathcal{R}^n$ and there exists an element y of $\mathcal{R}^m$ such that $g = f$ and $y = x$ and $it = \text{Jacobian}(g, y)$.

Now we state the proposition:

(29) Let us consider non zero elements m, n of $\mathbb{N}$, a point x of $\langle \mathcal{E}^m, \|\cdot\|\rangle$, and a partial function f from $\langle \mathcal{E}^m, \|\cdot\|\rangle$ to $\langle \mathcal{E}^n, \|\cdot\|\rangle$. Suppose f is differentiable in x. Then $f'(x) = \text{Mx2Tran}(\text{Jacobian}(f, x))$. The theorem is a consequence of (28).

Let us consider a non zero element m of $\mathbb{N}$, a partial function f from $\langle \mathcal{E}^m, \|\cdot\|\rangle$ to $\langle \mathcal{E}^m, \|\cdot\|\rangle$, and a point x of $\langle \mathcal{E}^m, \|\cdot\|\rangle$. Now we state the propositions:

(30) If f is differentiable in x, then $f'(x)$ is invertible iff Jacobian(f, x) is invertible. The theorem is a consequence of (29) and (12).

(31) If f is differentiable in x, then $f'(x)$ is invertible iff $\operatorname{Det} \text{Jacobian}(f, x) \neq 0_{\mathbb{R}_{\rm F}}$. The theorem is a consequence of (30).

4. Implicit and Inverse Function Theorems on Euclidean Spaces

Now we state the propositions:

(32) Let us consider non zero elements l, m, n of $\mathbb{N}$, a subset Z of $\langle \mathcal{E}^l, \| \cdot \| \rangle \times \langle \mathcal{E}^m, \| \cdot \| \rangle$, a partial function f from $\langle \mathcal{E}^l, \| \cdot \| \rangle \times \langle \mathcal{E}^m, \| \cdot \| \rangle$ to $\langle \mathcal{E}^n, \| \cdot \| \rangle$, a point a of $\langle \mathcal{E}^l, \| \cdot \| \rangle$, a point b of $\langle \mathcal{E}^m, \| \cdot \| \rangle$, a point c of $\langle \mathcal{E}^n, \| \cdot \| \rangle$, and a point z of $\langle \mathcal{E}^l, \| \cdot \| \rangle \times \langle \mathcal{E}^m, \| \cdot \| \rangle$. Suppose Z is open and $\operatorname{dom} f = Z$ and f is differentiable on Z and $f'_{\restriction Z}$ is continuous on Z and $\langle\!\langle a, b \rangle\!\rangle \in Z$ and $f(a, b) = c$ and $z = \langle\!\langle a, b \rangle\!\rangle$ and partdiff(f, z) w.r.t. 2 is invertible. Then there exist real numbers r_1, r_2 such that

(i) $0 < r_1$, and

(ii) $0 < r_2$, and

(iii) $\operatorname{Ball}(a, r_1) \times \overline{\operatorname{Ball}}(b, r_2) \subseteq Z$, and

(iv) for every point x of $\langle \mathcal{E}^l, \| \cdot \| \rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ there exists a point y of $\langle \mathcal{E}^m, \| \cdot \| \rangle$ such that $y \in \operatorname{Ball}(b, r_2)$ and $f(x, y) = c$, and

(v) for every point x of $\langle \mathcal{E}^l, \| \cdot \| \rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ for every points y_1, y_2 of $\langle \mathcal{E}^m, \| \cdot \| \rangle$ such that y_1, $y_2 \in \operatorname{Ball}(b, r_2)$ and $f(x, y_1) = c$ and $f(x, y_2) = c$ holds $y_1 = y_2$, and

(vi) there exists a partial function g from $\langle \mathcal{E}^l, \| \cdot \| \rangle$ to $\langle \mathcal{E}^m, \| \cdot \| \rangle$ such that $\operatorname{dom} g = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g \subseteq \operatorname{Ball}(b, r_2)$ and g is continuous on $\operatorname{Ball}(a, r_1)$ and $g(a) = b$ and for every point x of $\langle \mathcal{E}^l, \| \cdot \| \rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g(x)) = c$ and g is differentiable on $\operatorname{Ball}(a, r_1)$ and $g'_{\restriction \operatorname{Ball}(a, r_1)}$ is continuous on $\operatorname{Ball}(a, r_1)$ and for every point x of $\langle \mathcal{E}^l, \| \cdot \| \rangle$ and for every point z of $\langle \mathcal{E}^l, \| \cdot \| \rangle \times \langle \mathcal{E}^m, \| \cdot \| \rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ and $z = \langle\!\langle x, g(x) \rangle\!\rangle$ holds $g'(x) = -(\text{Inv partdiff}(f, z)$ w.r.t. 2$) \cdot (\text{partdiff}(f, z)$ w.r.t. 1$)$ and for every point x of $\langle \mathcal{E}^l, \| \cdot \| \rangle$ and for every point z of $\langle \mathcal{E}^l, \| \cdot \| \rangle \times \langle \mathcal{E}^m, \| \cdot \| \rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ and $z = \langle\!\langle x, g(x) \rangle\!\rangle$ holds partdiff(f, z) w.r.t. 2 is invertible, and

(vii) for every partial functions g_1, g_2 from $\langle \mathcal{E}^l, \| \cdot \| \rangle$ to $\langle \mathcal{E}^m, \| \cdot \| \rangle$ such that $\operatorname{dom} g_1 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_1 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of $\langle \mathcal{E}^l, \| \cdot \| \rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_1(x)) = c$ and $\operatorname{dom} g_2 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_2 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of $\langle \mathcal{E}^l, \| \cdot \| \rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_2(x)) = c$ holds $g_1 = g_2$.

(33) Let us consider non zero elements l, m of $\mathbb{N}$, a subset Z of $\langle \mathcal{E}^l, \| \cdot \| \rangle \times \langle \mathcal{E}^m, \| \cdot \| \rangle$, a partial function f from $\langle \mathcal{E}^l, \| \cdot \| \rangle \times \langle \mathcal{E}^m, \| \cdot \| \rangle$ to $\langle \mathcal{E}^m, \| \cdot \| \rangle$, a point a of $\langle \mathcal{E}^l, \| \cdot \| \rangle$, points b, c of $\langle \mathcal{E}^m, \| \cdot \| \rangle$, and a point z of $\langle \mathcal{E}^l, \| \cdot \| \rangle \times \langle \mathcal{E}^m, \| \cdot \| \rangle$. Suppose Z is open and $\operatorname{dom} f = Z$ and f is differentiable on

Z and $f'_{\restriction Z}$ is continuous on Z and $\langle a, b\rangle \in Z$ and $f(a,b) = c$ and $z = \langle a, b\rangle$ and $\operatorname{Det}\operatorname{Jacobian}(f \cdot (\operatorname{reproj2}(z)), (z)_{\mathbf{2}}) \neq 0_{\mathbb{R}_{\mathrm{F}}}$. Then there exist real numbers r_1, r_2 such that

(i) $0 < r_1$, and

(ii) $0 < r_2$, and

(iii) $\operatorname{Ball}(a, r_1) \times \overline{\operatorname{Ball}}(b, r_2) \subseteq Z$, and

(iv) for every point x of $\langle \mathcal{E}^l, \|\cdot\|\rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ there exists a point y of $\langle \mathcal{E}^m, \|\cdot\|\rangle$ such that $y \in \operatorname{Ball}(b, r_2)$ and $f(x, y) = c$, and

(v) for every point x of $\langle \mathcal{E}^l, \|\cdot\|\rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ for every points y_1, y_2 of $\langle \mathcal{E}^m, \|\cdot\|\rangle$ such that $y_1, y_2 \in \operatorname{Ball}(b, r_2)$ and $f(x, y_1) = c$ and $f(x, y_2) = c$ holds $y_1 = y_2$, and

(vi) there exists a partial function g from $\langle \mathcal{E}^l, \|\cdot\|\rangle$ to $\langle \mathcal{E}^m, \|\cdot\|\rangle$ such that $\operatorname{dom} g = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g \subseteq \operatorname{Ball}(b, r_2)$ and g is continuous on $\operatorname{Ball}(a, r_1)$ and $g(a) = b$ and for every point x of $\langle \mathcal{E}^l, \|\cdot\|\rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g(x)) = c$ and g is differentiable on $\operatorname{Ball}(a, r_1)$ and $g'_{\restriction \operatorname{Ball}(a,r_1)}$ is continuous on $\operatorname{Ball}(a, r_1)$ and for every point x of $\langle \mathcal{E}^l, \|\cdot\|\rangle$ and for every point z of $\langle \mathcal{E}^l, \|\cdot\|\rangle \times \langle \mathcal{E}^m, \|\cdot\|\rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ and $z = \langle x, g(x)\rangle$ holds $g'(x) = -(\operatorname{Inv}\operatorname{partdiff}(f, z)\text{ w.r.t. }2) \cdot (\operatorname{partdiff}(f, z)\text{ w.r.t. }1)$ and for every point x of $\langle \mathcal{E}^l, \|\cdot\|\rangle$ and for every point z of $\langle \mathcal{E}^l, \|\cdot\|\rangle \times \langle \mathcal{E}^m, \|\cdot\|\rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ and $z = \langle x, g(x)\rangle$ holds $\operatorname{partdiff}(f, z)\text{ w.r.t. }2$ is invertible, and

(vii) for every partial functions g_1, g_2 from $\langle \mathcal{E}^l, \|\cdot\|\rangle$ to $\langle \mathcal{E}^m, \|\cdot\|\rangle$ such that $\operatorname{dom} g_1 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_1 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of $\langle \mathcal{E}^l, \|\cdot\|\rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_1(x)) = c$ and $\operatorname{dom} g_2 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_2 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of $\langle \mathcal{E}^l, \|\cdot\|\rangle$ such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_2(x)) = c$ holds $g_1 = g_2$.

The theorem is a consequence of (31).

(34) Let us consider a non zero element m of $\mathbb{N}$, a subset Z of $\langle \mathcal{E}^m, \|\cdot\|\rangle$, a partial function f from $\langle \mathcal{E}^m, \|\cdot\|\rangle$ to $\langle \mathcal{E}^m, \|\cdot\|\rangle$, a point a of $\langle \mathcal{E}^m, \|\cdot\|\rangle$, and a point b of $\langle \mathcal{E}^m, \|\cdot\|\rangle$. Suppose Z is open and $\operatorname{dom} f = Z$ and f is differentiable on Z and $f'_{\restriction Z}$ is continuous on Z and $a \in Z$ and $f(a) = b$ and $\operatorname{Det}\operatorname{Jacobian}(f, a) \neq 0_{\mathbb{R}_{\mathrm{F}}}$.

Then there exists a subset A of $\langle \mathcal{E}^m, \|\cdot\|\rangle$ and there exists a subset B of $\langle \mathcal{E}^m, \|\cdot\|\rangle$ and there exists a partial function g from $\langle \mathcal{E}^m, \|\cdot\|\rangle$ to $\langle \mathcal{E}^m, \|\cdot\|\rangle$ such that A is open and B is open and $A \subseteq \operatorname{dom} f$ and $a \in A$ and $b \in B$ and $f^{\circ}A = B$ and $\operatorname{dom} g = B$ and $\operatorname{rng} g = A$ and $\operatorname{dom}(f{\restriction}A) = A$ and $\operatorname{rng}(f{\restriction}A) = B$ and $f{\restriction}A$ is one-to-one and g is one-to-one and $g = (f{\restriction}A)^{-1}$

and $f \restriction A = g^{-1}$ and $g(b) = a$ and g is continuous on B and differentiable on B and $g'_{\restriction B}$ is continuous on B and for every point y of $\langle \mathcal{E}^m, \|\cdot\| \rangle$ such that $y \in B$ holds $f'(g_{/y})$ is invertible and for every point y of $\langle \mathcal{E}^m, \|\cdot\| \rangle$ such that $y \in B$ holds $g'(y) = \mathrm{Inv}\, f'(g_{/y})$. The theorem is a consequence of (31).

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, Yasunari Shidama, and Keiichi Miyajima. Partial differentiation on normed linear spaces $\mathcal{R}^n$. *Formalized Mathematics*, 15(**2**):65–72, 2007. doi:10.2478/v10037-007-0008-5.

[4] Miyadera Isao. *Functional Analysis.* Riko-Gaku-Sya, 1972.

[5] Kazuhisa Nakasho and Yuichi Futa. Inverse function theorem. Part I. *Formalized Mathematics*, 29(**1**):9–19, 2021. doi:10.2478/forma-2021-0002.

[6] Kazuhisa Nakasho and Yasunari Shidama. Implicit function theorem. Part II. *Formalized Mathematics*, 27(**2**):117–131, 2019. doi:10.2478/forma-2019-0013.

[7] Kazuhisa Nakasho, Yuichi Futa, and Yasunari Shidama. Implicit function theorem. Part I. *Formalized Mathematics*, 25(**4**):269–281, 2017. doi:10.1515/forma-2017-0026.

[8] Kazuhisa Nakasho, Hiroyuki Okazaki, and Yasunari Shidama. Real vector space and related notions. *Formalized Mathematics*, 29(**3**):117–127, 2021. doi:10.2478/forma-2021-0012.

[9] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. Cartesian products of family of real linear spaces. *Formalized Mathematics*, 19(**1**):51–59, 2011. doi:10.2478/v10037-011-0009-2.

[10] Laurent Schwartz. *Théorie des ensembles et topologie, tome 1. Analyse.* Hermann, 1997.

[11] Laurent Schwartz. *Calcul différentiel, tome 2. Analyse.* Hermann, 1997.

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

Accepted September 30, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 3, Pages 169–198, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0013

sciendo.com/journal/forma

Prime Representing Polynomial with 10 Unknowns – Introduction

Karol Pąk
Institute of Computer Science
University of Białystok
Poland

Summary. The main purpose of the article is to construct a sophisticated polynomial proposed by Matiyasevich and Robinson [5] that is often used to reduce the number of unknowns in diophantine representations, using the Mizar [1], [2] formalism. The polynomial

$$J_k(a_1,\ldots,a_k,x) = \prod_{\epsilon_1,\ldots,\epsilon_k\in\{\pm1\}} (x+\epsilon_1\sqrt{a_1}+\epsilon_2\sqrt{a_2}W+\ldots+\epsilon_k\sqrt{a_k}W^{k-1})$$

with $W = \sum_{i=1}^{k} x_i^2$ has integer coefficients and $J_k(a_1,\ldots,a_k,x) = 0$ for some $a_1,\ldots,a_k,x \in \mathbb{Z}$ if and only if $a_1,\ldots,a_k$ are all squares. However although it is nontrivial to observe that this expression is a polynomial, i.e., eliminating similar elements in the product of all combinations of signs we obtain an expression where every square root will occur with an even power. This work has been partially presented in [7].

MSC: 11D45 68V20

Keywords: polynomial reduction; diophantine equation

MML identifier: HILB10_7, version: 8.1.12 5.71.1431

1. Preliminaries

From now on i, j, n, k, m denote natural numbers, a, b, x, y, z denote objects, F, G denote finite sequence-yielding finite sequences, f, g, p, q denote finite sequences, X, Y denote sets, and D denotes a non empty set.

Let X be a finite set. The functor Ω_X yielding an element of Fin X is defined by the term

(Def. 1) X.

Now we state the propositions:

(1) Let us consider non empty sets X_1, X_2, Y, a binary operation F on Y, an element B_1 of $\operatorname{Fin} X_1$, and an element B_2 of $\operatorname{Fin} X_2$. Suppose $B_1 = B_2$ and ($B_1 \neq \emptyset$ or F is unital) and F is associative and commutative. Let us consider a function f_1 from X_1 into Y, and a function f_2 from X_2 into Y. Suppose $f_1 \restriction B_1 = f_2 \restriction B_2$. Then $F\text{-}\sum_{B_1} f_1 = F\text{-}\sum_{B_2} f_2$.

PROOF: Consider G_1 being a function from $\operatorname{Fin} X_1$ into Y such that $F\text{-}\sum_{B_1} f_1 = G_1(B_1)$ and for every element e of Y such that e is a unity w.r.t. F holds $G_1(\emptyset) = e$ and for every element x of X_1, $G_1(\{x\}) = f_1(x)$ and for every element B' of $\operatorname{Fin} X_1$ such that $B' \subseteq B_1$ and $B' \neq \emptyset$ for every element x of X_1 such that $x \in B_1 \setminus B'$ holds $G_1(B' \cup \{x\}) = F(G_1(B'), f_1(x))$.

Consider G_2 being a function from $\operatorname{Fin} X_2$ into Y such that $F\text{-}\sum_{B_2} f_2 = G_2(B_2)$ and for every element e of Y such that e is a unity w.r.t. F holds $G_2(\emptyset) = e$ and for every element x of X_2, $G_2(\{x\}) = f_2(x)$ and for every element B' of $\operatorname{Fin} X_2$ such that $B' \subseteq B_2$ and $B' \neq \emptyset$ for every element x of X_2 such that $x \in B_2 \setminus B'$ holds $G_2(B' \cup \{x\}) = F(G_2(B'), f_2(x))$. Define $\mathcal{P}[\text{set}] \equiv$ if $\$_1 \subseteq B_1$, then $G_1(\$_1) = G_2(\$_1)$ or $\$_1 = \emptyset$. For every element B' of $\operatorname{Fin} X_1$ and for every element b of X_1 such that $\mathcal{P}[B']$ and $b \notin B'$ holds $\mathcal{P}[B' \cup \{b\}]$. For every element B of $\operatorname{Fin} X_1$, $\mathcal{P}[B]$. □

(2) Let us consider a non empty set D, elements d_1, d_2 of D, and a binary operation B on D. Suppose B is unital, associative, and commutative and has inverse operation. Then

(i) $B(($the inverse operation w.r.t. $B)(d_1), d_2) =($the inverse operation w.r.t. $B)(B(d_1, ($the inverse operation w.r.t. $B)(d_2)))$, and

(ii) $B(d_1, ($the inverse operation w.r.t. $B)(d_2)) =($the inverse operation w.r.t. $B)(B(($the inverse operation w.r.t. $B)(d_1), d_2))$.

(3) Let us consider a non empty set D, and binary operations A, M on D. Suppose A is commutative, associative, and unital and M is commutative and distributive w.r.t. A and for every element d of D, $M(\mathbf{1}_A, d) = \mathbf{1}_A$. Let us consider non empty, finite sets X, Y, a function f from X into D, a function g from Y into D, an element a of $\operatorname{Fin} X$, and an element b of $\operatorname{Fin} Y$. Then $A\text{-}\sum_{a \times b} M_{f,g} = M(A\text{-}\sum_a f, A\text{-}\sum_b g)$.

PROOF: Set $m = M_{f,g}$. Define $\mathcal{P}[\text{set}] \equiv$ for every element a of $\operatorname{Fin} X$ for every element b of $\operatorname{Fin} Y$ such that $a = \$_1$ holds $A\text{-}\sum_{a \times b} m = M(A\text{-}\sum_a f, A\text{-}\sum_b g)$. $\mathcal{P}[\emptyset_X]$. For every element E of $\operatorname{Fin} X$ and for every element e of X such that $\mathcal{P}[E]$ and $e \notin E$ holds $\mathcal{P}[E \cup \{e\}]$. For every element E of $\operatorname{Fin} X$, $\mathcal{P}[E]$. □

(4) Let us consider a non empty set D, binary operations M, A on D, and an element d of D. Suppose M is unital and A is associative and unital and has inverse operation and M is distributive w.r.t. A. Then

(i) if n is even, then $M \odot n \mapsto (\text{the inverse operation w.r.t. } A)(d) = M \odot n \mapsto d$, and

(ii) if n is odd, then $M \odot n \mapsto (\text{the inverse operation w.r.t. } A)(d) = (\text{the inverse operation w.r.t. } A)(M \odot n \mapsto d)$.

Proof: Set $I =$ the inverse operation w.r.t. A. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1$ is even, then $M \odot \$_1 \mapsto I(d) = M \odot \$_1 \mapsto d$ and if $\$_1$ is not even, then $M \odot \$_1 \mapsto I(d) = I(M \odot \$_1 \mapsto d)$. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. □

(5) Let us consider a finite sequence s. Suppose $s^{-1}(\{y\}) \neq \emptyset$. Then there exists a permutation p of $\operatorname{Seg} \operatorname{len} s$ such that

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

(ii) $p = p^{-1}$.

Let D be a non empty set. Let us note that there exists a finite sequence of elements of D^* which is non empty and non-empty. Let X, Y be non empty sets. Let us note that $X \Cup Y$ is non empty. Let X, Y be finite sets. One can check that $X \Cup Y$ is finite. Now we state the propositions:

(6) Let us consider sets X, Y. Then $2^X \Cup 2^Y = 2^{X \cup Y}$.

(7) Let us consider sets X, Y_1, Y_2. Then $X \Cup (Y_1 \cup Y_2) = (X \Cup Y_1) \cup (X \Cup Y_2)$.

(8) If X misses $\bigcup Y$, then $\overline{\overline{Y \Cup \{X\}}} = \overline{\overline{Y}}$.

Proof: Define $\mathcal{F}(\text{set}) = \$_1 \cup X$. Consider f being a function such that $\operatorname{dom} f = Y$ and for every set A such that $A \in Y$ holds $f(A) = \mathcal{F}(A)$. $\operatorname{rng} f \subseteq Y \Cup \{X\}$. $Y \Cup \{X\} \subseteq \operatorname{rng} f$. f is one-to-one. □

(9) Suppose $m \neq 0$. Then $2 \cdot \overline{\overline{2^{(\operatorname{Seg} m) \setminus \{1\}}}} = \overline{\overline{2^{(\operatorname{Seg}(1+m)) \setminus \{1\}}}}$.

Proof: Set $S = (\operatorname{Seg} m) \setminus \{1\}$. Set $F = 2^S$. $\overline{\overline{F \Cup \{\emptyset\}}} = \overline{\overline{F}}$. $\{m+1\}$ misses $\bigcup F$. $\overline{\overline{F \Cup \{\{m+1\}\}}} = \overline{\overline{F}}$. $F \Cup 2^{\{m+1\}} = (F \Cup \{\emptyset\}) \cup (F \Cup \{\{m+1\}\})$. $F \Cup \{\emptyset\}$ misses $F \Cup \{\{m+1\}\}$. □

2. Selected Operations on Set Families

Let X be a set and a, b be objects. The functor $\operatorname{ext}(X, a, b)$ yielding a set is defined by the term

(Def. 2) $\{A \cup \{b\}$, where A is an element of $X : a \in A\} \cup \{A$, where A is an element of $X : a \notin A$ and $A \in X\}$.

The functor $\operatorname{swap}(X, a, b)$ yielding a set is defined by the term

(Def. 3) $\{A \setminus \{a\} \cup \{b\}$, where A is an element of $X : a \in A\} \cup \{A \cup \{a\}$, where A is an element of $X : a \notin A$ and $A \in X\}$.

Now we state the propositions:

(10) If $y \notin \bigcup Y$, then $\overline{\overline{Y}} = \overline{\overline{\mathrm{ext}(Y, x, y)}}$.

PROOF: Set $P = \{X$, where X is an element of $Y : x \in X\}$. Set $P_5 = \{X \cup \{y\}$, where X is an element of $Y : x \in X\}$. Set $N = \{X$, where X is an element of $Y : x \notin X$ and $X \in Y\}$. Define $\mathcal{F}(\text{set}) = \$_1 \cup \{y\}$. Consider f being a function such that $\mathrm{dom}\, f = P$ and for every set A such that $A \in P$ holds $f(A) = \mathcal{F}(A)$. $\mathrm{rng}\, f \subseteq P_5$. $P_5 \subseteq \mathrm{rng}\, f$. f is one-to-one. $P \subseteq Y$. $N \subseteq Y$. $Y \subseteq N \cup P$. N misses P_5. N misses P. □

(11) If $y \notin \bigcup Y$, then $\overline{\overline{Y}} = \overline{\overline{\mathrm{swap}(Y, x, y)}}$.

PROOF: Set $P = \{X$, where X is an element of $Y : x \in X\}$. Set $P_5 = \{X \setminus \{x\} \cup \{y\}$, where X is an element of $Y : x \in X\}$. Set $N = \{X$, where X is an element of $Y : x \notin X$ and $X \in Y\}$. Set $N_2 = \{X \cup \{x\}$, where X is an element of $Y : x \notin X$ and $X \in Y\}$. Define $\mathcal{F}(\text{set}) = \$_1 \setminus \{x\} \cup \{y\}$.

Consider f being a function such that $\mathrm{dom}\, f = P$ and for every set A such that $A \in P$ holds $f(A) = \mathcal{F}(A)$. $\mathrm{rng}\, f \subseteq P_5$. $P_5 \subseteq \mathrm{rng}\, f$. f is one-to-one. Define $\mathcal{G}(\text{set}) = \$_1 \cup \{x\}$. Consider g being a function such that $\mathrm{dom}\, g = N$ and for every set A such that $A \in N$ holds $g(A) = \mathcal{G}(A)$. $\mathrm{rng}\, g \subseteq N_2$. $N_2 \subseteq \mathrm{rng}\, g$. g is one-to-one. $P \subseteq Y$. $N \subseteq Y$. $Y \subseteq N \cup P$. N_2 misses P_5. N misses P. □

(12) $\mathrm{swap}(\emptyset, x, y) = \emptyset$.

(13) $\mathrm{swap}(X \cup Y, x, y) = \mathrm{swap}(X, x, y) \cup \mathrm{swap}(Y, x, y)$.

(14) If $Y \in \mathrm{swap}(X, x, y)$ and $x \neq y$ and $y \notin \bigcup X$, then $x \in Y$ iff $y \notin Y$.

(15) $\mathrm{ext}(\emptyset, x, y) = \emptyset$.

(16) $\mathrm{ext}(X \cup Y, x, y) = \mathrm{ext}(X, x, y) \cup \mathrm{ext}(Y, x, y)$.

(17) If $Y \in \mathrm{ext}(X, x, y)$ and $y \notin \bigcup X$, then $x \in Y$ iff $y \in Y$.

Let X be a finite set and a, b be objects. Observe that $\mathrm{swap}(X, a, b)$ is finite and $\mathrm{ext}(X, a, b)$ is finite.

Let f be a function. The functor $\mathrm{Swap}(f, a, b)$ yielding a function is defined by

(Def. 4) $\mathrm{dom}\, \mathit{it} = \mathrm{dom}\, f$ and for every x such that $x \in \mathrm{dom}\, f$ holds if $a \in f(x)$, then $\mathit{it}(x) = f(x) \setminus \{a\} \cup \{b\}$ and if $a \notin f(x)$, then $\mathit{it}(x) = f(x) \cup \{a\}$.

The functor $\mathrm{Ext}(f, a, b)$ yielding a function is defined by

(Def. 5) $\mathrm{dom}\, \mathit{it} = \mathrm{dom}\, f$ and for every x such that $x \in \mathrm{dom}\, f$ holds if $a \in f(x)$, then $\mathit{it}(x) = f(x) \cup \{b\}$ and if $a \notin f(x)$, then $\mathit{it}(x) = f(x)$.

Let f be a finite sequence. Observe that $\mathrm{Swap}(f, a, b)$ is $(\mathrm{len}\, f)$-element and finite sequence-like and $\mathrm{Ext}(f, a, b)$ is $(\mathrm{len}\, f)$-element and finite sequence-like.

Let us consider finite sequences f, g. Now we state the propositions:

(18) $\mathrm{Swap}(f \frown g, a, b) = \mathrm{Swap}(f, a, b) \frown \mathrm{Swap}(g, a, b)$.
PROOF: Set $S_9 = \mathrm{Swap}(f, a, b)$. Set $S_{11} = \mathrm{Swap}(g, a, b)$. Set $S_{10} = \mathrm{Swap}(f \frown g, a, b)$. For every k such that $1 \leqslant k \leqslant \mathrm{len}\, S_{10}$ holds $S_{10}(k) = (S_9 \frown S_{11})(k)$. □

(19) $\mathrm{Ext}(f \frown g, a, b) = \mathrm{Ext}(f, a, b) \frown \mathrm{Ext}(g, a, b)$.
PROOF: Set $E_{25} = \mathrm{Ext}(f, a, b)$. Set $E_{27} = \mathrm{Ext}(g, a, b)$. Set $E_{26} = \mathrm{Ext}(f \frown g, a, b)$. For every k such that $1 \leqslant k \leqslant \mathrm{len}\, E_{26}$ holds $E_{26}(k) = (E_{25} \frown E_{27})(k)$. □

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

(20) If $b \neq x$ and $b \neq y$, then $b \in (\mathrm{Ext}(f, x, y))(a)$ iff $b \in f(a)$.
PROOF: If $b \in (\mathrm{Ext}(f, x, y))(a)$, then $b \in f(a)$. □

(21) If $b \neq x$ and $b \neq y$, then $b \in (\mathrm{Swap}(f, x, y))(a)$ iff $b \in f(a)$.
PROOF: If $b \in (\mathrm{Swap}(f, x, y))(a)$, then $b \in f(a)$. □

(22) If $x \neq y$ and $y \notin \bigcup X$ and $y \notin \bigcup Y$, then $\mathrm{ext}(X, x, y)$ misses $\mathrm{swap}(Y, x, y)$. The theorem is a consequence of (14) and (17).

(23) Let us consider functions f, g. Then $(\mathrm{Swap}(f, x, y)) \cdot g = \mathrm{Swap}(f \cdot g, x, y)$.
PROOF: Set $S = \mathrm{Swap}(f, x, y)$. Set $S_{11} = \mathrm{Swap}(f \cdot g, x, y)$. $\mathrm{dom}(S \cdot g) \subseteq \mathrm{dom}(f \cdot g)$. $\mathrm{dom}(f \cdot g) \subseteq \mathrm{dom}(S \cdot g)$. For every a such that $a \in \mathrm{dom}\, S_{11}$ holds $S_{11}(a) = (S \cdot g)(a)$. □

(24) Let us consider a function f. Then $\mathrm{Swap}(f, x, y) \restriction X = \mathrm{Swap}(f \restriction X, x, y)$. The theorem is a consequence of (23).

(25) Let us consider functions f, g. Then $(\mathrm{Ext}(f, x, y)) \cdot g = \mathrm{Ext}(f \cdot g, x, y)$.
PROOF: Set $E = \mathrm{Ext}(f, x, y)$. Set $E_{27} = \mathrm{Ext}(f \cdot g, x, y)$. $\mathrm{dom}(E \cdot g) \subseteq \mathrm{dom}(f \cdot g)$. $\mathrm{dom}(f \cdot g) \subseteq \mathrm{dom}(E \cdot g)$. For every a such that $a \in \mathrm{dom}\, E_{27}$ holds $E_{27}(a) = (E \cdot g)(a)$. □

(26) Let us consider a function f. Then $\mathrm{Ext}(f, x, y) \restriction X = \mathrm{Ext}(f \restriction X, x, y)$. The theorem is a consequence of (25).

Let X be a finite set. Let us observe that every enumeration of X is $\overline{\overline{X}}$-element and X-valued. Let us consider a finite set F and an enumeration E of F. Now we state the propositions:

(27) If $y \notin \bigcup F$, then $\mathrm{Swap}(E, x, y)$ is an enumeration of $\mathrm{swap}(F, x, y)$. The theorem is a consequence of (11).

(28) If $y \notin \bigcup F$, then $\mathrm{Ext}(E, x, y)$ is an enumeration of $\mathrm{ext}(F, x, y)$. The theorem is a consequence of (10).

(29) If $x \in X$, then $\mathrm{ext}(\{X\}, x, y) = \{X \cup \{y\}\}$.

(30) If $x \notin X$, then $\mathrm{ext}(\{X\}, x, y) = \{X\}$.

(31) If $x \in X$, then $\mathrm{swap}(\{X\}, x, y) = \{X \setminus \{x\} \cup \{y\}\}$.

(32) If $x \notin X$, then $\mathrm{swap}(\{X\}, x, y) = \{X \cup \{x\}\}$.

Let X be a non empty set and a, b be objects. One can check that $\mathrm{ext}(X, a, b)$ is non empty and $\mathrm{swap}(X, a, b)$ is non empty. Now we state the propositions:

(33) If $y \notin \bigcup X$ and $y \notin \bigcup Y$, then X misses Y iff $\mathrm{ext}(X, x, y)$ misses $\mathrm{ext}(Y, x, y)$.
PROOF: If X misses Y, then $\mathrm{ext}(X, x, y)$ misses $\mathrm{ext}(Y, x, y)$. Consider a being an object such that $a \in X$ and $a \in Y$. □

(34) If $x \neq y$ and $y \notin \bigcup X$ and $y \notin \bigcup Y$, then X misses Y iff $\mathrm{swap}(X, x, y)$ misses $\mathrm{swap}(Y, x, y)$.
PROOF: If X misses Y, then $\mathrm{swap}(X, x, y)$ misses $\mathrm{swap}(Y, x, y)$. Consider a being an object such that $a \in X$ and $a \in Y$. □

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

(35) If $z \in \mathrm{dom}\, f$, then $\mathrm{Ext}(\langle f(z)\rangle, x, y) = \langle(\mathrm{Ext}(f, x, y))(z)\rangle$.

(36) If $z \in \mathrm{dom}\, f$, then $\mathrm{Swap}(\langle f(z)\rangle, x, y) = \langle(\mathrm{Swap}(f, x, y))(z)\rangle$.

(37) If $z \in \mathrm{dom}\, f$, then $\mathrm{ext}(\{f(z)\}, x, y) = \{(\mathrm{Ext}(f, x, y))(z)\}$. The theorem is a consequence of (29) and (30).

(38) If $z \in \mathrm{dom}\, f$, then $\mathrm{swap}(\{f(z)\}, x, y) = \{(\mathrm{Swap}(f, x, y))(z)\}$. The theorem is a consequence of (31) and (32).

(39) Suppose $m \neq 0$. Then $2^{(\mathrm{Seg}(m+2)) \setminus \{1\}} = \mathrm{ext}(2^{(\mathrm{Seg}(m+1)) \setminus \{1\}}, 1 + m, 2 + m) \cup \mathrm{swap}(2^{(\mathrm{Seg}(m+1)) \setminus \{1\}}, 1 + m, 2 + m)$. The theorem is a consequence of (10), (11), (9), and (22).

3. Function where Each Value is Repeated an Even Number of Times

Let f be a finite function. We say that f has evenly repeated values if and only if

(Def. 6) $\overline{\overline{f^{-1}(\{y\})}}$ is even.

One can verify that every finite function which is empty has also evenly repeated values.

Let x be an object. Observe that $\langle x, x\rangle$ has evenly repeated values.

Now we state the proposition:

(40) Let us consider finite sequences f, g with evenly repeated values. Then $f \frown g$ has evenly repeated values.

Let F be a set. We say that F is with evenly repeated values-member if and only if

(Def. 7) for every object y such that $y \in F$ holds y is a finite function with evenly repeated values.

One can verify that every set which is empty is also with evenly repeated values-member.

Let X be a finite sequence-membered set. Note that every element of $\mathrm{Fin}\, X$ is finite sequence-membered.

Let Y be a finite sequence-membered set. Note that $X \cup Y$ is finite sequence-membered. Now we state the propositions:

(41) Let us consider finite sequence-membered sets P_1, S_1, S_2. Then $P_1 \frown (S_1 \cup S_2) = P_1 \frown S_1 \cup P_1 \frown S_2$.

(42) Let us consider finite sequence-membered sets P_1, P_2, S_1. Then $(P_1 \cup P_2) \frown S_1 = P_1 \frown S_1 \cup P_2 \frown S_1$.

(43) Let us consider finite sequences f, g. Then $\{f\} \frown \{g\} = \{f \frown g\}$.

Let f be a finite function with evenly repeated values. Observe that $\{f\}$ is with evenly repeated values-member. Let g be a finite function with evenly repeated values. Let us note that $\{f, g\}$ is with evenly repeated values-member. Let F, G be with evenly repeated values-member, finite sequence-membered sets. Let us note that $F \frown G$ is with evenly repeated values-member. Now we state the proposition:

(44) Let us consider a finite function f, and a permutation p of $\mathrm{dom}\, f$. Then f has evenly repeated values if and only if $f \cdot p$ has evenly repeated values.
Proof: If f has evenly repeated values, then $f \cdot p$ has evenly repeated values. □

4. Cartesian Product of Domains in Finite Sequences

Let F be a finite sequence-yielding finite sequence. The functor $\mathrm{dom}_\kappa\, F(\kappa)$ yielding a finite subset of $\mathbb{N}^*$ is defined by

(Def. 8) for every object x, $x \in it$ iff there exists a finite sequence p such that $p = x$ and $\mathrm{len}\, p = \mathrm{len}\, F$ and for every i such that $i \in \mathrm{dom}\, p$ holds $p(i) \in \mathrm{dom}(F(i))$.

Now we state the propositions:

(45) $\mathrm{dom}_\kappa\, F(\kappa)$ is not empty if and only if F is non-empty.
Proof: If $\mathrm{dom}_\kappa\, F(\kappa)$ is not empty, then F is non-empty. Set $L = \mathrm{len}\, F \mapsto 1$. For every i such that $i \in \mathrm{dom}\, L$ holds $L(i) \in \mathrm{dom}(F(i))$. □

(46) $\mathrm{dom}_\kappa\, \emptyset(\kappa) = \{\emptyset\}$.

Let F be a finite sequence-yielding finite sequence. Let us observe that $\mathrm{dom}_\kappa\, F(\kappa)$ is finite sequence-membered. Now we state the proposition:

(47) $p \in \mathrm{dom}_\kappa\, F(\kappa)$ if and only if $\mathrm{len}\, p = \mathrm{len}\, F$ and for every i such that $i \in \mathrm{dom}\, p$ holds $p(i) \in \mathrm{dom}(F(i))$.

Let F be a finite sequence-yielding finite sequence. Let us note that every element of $\operatorname{dom}_\kappa F(\kappa)$ is $\mathbb{N}$-valued.

Let F be a non-empty, finite sequence-yielding finite sequence. Let us note that $\operatorname{dom}_\kappa F(\kappa)$ is non empty. Now we state the propositions:

(48) If $f \in \operatorname{dom}_\kappa F(\kappa)$ and $g \in \operatorname{dom}_\kappa G(\kappa)$, then $f \frown g \in \operatorname{dom}_\kappa F \frown G(\kappa)$.
PROOF: Set $f_{11} = f \frown g$. Set $F_8 = F \frown G$. $\operatorname{len} f = \operatorname{len} F$ and $\operatorname{len} g = \operatorname{len} G$. For every i such that $i \in \operatorname{dom} f_{11}$ holds $f_{11}(i) \in \operatorname{dom}(F_8(i))$. □

(49) Let us consider finite sequence-membered sets P, S. Suppose $P \subseteq \operatorname{dom}_\kappa F(\kappa)$ and $S \subseteq \operatorname{dom}_\kappa G(\kappa)$. Then $P \frown S \subseteq \operatorname{dom}_\kappa F \frown G(\kappa)$. The theorem is a consequence of (48).

(50) Suppose ($\operatorname{len} f = \operatorname{len} F$ or $\operatorname{len} g = \operatorname{len} G$) and $f \frown g \in \operatorname{dom}_\kappa F \frown G(\kappa)$. Then

(i) $f \in \operatorname{dom}_\kappa F(\kappa)$, and

(ii) $g \in \operatorname{dom}_\kappa G(\kappa)$.

PROOF: Set $f_{11} = f \frown g$. Set $F_8 = F \frown G$. $\operatorname{len} f_{11} = \operatorname{len} f + \operatorname{len} g$ and $\operatorname{len} F_8 = \operatorname{len} F + \operatorname{len} G$ and $\operatorname{len} F_8 = \operatorname{len} f_{11}$. For every i such that $i \in \operatorname{dom} f$ holds $f(i) \in \operatorname{dom}(F(i))$. For every i such that $i \in \operatorname{dom} g$ holds $g(i) \in \operatorname{dom}(G(i))$. □

(51) $f \in \operatorname{dom}_\kappa \langle g \rangle(\kappa)$ if and only if $\operatorname{len} f = 1$ and $f(1) \in \operatorname{dom} g$. The theorem is a consequence of (47).

(52) $\operatorname{dom}_\kappa F \frown \langle g \frown \langle x \rangle \rangle(\kappa) = \operatorname{dom}_\kappa F \frown \langle g \rangle(\kappa) \cup \{f \frown \langle 1 + \operatorname{len} g \rangle$, where f is an element of $\operatorname{dom}_\kappa F(\kappa) : f \in \operatorname{dom}_\kappa F(\kappa)\}$.
PROOF: Set $S = \{f \frown \langle 1 + \operatorname{len} g \rangle$, where f is an element of $\operatorname{dom}_\kappa F(\kappa) : f \in \operatorname{dom}_\kappa F(\kappa)\}$. Set $g_4 = g \frown \langle x \rangle$. $\operatorname{dom}_\kappa F \frown \langle g_4 \rangle(\kappa) \subseteq \operatorname{dom}_\kappa F \frown \langle g \rangle(\kappa) \cup S$. □

(53) $\operatorname{dom}_\kappa F \frown \langle \langle x \rangle \rangle(\kappa) = \{f \frown \langle 1 \rangle$, where f is an element of $\operatorname{dom}_\kappa F(\kappa) : f \in \operatorname{dom}_\kappa F(\kappa)\}$. The theorem is a consequence of (45) and (52).

(54) Let us consider finite sequence-yielding finite sequences F, G. Then (the concatenation of $\mathbb{N})^\circ((\operatorname{dom}_\kappa F(\kappa)) \times (\operatorname{dom}_\kappa G(\kappa))) = \operatorname{dom}_\kappa F \frown G(\kappa)$.
PROOF: Set $C =$ the concatenation of $\mathbb{N}$. $C^\circ((\operatorname{dom}_\kappa F(\kappa)) \times (\operatorname{dom}_\kappa G(\kappa))) \subseteq \operatorname{dom}_\kappa F \frown G(\kappa)$ by [3, (4)], (48). Reconsider $f_{11} = xy$ as an $\mathbb{N}$-valued finite sequence. $\operatorname{len} f_{11} = \operatorname{len}(F \frown G) = \operatorname{len} F + \operatorname{len} G$. Set $f = f_{11} \restriction \operatorname{len} F$. Consider g being a finite sequence such that $f_{11} = f \frown g$. $f \in \operatorname{dom}_\kappa F(\kappa)$ and $g \in \operatorname{dom}_\kappa G(\kappa)$. □

(55) $\operatorname{dom}_\kappa \langle f \rangle(\kappa) = \{\langle i \rangle$, where i is an element of $\mathbb{N} : i \in \operatorname{dom} f\}$.
PROOF: $\operatorname{dom}_\kappa \langle f \rangle(\kappa) \subseteq \{\langle i \rangle$, where i is an element of $\mathbb{N} : i \in \operatorname{dom} f\}$. Consider i being an element of $\mathbb{N}$ such that $y = \langle i \rangle$ and $i \in \operatorname{dom} f$. □

Let us consider n and F. One can check that $F \restriction n$ is finite sequence-yielding.

Now we state the propositions:

(56) If $f \in \mathrm{dom}_\kappa F(\kappa)$, then $f{\restriction}n \in \mathrm{dom}_\kappa F{\restriction}n(\kappa)$. The theorem is a consequence of (47).

(57) $\overline{\overline{\mathrm{dom}_\kappa \langle g \rangle(\kappa)}} = \mathrm{len}\, g$.

Proof: Set $G = \langle g \rangle$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ for every finite sequence f such that $f = \$_1$ holds $f(1) = \$_2$. For every object x such that $x \in \mathrm{dom}_\kappa G(\kappa)$ there exists an object y such that $y \in \mathrm{dom}\, g$ and $\mathcal{P}[x, y]$. Consider F being a function such that $\mathrm{dom}\, F = \mathrm{dom}_\kappa G(\kappa)$ and $\mathrm{rng}\, F \subseteq \mathrm{dom}\, g$ and for every object x such that $x \in \mathrm{dom}_\kappa G(\kappa)$ holds $\mathcal{P}[x, F(x)]$. F is one-to-one. $\mathrm{dom}\, g \subseteq \mathrm{rng}\, F$. □

(58) $\overline{\overline{\mathrm{dom}_\kappa F \mathbin{^\frown} \langle f \rangle(\kappa)}} = \overline{\overline{\mathrm{dom}_\kappa F(\kappa)}} \cdot (\mathrm{len}\, f)$.

Proof: Define $\mathcal{D}[\text{natural number}] \equiv$ for every finite sequence f such that $\mathrm{len}\, f = \$_1$ holds $\overline{\overline{\mathrm{dom}_\kappa F \mathbin{^\frown} \langle f \rangle(\kappa)}} = \overline{\overline{\mathrm{dom}_\kappa F(\kappa)}} \cdot (\mathrm{len}\, f)$. $\mathcal{D}[0]$. If $\mathcal{D}[n]$, then $\mathcal{D}[n+1]$. $\mathcal{D}[n]$. □

5. Some Operations on Finite Sequences

Let F be a finite sequence-yielding finite sequence. The functor $\mathrm{App}(F)$ yielding a finite sequence-yielding function is defined by

(Def. 9) $\mathrm{dom}\, \mathit{it} = \mathrm{dom}_\kappa F(\kappa)$ and for every finite sequence p such that $p \in \mathrm{dom}_\kappa F(\kappa)$ holds $\mathrm{len}\, \mathit{it}(p) = \mathrm{len}\, p$ and for every i such that $i \in \mathrm{dom}\, p$ holds $(\mathit{it}(p))(i) = F(i)(p(i))$.

Let D be a non empty set and F be a (D^*)-valued finite sequence. Let us note that the functor $\mathrm{App}(F)$ yields a function from $\mathrm{dom}_\kappa F(\kappa)$ into D^*. Now we state the propositions:

(59) $(\mathrm{App}(\emptyset))(\emptyset) = \emptyset$. The theorem is a consequence of (46).

(60) If $i \in \mathrm{dom}\, f$, then $(\mathrm{App}(\langle f \rangle))(\langle i \rangle) = \langle f(i) \rangle$. The theorem is a consequence of (51).

(61) Suppose $f \in \mathrm{dom}_\kappa F(\kappa)$ and $g \in \mathrm{dom}_\kappa G(\kappa)$. Then $(\mathrm{App}(F \mathbin{^\frown} G))(f \mathbin{^\frown} g) = (\mathrm{App}(F))(f) \mathbin{^\frown} (\mathrm{App}(G))(g)$.

Proof: Set $F_8 = F \mathbin{^\frown} G$. Set $A_1 = \mathrm{App}(F)$. Set $A_3 = \mathrm{App}(G)$. Set $A_2 = \mathrm{App}(F_8)$. $f \mathbin{^\frown} g \in \mathrm{dom}_\kappa F_8(\kappa)$. $\mathrm{len}\, f = \mathrm{len}\, F$ and $\mathrm{len}\, g = \mathrm{len}\, G$. For every i such that $1 \leqslant i \leqslant \mathrm{len}\, A_2(f \mathbin{^\frown} g)$ holds $A_2(f \mathbin{^\frown} g)(i) = (A_1(f) \mathbin{^\frown} A_3(g))(i)$. □

Let D be a non empty set and F be a non empty, (D^*)-valued finite sequence. One can verify that $\mathrm{App}(F)$ is non-empty.

Let f be a (D^*)-valued function and x be an object. One can check that the functor $f(x)$ yields a finite sequence of elements of D. Let B be a binary operation on D and F be a (D^*)-valued function. The functor $B \odot F$ yielding a function from $\operatorname{dom} F$ into D is defined by

(Def. 10) for every x such that $x \in \operatorname{dom} F$ holds $it(x) = B \odot F(x)$.

From now on B, A, M denote binary operations on D, F, G denote (D^*)-valued finite sequences, f denotes a finite sequence of elements of D, and d, d_1, d_2 denote elements of D.

Let D be a non empty set, B be a binary operation on D, and F be a (D^*)-valued finite sequence. Let us observe that $B \odot F$ is $(\operatorname{len} F)$-element and finite sequence-like.

Let D be a set and f be a finite sequence of elements of D. Observe that the functor $\langle f \rangle$ yields a finite sequence of elements of D^*. Now we state the propositions:

(62) $A \odot \langle f \rangle = \langle A \odot f \rangle$.

(63) $A \odot F \mathbin{^\frown} G = (A \odot F) \mathbin{^\frown} (A \odot G)$.

PROOF: Set $F_8 = F \mathbin{^\frown} G$. For every n such that $1 \leqslant n \leqslant \operatorname{len} F + \operatorname{len} G$ holds $(A \odot F_8)(n) = ((A \odot F) \mathbin{^\frown} (A \odot G))(n)$. □

Let f be a non empty finite sequence. Observe that $\langle f \rangle$ is non-empty.

From now on F, G denote non-empty, non empty finite sequences of elements of D^* and f denotes a non empty finite sequence of elements of D.

Now we state the propositions:

(64) Suppose A is commutative and associative. Let us consider non empty finite sequences f, g, a function F from $\operatorname{dom} f$ into D, a function G from $\operatorname{dom} g$ into D, and a function F_8 from $\operatorname{dom}(f \mathbin{^\frown} g)$ into D. Suppose $f = F$ and $g = G$ and $f \mathbin{^\frown} g = F_8$. Then $A\text{-}\sum_{\Omega_{\operatorname{dom}(f \mathbin{^\frown} g)}} F_8 = A(A\text{-}\sum_{\Omega_{\operatorname{dom} f}} F, A\text{-}\sum_{\Omega_{\operatorname{dom} g}} G)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non empty finite sequences f, g such that $\$_1 = \operatorname{len} g$ for every function F from $\operatorname{dom} f$ into D for every function G from $\operatorname{dom} g$ into D for every function F_8 from $\operatorname{dom}(f \mathbin{^\frown} g)$ into D such that $f = F$ and $g = G$ and $f \mathbin{^\frown} g = F_8$ holds $A\text{-}\sum_{\Omega_{\operatorname{dom}(f \mathbin{^\frown} g)}} F_8 = A(A\text{-}\sum_{\Omega_{\operatorname{dom} f}} F, A\text{-}\sum_{\Omega_{\operatorname{dom} g}} G)$. $\mathcal{P}[1]$. For every n such that $1 \leqslant n$ holds if $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. For every n such that $1 \leqslant n$ holds $\mathcal{P}[n]$. □

(65) Suppose M is commutative and associative. Then $M\text{-}\sum_{\Omega_{\operatorname{dom}(F \mathbin{^\frown} G)}}(A \odot F \mathbin{^\frown} G) = M(M\text{-}\sum_{\Omega_{\operatorname{dom} F}}(A \odot F), M\text{-}\sum_{\Omega_{\operatorname{dom} G}}(A \odot G))$. The theorem is a consequence of (63) and (64).

(66) If M is commutative and associative, then $M\text{-}\sum_{\Omega_{\operatorname{dom}\langle f \rangle}}(A \odot \langle f \rangle) = A \odot f$. The theorem is a consequence of (62).

(67) Suppose M is commutative and associative and A is commutative and associative and M is left distributive w.r.t. A. Let us consider a function

f_9 from $\operatorname{dom} f$ into D. Suppose for every x such that $x \in \operatorname{dom} f$ holds $f_9(x) = M(M\text{-}\sum_{\Omega_{\operatorname{dom} F}}(A \odot F), f(x))$. Then $M\text{-}\sum_{\Omega_{\operatorname{dom}(F \frown \langle f \rangle)}}(A \odot F \frown \langle f \rangle) = A\text{-}\sum_{\Omega_{\operatorname{dom} f}} f_9$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every f such that $\operatorname{len} f = \$_1$ for every function f_9 from $\operatorname{dom} f$ into D such that for every x such that $x \in \operatorname{dom} f$ holds $f_9(x) = M(M\text{-}\sum_{\Omega_{\operatorname{dom} F}}(A \odot F), f(x))$ holds $M\text{-}\sum_{\Omega_{\operatorname{dom}(F \frown \langle f \rangle)}}$ $(A \odot F \frown \langle f \rangle) = A\text{-}\sum_{\Omega_{\operatorname{dom} f}} f_9$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

(68) Suppose $\operatorname{len} F = 1$ and M is commutative and associative and A is commutative and associative. Then $M\text{-}\sum_{\Omega_{\operatorname{dom} F}}(A \odot F) = A\text{-}\sum_{\Omega_{\operatorname{dom}(\operatorname{App}(F))}}(M \odot \operatorname{App}(F))$.

Proof: Set $F_1 = F(1)$. Set $f = M \odot \operatorname{App}(F)$. Set $X = \operatorname{dom}(\operatorname{App}(F))$. Consider G being a function from $\operatorname{Fin} X$ into D such that $A\text{-}\sum_{\Omega_X} f = G(\Omega_X)$ and for every element e of D such that e is a unity w.r.t. A holds $G(\emptyset) = e$ and for every element x of X, $G(\{x\}) = f(x)$ and for every element B' of $\operatorname{Fin} X$ such that $B' \subseteq \Omega_X$ and $B' \neq \emptyset$ for every element x of X such that $x \in \Omega_X \setminus B'$ holds $G(B' \cup \{x\}) = A(G(B'), f(x))$.

Consider s being a sequence of D such that $s(1) = F_1(1)$ and for every natural number n such that $0 \neq n$ and $n < \operatorname{len} F_1$ holds $s(n+1) = A(s(n), F_1(n+1))$ and $A \odot F_1 = s(\operatorname{len} F_1)$. Define $\mathcal{R}$(natural number) $= \{\langle i \rangle$, where i is an element of $\mathbb{N} : i \in \operatorname{Seg} \$_1\}$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant \operatorname{len} F_1$, then for every element B' of $\operatorname{Fin} X$ such that $B' = \mathcal{R}(\$_1)$ holds $G(B') = s(\$_1)$. $\mathcal{P}[1]$. For every j such that $1 \leqslant j$ holds if $\mathcal{P}[j]$, then $\mathcal{P}[j+1]$. For every i such that $1 \leqslant i$ holds $\mathcal{P}[i]$. $\mathcal{R}(\operatorname{len} F_1) = X$. □

(69) Suppose M is commutative and associative and A is commutative, associative, and unital and M is distributive w.r.t. A. Then $M\text{-}\sum_{\Omega_{\operatorname{dom} F}}(A \odot F) = A\text{-}\sum_{\Omega_{\operatorname{dom}(\operatorname{App}(F))}}(M \odot \operatorname{App}(F))$.

Proof: Define $\mathcal{R}$[natural number] $\equiv$ for every non-empty, non empty finite sequence F of elements of D^* such that $\operatorname{len} F = \$_1$ holds $M\text{-}\sum_{\Omega_{\operatorname{dom} F}}(A \odot F) = A\text{-}\sum_{\Omega_{\operatorname{dom}(\operatorname{App}(F))}}(M \odot \operatorname{App}(F))$. If $\mathcal{R}[n]$, then $\mathcal{R}[n+1]$. $\mathcal{R}[n]$. □

6. Combination of Sign and Characteristic Functions

Let D be a non empty set, B be a binary operation on D, f be a finite sequence of elements of D, and X be a set. The functor $\operatorname{SignGen}(f, B, X)$ yielding a finite sequence of elements of D is defined by

(Def. 11) $\operatorname{dom} \mathit{it} = \operatorname{dom} f$ and for every i such that $i \in \operatorname{dom} \mathit{it}$ holds if $i \in X$, then $\mathit{it}(i) =$ (the inverse operation w.r.t. B)$(f(i))$ and if $i \notin X$, then $\mathit{it}(i) = f(i)$.

Note that $\operatorname{SignGen}(f, B, X)$ is $(\operatorname{len} f)$-element.

From now on f, g denote finite sequences of elements of D, a, b, c denote sets, and F, F_1, F_2 denote finite sets. Now we state the propositions:

(70) If X misses $\operatorname{dom} f$, then $\mathrm{SignGen}(f, B, X) = f$.

(71) $\mathrm{SignGen}(f, B, \emptyset) = f$. The theorem is a consequence of (70).

(72) $\mathrm{SignGen}(f \restriction n, B, X) = \mathrm{SignGen}(f, B, X) \restriction n$.

(73) Suppose $n + 1 = \operatorname{len} f$ and $n + 1 \in X$. Then $\mathrm{SignGen}(f, B, X) = \mathrm{SignGen}(f \restriction n, B, X) \frown \langle(\text{the inverse operation w.r.t. } B)(f(n+1))\rangle$.
PROOF: Set $n_1 = n + 1$. Set $I = (\text{the inverse operation w.r.t. } B)(f(n_1))$. $\mathrm{SignGen}(f \restriction n, B, X) = \mathrm{SignGen}(f, B, X) \restriction n$. For every i such that $1 \leqslant i \leqslant \operatorname{len} \mathrm{SignGen}(f, B, X)$ holds $(\mathrm{SignGen}(f, B, X))(i) = (\mathrm{SignGen}(f \restriction n, B, X) \frown \langle I\rangle)(i)$. □

(74) If $n+1 = \operatorname{len} f$ and $n+1 \notin X$, then $\mathrm{SignGen}(f, B, X) = \mathrm{SignGen}(f \restriction n, B, X) \frown \langle f(n+1)\rangle$.
PROOF: Set $n_1 = n+1$. Set $I = f(n_1)$. $\mathrm{SignGen}(f \restriction n, B, X) = \mathrm{SignGen}(f, B, X) \restriction n$. For every i such that $1 \leqslant i \leqslant \operatorname{len} \mathrm{SignGen}(f, B, X)$ holds $(\mathrm{SignGen}(f, B, X))(i) = (\mathrm{SignGen}(f \restriction n, B, X) \frown \langle I\rangle)(i)$. □

(75) If $\operatorname{dom} f \subseteq X$, then $\mathrm{SignGen}(f, B, X) = (\text{the inverse operation w.r.t. } B) \cdot f$.
PROOF: For every k such that $k \in \operatorname{dom}(\mathrm{SignGen}(f, B, X))$ holds $(\mathrm{SignGen}(f, B, X))(k) = ((\text{the inverse operation w.r.t. } B) \cdot f)(k)$. □

(76) If B is unital and associative and has inverse operation, then $\mathrm{SignGen}(\mathrm{SignGen}(f, B, X), B, X) = f$.
PROOF: Set $C = \mathrm{SignGen}(f, B, X)$. For every k such that $1 \leqslant k \leqslant \operatorname{len} f$ holds $(\mathrm{SignGen}(C, B, X))(k) = f(k)$. □

Let E be a non empty set, D be a set, p be a D-valued finite sequence, and h be a function from D into E. Let us observe that $h \cdot p$ is $(\operatorname{len} p)$-element and finite sequence-like.

Let D be a non empty set, B be a binary operation on D, f be a finite sequence of elements of D, and F be a finite set. The functor $\mathrm{SignGenOp}(f, B, F)$ yielding a function from F into D^* is defined by

(Def. 12) if $X \in F$, then $\mathit{it}(X) = \mathrm{SignGen}(f, B, X)$.

Now we state the propositions:

(77) Let us consider an enumeration E of $\{x\}$. Then $E = \langle x\rangle$.

(78) Let us consider an enumeration E of $\{X\}$. Then $(\mathrm{SignGenOp}(f, B, \{X\})) \cdot E = \langle\mathrm{SignGen}(f, B, X)\rangle$. The theorem is a consequence of (77).

(79) Let us consider an enumeration E_1 of F_1, and an enumeration E_2 of F_2. Suppose F_1 misses F_2. Then $E_1 \frown E_2$ is an enumeration of $F_1 \cup F_2$.

(80) Let us consider an enumeration E of F. Suppose $i \in \operatorname{dom} E$ or $i \in \operatorname{dom}((\mathrm{SignGenOp}(f, B, F)) \cdot E)$. Then $((\mathrm{SignGenOp}(f, B, F)) \cdot E)(i) = \mathrm{SignGen}(f, B, E(i))$.
Proof: Set $C = \mathrm{SignGenOp}(f, B, F)$. $i \in \operatorname{dom}(C \cdot E)$. □

(81) Let us consider an enumeration E_1 of F_1, an enumeration E_2 of F_2, and an enumeration E_{12} of $F_1 \cup F_2$. Suppose $E_{12} = E_1 \frown E_2$. Then $(\mathrm{SignGenOp}(f, B, F_1 \cup F_2)) \cdot E_{12} =$
$(\mathrm{SignGenOp}(f, B, F_1)) \cdot E_1 \frown (\mathrm{SignGenOp}(f, B, F_2)) \cdot E_2$.
Proof: Set $C_1 = \mathrm{SignGenOp}(f, B, F_1)$. Set $C_2 = \mathrm{SignGenOp}(f, B, F_2)$. Set $C_{12} = \mathrm{SignGenOp}(f, B, F_1 \cup F_2)$. For every k such that $1 \leqslant k \leqslant \operatorname{len} C_{12} \cdot E_{12}$ holds $(C_{12} \cdot E_{12})(k) = (C_1 \cdot E_1 \frown C_2 \cdot E_2)(k)$. □

Let us consider an enumeration E of F. Now we state the propositions:

(82) Suppose (B is unital or $\operatorname{len} f \geqslant 1$) and $1 + \operatorname{len} f \notin \bigcup F$. Then $B \odot (\mathrm{SignGenOp}(f \frown \langle d \rangle, B, F)) \cdot E = B^{\circ}(B \odot (\mathrm{SignGenOp}(f, B, F)) \cdot E, d)$.
Proof: Set $f_{10} = f \frown \langle d \rangle$. Set $C = \mathrm{SignGenOp}(f, B, F)$. Set $C_{23} = \mathrm{SignGenOp}(f_{10}, B, F)$. For every x such that $x \in \operatorname{dom}(C \cdot E)$ holds $(B^{\circ}(B \odot C \cdot E, d))(x) = (B \odot C_{23} \cdot E)(x)$. □

(83) Suppose (B is unital or $\operatorname{len} f \geqslant 1$) and $1 + \operatorname{len} f \in \bigcap F$. Then $B \odot (\mathrm{SignGenOp}(f \frown \langle d \rangle, B, F)) \cdot E =$
$B^{\circ}(B \odot (\mathrm{SignGenOp}(f, B, F)) \cdot E, (\text{the inverse operation w.r.t. } B)(d))$.
Proof: Set $f_{10} = f \frown \langle d \rangle$. Set $C = \mathrm{SignGenOp}(f, B, F)$. Set $C_{23} = \mathrm{SignGenOp}(f_{10}, B, F)$. Set $I =$ the inverse operation w.r.t. B. For every x such that $x \in \operatorname{dom}(C \cdot E)$ holds $(B^{\circ}(B \odot C \cdot E, I(d)))(x) = (B \odot C_{23} \cdot E)(x)$.
□

(84) Suppose (B is unital or $\operatorname{len} f \geqslant 1$) and B is associative and $1 + \operatorname{len} f \notin \bigcup F$ and $2 + \operatorname{len} f \notin \bigcup F$. Then $B \odot (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, B, F)) \cdot E = B \odot (\mathrm{SignGenOp}(f \frown \langle B(d_1, d_2) \rangle, B, F)) \cdot E$. The theorem is a consequence of (82).

(85) Suppose (B is unital or $\operatorname{len} f \geqslant 1$) and B is associative and $1 + \operatorname{len} f \notin \bigcup F$ and $2 + \operatorname{len} f \in \bigcap F$. Then $B \odot (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, B, F)) \cdot E = B \odot (\mathrm{SignGenOp}(f \frown \langle B(d_1, (\text{the inverse operation w.r.t. } B)(d_2)) \rangle, B, F)) \cdot E$. The theorem is a consequence of (83) and (82).

(86) Suppose B is unital, associative, and commutative and has inverse operation and $1 + \operatorname{len} f \in \bigcap F$ and $2 + \operatorname{len} f \notin \bigcup F$. Then $B \odot (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, B, F)) \cdot E = B \odot (\mathrm{SignGenOp}(f \frown \langle B(d_1, ((\text{the inverse operation w.r.t. } B)(d_2))) \rangle, B, F)) \cdot E$. The theorem is a consequence of (82), (83), and (2).

(87) Suppose B is unital, associative, and commutative and has inverse operation and $1 + \operatorname{len} f$, $2 + \operatorname{len} f \in \bigcap F$. Then $B \odot (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown$

$\langle d_2\rangle, B, F))\cdot E = B\odot(\mathrm{SignGenOp}(f ^\frown \langle B(d_1, d_2)\rangle, B, F))\cdot E$. The theorem is a consequence of (83) and (2).

(88) If X misses $\bigcup F$, then there exists an enumeration E_{36} of $F \Cup \{X\}$ such that for every i such that $i \in \mathrm{dom}\, E$ holds $E_{36}(i) = X \cup E(i)$.

PROOF: Define $\mathcal{F}(\text{set}) = E(\$_1) \cup X$. Consider f being a function such that $\mathrm{dom}\, f = \mathrm{dom}\, E$ and for every set A such that $A \in \mathrm{dom}\, E$ holds $f(A) = \mathcal{F}(A)$. $\mathrm{rng}\, f \subseteq F \Cup \{X\}$. $F \Cup \{X\} \subseteq \mathrm{rng}\, f$. f is one-to-one. □

(89) $\mathrm{SignGen}(f, B, X) = \mathrm{SignGen}(f, B, X \cap \mathrm{dom}\, f)$.

(90) Let us consider an enumeration E_1 of F_1, and an enumeration E_2 of F_2. Suppose $\overline{\overline{F_1}} = \overline{\overline{F_2}}$ and for every i such that $i \in \mathrm{dom}\, E_1$ holds $\mathrm{dom}\, f \cap E_1(i) = \mathrm{dom}\, f \cap E_2(i)$. Then $(\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1 = (\mathrm{SignGenOp}(f, A, F_2)) \cdot E_2$.

PROOF: Set $C_1 = \mathrm{SignGenOp}(f, A, F_1)$. Set $C_2 = \mathrm{SignGenOp}(f, A, F_2)$. For every i such that $1 \leqslant i \leqslant \mathrm{len}\, E_1$ holds $(C_1 \cdot E_1)(i) = (C_2 \cdot E_2)(i)$. □

(91) Suppose A is unital, associative, and commutative and has inverse operation. Let us consider a finite, non empty set F. Suppose $\bigcup F \subseteq \mathrm{dom}\, f$. Let us consider finite sets F_1, F_2. Suppose $F_1 = F \Cup 2^{\{\mathrm{len}\, f+1\}}$ and $F_2 = F \Cup 2^{\{\mathrm{len}\, f+1, \mathrm{len}\, f+2\}}$. Then there exists an enumeration E_1 of F_1 and there exists an enumeration E_2 of F_2 such that $A \odot (\mathrm{SignGenOp}((f ^\frown \langle d_1\rangle) ^\frown \langle d_2\rangle, A, F_2)) \cdot E_2 = (A \odot (\mathrm{SignGenOp}(f ^\frown \langle A(d_1, d_2)\rangle, A, F_1)) \cdot E_1) ^\frown (A \odot (\mathrm{SignGenOp}(f ^\frown \langle A(d_1, (\text{the inverse operation w.r.t. } A)(d_2))\rangle, A, F_1))\cdot E_1)$.

PROOF: Set $L = \mathrm{len}\, f$. Set $U_1 = F \Cup \{\{L+1\}\}$. Set $U_2 = F \Cup \{\{L+2\}\}$. Set $U_{12} = F \Cup \{\{L+1, L+2\}\}$. Set $E =$ the enumeration of F. Set $I =$ the inverse operation w.r.t. A. Set $f_{12} = (f ^\frown \langle d_1\rangle) ^\frown \langle d_2\rangle$. Set $f_3 = f ^\frown \langle A(d_1, d_2)\rangle$. Set $f_4 = f ^\frown \langle A(d_1, I(d_2))\rangle$.

Consider E_1 being an enumeration of U_1 such that for every i such that $i \in \mathrm{dom}\, E$ holds $E_1(i) = \{L+1\} \cup E(i)$. $L+2 \notin \bigcup U_1$. $L+1 \notin \bigcup U_2$. If $a \in U_{12}$, then $L+1$, $L+2 \in a$. Consider E_2 being an enumeration of U_2 such that for every i such that $i \in \mathrm{dom}\, E$ holds $E_2(i) = \{L+2\} \cup E(i)$. Consider E_{12} being an enumeration of U_{12} such that for every i such that $i \in \mathrm{dom}\, E$ holds $E_{12}(i) = \{L+1, L+2\} \cup E(i)$. F misses U_1. U_1 misses U_2. Reconsider $E_7 = E_2 ^\frown E_1$ as an enumeration of $U_2 \cup U_1$. F misses U_{12}. Reconsider $E_{37} = E ^\frown E_{12}$ as an enumeration of $F \cup U_{12}$. $\overline{\overline{U_{12}}} = \overline{\overline{F}} = \overline{\overline{U_2}}$. $\overline{\overline{U_{12}}} = \overline{\overline{F}} = \overline{\overline{U_1}}$. For every i such that $i \in \mathrm{dom}\, E_1$ holds $\mathrm{dom}\, f_3 \cap E_1(i) = \mathrm{dom}\, f_3 \cap E_{12}(i)$. For every i such that $i \in \mathrm{dom}\, E$ holds $\mathrm{dom}\, f_4 \cap E(i) = \mathrm{dom}\, f_4 \cap E_2(i)$. $F \cup U_{12}$ misses $U_2 \cup U_1$.

Reconsider $E_{16} = E_{37} ^\frown E_7$ as an enumeration of $(F \cup U_{12}) \cup (U_2 \cup U_1)$. $(\{\emptyset\} \cup \{\{L+1, L+2\}\}) \cup (\{\{L+1\}\} \cup \{\{L+2\}\}) = 2^{\{L+1, L+2\}}$. $F = F \Cup \{\emptyset\}$. $F \cup U_{12} = F \Cup (\{\emptyset\} \cup \{\{L+1, L+2\}\})$ and $U_2 \cup U_1 =$

$F \Cup (\{\{L+1\}\} \cup \{\{L+2\}\})$. Reconsider $e_1 = E_{16}$ as an enumeration of F_2. $F \cup U_1 = F \Cup (\{\emptyset\} \cup \{\{L+1\}\})$. $A \odot (\mathrm{SignGenOp}(f_{12}, A, F \cup U_{12})) \cdot E_{37} = A \odot (\mathrm{SignGenOp}(f_{12}, A, F)) \cdot E \frown (\mathrm{SignGenOp}(f_{12}, A, U_{12})) \cdot E_{12}$. $A \odot (\mathrm{SignGenOp}(f_{12}, A, U_2 \cup U_1)) \cdot E_7 = A \odot (\mathrm{SignGenOp}(f_{12}, A, U_2)) \cdot E_2 \frown (\mathrm{SignGenOp}(f_{12}, A, U_1)) \cdot E_1$. $(\mathrm{SignGenOp}(f_{12}, A, F_2)) \cdot e_1 = (\mathrm{SignGenOp}(f_{12}, A, (F \cup U_{12}) \cup (U_2 \cup U_1))) \cdot E_{16}$. □

7. Product over All Combinations of Sings

Let D be a non empty set, A be a binary operation on D, and M be a binary operation on D. Assume M is commutative and associative. Let f be a finite sequence of elements of D and F be a finite set. The functor $\mathrm{SignGenOp}(f, M, A, F)$ yielding an element of D is defined by

(Def. 13) for every enumeration E of 2^F, *it* $= M\text{-}\sum_{\Omega_{\mathrm{dom}((\mathrm{SignGenOp}(f,A,2^F))\cdot E)}} (A \odot (\mathrm{SignGenOp}(f, A, 2^F)) \cdot E)$.

Now we state the propositions:

(92) Suppose M is commutative and associative and A is commutative, associative, and unital and has inverse operation and M is distributive w.r.t. A. Let us consider non-empty, non empty finite sequences C_4, C_7, C_5 of elements of D^*. Suppose $C_5 = C_4 \frown C_7$. Let us consider an element S_1 of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_4))$, an element s_2 of $\mathrm{dom}(\mathrm{App}(C_7))$, and an element S_{12} of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_5))$. Suppose $S_{12} = S_1 \frown \{s_2\}$. Then $M(A\text{-}\sum_{S_1}(M \odot \mathrm{App}(C_4)), (M \odot \mathrm{App}(C_7))(s_2)) = A\text{-}\sum_{S_{12}}(M \odot \mathrm{App}(C_5))$.

Proof: Define $\mathcal{P}[\text{set}] \equiv$ for every element S_1 of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_4))$ for every element S_{12} of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_5))$ such that $S_1 = \$_1$ and $S_{12} = S_1 \frown \{s_2\}$ holds $M(A\text{-}\sum_{S_1}(M \odot \mathrm{App}(C_4)), A\text{-}\sum_{\{s_2\}_f}(M \odot \mathrm{App}(C_7))) = A\text{-}\sum_{S_{12}}(M \odot \mathrm{App}(C_5))$. $\mathcal{P}[\emptyset_{\mathrm{dom}(\mathrm{App}(C_4))}]$. For every element B' of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_4))$ and for every element b of $\mathrm{dom}(\mathrm{App}(C_4))$ such that $\mathcal{P}[B']$ and $b \notin B'$ holds $\mathcal{P}[B' \cup \{b\}]$. For every element B of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_4))$, $\mathcal{P}[B]$. □

(93) Suppose M is commutative and associative and A is commutative, associative, and unital and has inverse operation and M is distributive w.r.t. A. Let us consider non-empty, non empty finite sequences C_4, C_7, C_5 of elements of D^*. Suppose $C_5 = C_4 \frown C_7$. Let us consider an element S_1 of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_4))$, an element S_2 of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_7))$, and an element S_{12} of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_5))$. Suppose $S_{12} = S_1 \frown S_2$. Then $M(A\text{-}\sum_{S_1}(M \odot \mathrm{App}(C_4)), A\text{-}\sum_{S_2}(M \odot \mathrm{App}(C_7))) = A\text{-}\sum_{S_{12}}(M \odot \mathrm{App}(C_5))$.

Proof: Set $a_1 = A\text{-}\sum_{S_1}(M \odot \mathrm{App}(C_4))$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every element S_2 of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_7))$ for every element S_{12} of Fin dom(App(C_5)) such that $\overline{\overline{S_2}} = \$_1$ and $S_{12} = S_1 \frown S_2$ holds $M(a_1, A\text{-}\sum_{S_2}(M \odot \mathrm{App}(C_7))) = A\text{-}\sum_{S_{12}}(M \odot \mathrm{App}(C_5))$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$ by [6, (55)], [4, (16)]. $\mathcal{P}[n]$. □

(94) Let us consider an enumeration E_1 of F_1. Then $\mathrm{dom}_\kappa(\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1(\kappa) \subseteq \mathrm{dom}_\kappa(\mathrm{SignGenOp}(f \frown g, A, F_1)) \cdot E_1(\kappa)$.
PROOF: $\mathrm{len}\, x = \mathrm{len}\, E_1$. For every i such that $i \in \mathrm{dom}\, x$ holds $x(i) \in \mathrm{dom}(((\mathrm{SignGenOp}(f \frown g, A, F_1)) \cdot E_1)(i))$. □

(95) Suppose A is unital, commutative, and associative. Let us consider an enumeration E_1 of F_1, and non-empty, non empty finite sequences C_4, C_7 of elements of D^*. Suppose $C_4 = (\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1$ and $C_7 = (\mathrm{SignGenOp}(f{\frown}g, A, F_1)) \cdot E_1$. Let us consider an element S_1 of Fin dom(App(C_4)), and an element S_2 of Fin dom(App(C_7)). Suppose $S_1 = S_2$.
Then $A\text{-}\sum_{S_1}(M \odot \mathrm{App}(C_4)) = A\text{-}\sum_{S_2}(M \odot \mathrm{App}(C_7))$.
PROOF: For every x such that $x \in \mathrm{dom}((M \odot \mathrm{App}(C_4)) \restriction S_1)$ holds $((M \odot \mathrm{App}(C_4)) \restriction S_1)(x) = ((M \odot \mathrm{App}(C_7)) \restriction S_2)(x)$. □

(96) Let us consider an enumeration E of F. Suppose $\mathrm{len}\, E = n + 1$. Then

(i) $E \restriction n$ is an enumeration of $F \setminus \{E(\mathrm{len}\, E)\}$, and

(ii) $\langle E(\mathrm{len}\, E) \rangle$ is an enumeration of $\{E(\mathrm{len}\, E)\}$, and

(iii) $F = F \setminus \{E(\mathrm{len}\, E)\} \cup \{E(\mathrm{len}\, E)\}$.

Let F be a with evenly repeated values-member set. Note that every element of F is finite, function-like, and relation-like and every element of F has evenly repeated values. Now we state the proposition:

(97) Let us consider an enumeration E_1 of F_1, and a function p. Suppose $\bigcup F_1 \subseteq \mathrm{dom}\, p$ and $p \restriction \bigcup F_1$ is one-to-one. Then

(i) $({}^\circ p) \cdot E_1$ is an enumeration of $({}^\circ p)^\circ F_1$, and

(ii) $\overline{\overline{E_1}} = \overline{\overline{({}^\circ p) \cdot E_1}}$.

PROOF: Set $I_3 = {}^\circ f$. Reconsider $f_7 = I_3 \cdot E_1$ as a finite sequence. f_7 is one-to-one. $\mathrm{rng}\, f_7 \subseteq ({}^\circ f)^\circ F_1$. $({}^\circ f)^\circ F_1 \subseteq \mathrm{rng}\, f_7$. □

Let us consider an enumeration E_1 of F_1, a function g, an enumeration g_1 of $({}^\circ g)^\circ F_1$, a finite sequence f_{11} of elements of D, and a finite sequence s. Now we state the propositions:

(98) Suppose $\bigcup F_1 \subseteq \mathrm{dom}\, g$ and $g \restriction \bigcup F_1$ is one-to-one. Then suppose $g_1 = ({}^\circ g) \cdot E_1$. Then suppose $g^\circ \mathrm{dom}\, f \subseteq \mathrm{dom}\, f_{11}$. Then suppose $s \in \mathrm{dom}_\kappa(\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1(\kappa)$ and $\mathrm{rng}\, s \subseteq \mathrm{dom}\, g$.
Then $g \cdot s \in \mathrm{dom}_\kappa(\mathrm{SignGenOp}(f_{11}, A, ({}^\circ g)^\circ F_1)) \cdot g_1(\kappa)$.
PROOF: $\mathrm{len}(\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1 = \mathrm{len}\, E_1 = \mathrm{len}\, g_1 = \mathrm{len}(\mathrm{SignGenOp}(f, A, ({}^\circ g)^\circ F_1)) \cdot g_1$. Reconsider $g_3 = g \cdot s$ as a finite sequence. $\mathrm{len}\, s = \mathrm{len}(\mathrm{Sign}$-

GenOp$(f, A, F_1)) \cdot E_1$. For every i such that $i \in \operatorname{dom} g_3$ holds $g_3(i) \in \operatorname{dom}(((\operatorname{SignGenOp}(gf, A, (^\circ g)^\circ F_1)) \cdot g_1)(i))$. □

(99) Suppose $\bigcup F_1 \subseteq \operatorname{dom} g$ and g is one-to-one. Then suppose $g_1 = (^\circ g) \cdot E_1$. Then suppose $f_{11} = f \cdot (g^{-1}) \restriction \operatorname{dom} f_{11}$ and $g^\circ \operatorname{dom} f \subseteq \operatorname{dom} f_{11}$. Then suppose $s \in \operatorname{dom}_\kappa(\operatorname{SignGenOp}(f, A, F_1)) \cdot E_1(\kappa)$ and $\operatorname{rng} s \subseteq \operatorname{dom} g$. Then $(\operatorname{App}((\operatorname{SignGenOp}(f, A, F_1)) \cdot E_1))(s) = (\operatorname{App}((\operatorname{SignGenOp}(f_{11}, A, (^\circ g)^\circ F_1)) \cdot g_1))(g \cdot s)$.

Proof: $\operatorname{len}(\operatorname{SignGenOp}(f, A, F_1)) \cdot E_1 = \operatorname{len} E_1 = \operatorname{len} g_1 = \operatorname{len}(\operatorname{SignGenOp}$ $(f, A, (^\circ g)^\circ F_1)) \cdot g_1$. Reconsider $g_3 = g \cdot s$ as a finite sequence. Reconsider $g_3 = g \cdot s$ as a finite sequence. $\operatorname{len} g_3 = \operatorname{len} s = \operatorname{len}(\operatorname{SignGenOp}(f, A, (^\circ g)^\circ F_1)) \cdot g_1$. $g_3 \in \operatorname{dom}_\kappa(\operatorname{SignGenOp}(gf, A, (^\circ g)^\circ F_1)) \cdot g_1(\kappa)$. $\operatorname{len} s = \operatorname{len}(\operatorname{SignGenOp}(f, A, F_1)) \cdot E_1$. $g_3 = g \cdot s$ and $g_3 \in \operatorname{dom}_\kappa(\operatorname{SignGenOp}(gf, A, (^\circ g)^\circ F_1)) \cdot g_1(\kappa)$. For every i such that $1 \leqslant i \leqslant \operatorname{len} s$ holds $(\operatorname{App}((\operatorname{SignGenOp}(f, A, F_1)) \cdot E_1))(s)(i) = (\operatorname{App}((\operatorname{SignGenOp}(gf, A, (^\circ g)^\circ F_1)) \cdot g_1))(g_3)(i)$. □

(100) Let us consider an enumeration E_1 of F_1. Suppose $\bigcup F_1 \subseteq \operatorname{dom} f$. Let us consider a permutation g of $\operatorname{dom} f$, and an enumeration g_1 of $(^\circ g)^\circ F_1$. Suppose $g_1 = (^\circ g) \cdot E_1$. Let us consider a finite sequence f_{11} of elements of D. Suppose $f_{11} = f \cdot (g^{-1})$. Let us consider an element S_1 of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}((\operatorname{SignGenOp}(f, A, F_1)) \cdot E_1))$. Then $\{g \cdot s$, where s is a finite sequence of elements of $\mathbb{N} : s \in S_1\}$ is an element of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}((\operatorname{SignGenOp}(f_{11}, A, (^\circ g)^\circ F_1)) \cdot g_1))$.

Proof: $\{g \cdot s$, where s is a finite sequence of elements of $\mathbb{N} : s \in S_1\} \subseteq \operatorname{dom}(\operatorname{App}((\operatorname{SignGenOp}(f_{11}, A, (^\circ g)^\circ F_1)) \cdot g_1))$. □

(101) Suppose A is unital, commutative, and associative. Let us consider an enumeration E_1 of F_1. Suppose $\bigcup F_1 \subseteq \operatorname{dom} f$. Let us consider a permutation g of $\operatorname{dom} f$, and an enumeration g_1 of $(^\circ g)^\circ F_1$. Suppose $g_1 = (^\circ g) \cdot E_1$. Let us consider a finite sequence f_{11} of elements of D. Suppose $f_{11} = f \cdot (g^{-1})$. Let us consider non-empty, non empty finite sequences C_4, C_7 of elements of D^*. Suppose $C_4 = (\operatorname{SignGenOp}(f, A, F_1)) \cdot E_1$ and $C_7 = (\operatorname{SignGenOp}(f_{11}, A, (^\circ g)^\circ F_1)) \cdot g_1$. Let us consider an element S_1 of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}(C_4))$, and an element S_2 of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}(C_7))$. Suppose $S_2 = \{g \cdot s$, where s is a finite sequence of elements of $\mathbb{N} : s \in S_1\}$. Then $A\text{-}\sum_{S_1}(M \odot \operatorname{App}(C_4)) = A\text{-}\sum_{S_2}(M \odot \operatorname{App}(C_7))$.

Proof: Define $\mathcal{P}[\text{set}] \equiv$ for every element S_1 of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}(C_4))$ for every element S_2 of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}(C_7))$ such that $S_1 = \$_1$ and $S_2 = \{g \cdot s$, where s is a finite sequence of elements of $\mathbb{N} : s \in S_1\}$ holds $A\text{-}\sum_{S_1}(M \odot \operatorname{App}(C_4)) = A\text{-}\sum_{S_2}(M \odot \operatorname{App}(C_7))$. $\mathcal{P}[\emptyset_{\operatorname{dom}(\operatorname{App}(C_4))}]$. For every element B' of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}(C_4))$ and for every element b of $\operatorname{dom}(\operatorname{App}(C_4))$ such that $\mathcal{P}[B']$ and $b \notin B'$ holds $\mathcal{P}[B' \cup \{b\}]$. For every element B of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}(C_4))$, $\mathcal{P}[B]$. □

(102) Let us consider an enumeration E_1 of F_1. Suppose $n \in \operatorname{dom} f$. Then $\operatorname{len} E_1 \mapsto n \in \operatorname{dom}_\kappa(\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1(\kappa)$.
PROOF: Set $C_3 = (\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1$. Set $s = \operatorname{len} E_1 \mapsto n$. For every i such that $i \in \operatorname{dom} s$ holds $s(i) \in \operatorname{dom}(C_3(i))$. □

(103) Suppose B is unital, associative, and commutative and has inverse operation. Then (the inverse operation w.r.t. $B)(B(d_1, d_2)) = B(($the inverse operation w.r.t. $B)(d_1),($the inverse operation w.r.t. $B)(d_2))$.

Let x be an object and n be an even natural number. One can check that $n \mapsto x$ has evenly repeated values.

Let us consider finite sequences f, g. Now we state the propositions:

(104) If $f \frown g$ has evenly repeated values and f has evenly repeated values, then g has evenly repeated values.

(105) If $f \frown g$ has evenly repeated values and g has evenly repeated values, then f has evenly repeated values.

Let x be an object and n be an even natural number. Let us note that $n \mapsto x$ has evenly repeated values.

Let X, Y be with evenly repeated values-member sets. Note that $X \cup Y$ is with evenly repeated values-member.

Let n, k be natural numbers. The functor $\mathrm{doms}(n, k)$ yielding a finite sequence-membered, finite set is defined by the term

(Def. 14) $(\operatorname{Seg} n)^k$.

Note that every element of $\mathrm{doms}(n, k)$ is $(\operatorname{Seg} n)$-valued.

Let n be a non empty natural number and k be a natural number. Let us note that $\mathrm{doms}(n, k)$ is non empty and every element of $\mathrm{doms}(n, k)$ is k-element.

Now we state the proposition:

(106) Let us consider an enumeration E of F. Then $\operatorname{dom}_\kappa(\mathrm{SignGenOp}(f, A, F)) \cdot E(\kappa) = \mathrm{doms}(\operatorname{len} f, \overline{\overline{F}})$.
PROOF: $\operatorname{dom}_\kappa(\mathrm{SignGenOp}(f, A, F)) \cdot E(\kappa) \subseteq \mathrm{doms}(\operatorname{len} f, \overline{\overline{F}})$. Consider s being an element of $(\operatorname{Seg} \operatorname{len} f)^*$ such that $x = s$ and $\operatorname{len} s = \overline{\overline{F}}$. For every i such that $i \in \operatorname{dom} s$ holds $s(i) \in \operatorname{dom}(((\mathrm{SignGenOp}(f, A, F)) \cdot E)(i))$. □

Let us consider an enumeration E_1 of F_1 and an enumeration E_2 of F_2. Now we state the propositions:

(107) Suppose $\overline{\overline{F_1}} = \overline{\overline{F_2}}$ and $\operatorname{len} f \leqslant \operatorname{len} g$. Then $\operatorname{dom}_\kappa(\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1(\kappa) \subseteq \operatorname{dom}_\kappa(\mathrm{SignGenOp}(g, A, F_2)) \cdot E_2(\kappa)$.
PROOF: $\operatorname{len} x = \operatorname{len}(\mathrm{SignGenOp}(g, A, F_2)) \cdot E_2$. For every i such that $i \in \operatorname{dom} x$ holds $x(i) \in \operatorname{dom}(((\mathrm{SignGenOp}(g, A, F_2)) \cdot E_2)(i))$. □

(108) Suppose $\overline{\overline{F_1}} = \overline{\overline{F_2}}$. Then $\operatorname{dom}_\kappa(\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1(\kappa) = \operatorname{dom}_\kappa(\mathrm{SignGenOp}(f, A, F_2)) \cdot E_2(\kappa)$.

PROOF: $\mathrm{dom}_\kappa(\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1(\kappa) \subseteq \mathrm{dom}_\kappa(\mathrm{SignGenOp}(f, A, F_2)) \cdot E_2(\kappa)$. $\mathrm{len}\, x = \mathrm{len}(\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1$. For every i such that $i \in \mathrm{dom}\, x$ holds $x(i) \in \mathrm{dom}(((\mathrm{SignGenOp}(f, A, F_1)) \cdot E_1)(i))$. □

(109) Let us consider an enumeration E of F, and a permutation p of $\mathrm{dom}\, E$. Then $E \cdot p$ is an enumeration of F.

Let us consider an enumeration E of F, a permutation p of $\mathrm{dom}\, E$, and a finite sequence s. Now we state the propositions:

(110) If $s \in \mathrm{dom}_\kappa(\mathrm{SignGenOp}(f, A, F)) \cdot E(\kappa)$,
then $s \cdot p \in \mathrm{dom}_\kappa(\mathrm{SignGenOp}(f, A, F)) \cdot (E \cdot p)(\kappa)$.
PROOF: Reconsider $E_{28} = E \cdot p$ as an enumeration of F. $\mathrm{len}\, s = \mathrm{len}(\mathrm{SignGenOp}(f, A, F)) \cdot E = \mathrm{len}\, E = \overline{\overline{F}}$. Reconsider $s_7 = s \cdot p$ as a finite sequence. For every i such that $i \in \mathrm{dom}\, s_7$ holds $s_7(i) \in \mathrm{dom}(((\mathrm{SignGenOp}(f, A, F)) \cdot E_{28})(i))$. □

(111) Suppose $s \in \mathrm{dom}_\kappa(\mathrm{SignGenOp}(f, A, F)) \cdot E(\kappa)$. Then $(\mathrm{App}((\mathrm{SignGenOp}(f, A, F)) \cdot E))(s) \cdot p = (\mathrm{App}((\mathrm{SignGenOp}(f, A, F)) \cdot (E \cdot p)))(s \cdot p)$.
PROOF: Set $C = \mathrm{SignGenOp}(f, A, F)$. $s \cdot p \in \mathrm{dom}_\kappa\, C \cdot (E \cdot p)(\kappa)$. Reconsider $s_7 = s \cdot p$ as a finite sequence. $\mathrm{len}\, s = \mathrm{len}\, C \cdot E = \mathrm{len}\, E$. For every i such that $i \in \mathrm{dom}((\mathrm{App}(C \cdot (E \cdot p)))(s_7))$ holds $((\mathrm{App}(C \cdot E))(s) \cdot p)(i) = (\mathrm{App}(C \cdot (E \cdot p)))(s_7)(i)$. □

(112) Suppose M is commutative and associative. Then suppose $s \in \mathrm{dom}_\kappa(\mathrm{SignGenOp}(f, A, F)) \cdot E(\kappa)$ and ($\mathrm{len}\, s \geqslant 1$ or M is unital). Then $(M \odot \mathrm{App}((\mathrm{SignGenOp}(f, A, F)) \cdot E))(s) = (M \odot \mathrm{App}((\mathrm{SignGenOp}(f, A, F)) \cdot (E \cdot p)))(s \cdot p)$. The theorem is a consequence of (110), (47), and (111).

(113) Let us consider an enumeration E of F, a permutation p of $\mathrm{dom}\, E$, and an element S of $\mathrm{Fin}\, \mathrm{dom}(\mathrm{App}((\mathrm{SignGenOp}(f, A, F)) \cdot E))$. Then $\{s \cdot p$, where s is a finite sequence of elements of $\mathbb{N} : s \in S\}$ is an element of $\mathrm{Fin}\, \mathrm{dom}(\mathrm{App}((\mathrm{SignGenOp}(f, A, F)) \cdot (E \cdot p)))$. The theorem is a consequence of (110).

(114) Let us consider an enumeration E of F, a permutation p of $\mathrm{dom}\, E$, and an element S of $\mathrm{Fin}\, \mathrm{doms}(n, \overline{\overline{F}})$. Then $\{s \cdot p$, where s is a finite sequence of elements of $\mathbb{N} : s \in S\}$ is an element of $\mathrm{Fin}\, \mathrm{doms}(n, \overline{\overline{F}})$. The theorem is a consequence of (109), (110), and (106).

(115) Suppose M is commutative and associative and A is unital, commutative, and associative. Let us consider an enumeration E of F, and a permutation p of $\mathrm{dom}\, E$. Suppose M is unital or $\mathrm{len}\, E \geqslant 1$. Let us consider non-empty, non empty finite sequences C_3, C_{11} of elements of D^*. Suppose $C_3 = (\mathrm{SignGenOp}(f, A, F)) \cdot E$ and $C_{11} = (\mathrm{SignGenOp}(f, A, F)) \cdot (E \cdot p)$. Let us consider an element S of $\mathrm{Fin}\, \mathrm{dom}(\mathrm{App}(C_3))$, and an element S_{13} of $\mathrm{Fin}\, \mathrm{dom}(\mathrm{App}(C_{11}))$.

Suppose $S_{13} = \{s \cdot p$, where s is a finite sequence of elements of $\mathbb{N}$: $s \in S\}$. Then $A\text{-}\sum_S(M \odot \mathrm{App}(C_3)) = A\text{-}\sum_{S_{13}}(M \odot \mathrm{App}(C_{11}))$.

PROOF: Define $\mathcal{P}[\mathrm{set}] \equiv$ for every element S of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_3))$ for every element S_{13} of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_{11}))$ such that $S = \$_1$ and $S_{13} = \{s \cdot p$, where s is a finite sequence of elements of $\mathbb{N}$: $s \in S\}$ holds $A\text{-}\sum_S(M \odot \mathrm{App}(C_3)) = A\text{-}\sum_{S_{13}}(M \odot \mathrm{App}(C_{11}))$. $\mathcal{P}[\emptyset_{\mathrm{dom}(\mathrm{App}(C_3))}]$. For every element B' of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_3))$ and for every element b of $\mathrm{dom}(\mathrm{App}(C_3))$ such that $\mathcal{P}[B']$ and $b \notin B'$ holds $\mathcal{P}[B' \cup \{b\}]$. For every element B of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_3))$, $\mathcal{P}[B]$. □

(116) Suppose A is unital and associative and has inverse operation. Let us consider finite sets F, F_9. Suppose $F_9 = F \Cup 2^{\{\mathrm{len}\,f+1\}}$ and $\bigcup F \subseteq \mathrm{dom}\,f$. Let us consider an enumeration E_1 of F_9. Then there exists an enumeration E_2 of F_9 such that $(\mathrm{SignGenOp}(f \frown \langle d_1 \rangle, A, F_9)) \cdot E_1 = (\mathrm{SignGenOp}(f \frown \langle(\text{the inverse operation w.r.t. } A)(d_1)\rangle, A, F_9)) \cdot E_2$.

PROOF: Set $I =$ the inverse operation w.r.t. A. Define $\mathcal{P}[\mathrm{object}, \mathrm{object}] \equiv \$_2 \in \mathrm{dom}\,E_1$ and if $1 + \mathrm{len}\,f \in E_1(\$_1)$, then $E_1(\$_2) = E_1(\$_1) \setminus \{1 + \mathrm{len}\,f\}$ and if $1 + \mathrm{len}\,f \notin E_1(\$_1)$, then $E_1(\$_2) = E_1(\$_1) \cup \{1 + \mathrm{len}\,f\}$. For every x such that $x \in \mathrm{dom}\,E_1$ there exists y such that $\mathcal{P}[x, y]$.

Consider p being a function such that $\mathrm{dom}\,p = \mathrm{dom}\,E_1$ and for every x such that $x \in \mathrm{dom}\,E_1$ holds $\mathcal{P}[x, p(x)]$. $\mathrm{rng}\,p \subseteq \mathrm{dom}\,E_1$. $\mathrm{dom}\,E_1 \subseteq \mathrm{rng}\,p$. Reconsider $E_4 = E_1 \cdot p$ as an enumeration of F_9. For every i such that $1 \leqslant i \leqslant \mathrm{len}(\mathrm{SignGenOp}(f \frown \langle d_1 \rangle, A, F_9)) \cdot E_1$ holds $((\mathrm{SignGenOp}(f \frown \langle d_1 \rangle, A, F_9)) \cdot E_1)(i) = ((\mathrm{SignGenOp}(f \frown \langle I(d_1) \rangle, A, F_9)) \cdot E_4)(i)$. □

(117) Suppose A is unital, associative, and commutative and has inverse operation. Let us consider a finite, non empty set F. Suppose $\bigcup F \subseteq \mathrm{dom}\,f$. Let us consider finite sets F_1, F_2. Suppose $F_1 = F \Cup 2^{\{\mathrm{len}\,f+1\}}$ and $F_2 = F \Cup 2^{\{\mathrm{len}\,f+1, \mathrm{len}\,f+2\}}$. Then there exist enumerations E_1, E_2 of F_1 and there exists an enumeration E of F_2 such that $A \odot (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, A, F_2)) \cdot E = (A \odot (\mathrm{SignGenOp}(f \frown \langle A(d_1, d_2) \rangle, A, F_1)) \cdot E_1) \frown (A \odot (\mathrm{SignGenOp}(f \frown \langle A((\text{the inverse operation w.r.t. } A)(d_1), d_2) \rangle, A, F_1)) \cdot E_2)$. The theorem is a consequence of (91), (116), and (2).

(118) Suppose A is unital. Let us consider an enumeration E of F, and a finite sequence s. Suppose $F = \emptyset$ and $s \in \mathrm{dom}_\kappa(\mathrm{SignGenOp}(f, B, F)) \cdot E(\kappa)$. Then $(A \odot \mathrm{App}((\mathrm{SignGenOp}(f, B, F)) \cdot E))(s) = \mathbf{1}_A$. The theorem is a consequence of (47) and (59).

(119) Let us consider an enumeration E of F, a permutation p of $\mathrm{dom}\,E$, and a subset S of $\mathrm{doms}(n, \overline{\overline{F}})$. Then $\{s \cdot p$, where s is a finite sequence of elements of $\mathbb{N}$: $s \in S\}$ is a subset of $\mathrm{doms}(n, \overline{\overline{F}})$. The theorem is a consequence of (109), (110), and (106).

(120) Let us consider finite sequences f, g. Suppose ($\operatorname{len} f = n$ or $\operatorname{len} g = m$) and $f \smallfrown g \in \operatorname{doms}(k, n+m)$. Then

- (i) $f \in \operatorname{doms}(k, n)$, and
- (ii) $g \in \operatorname{doms}(k, m)$.

(121) Let us consider a finite sequence f. If $f \in \operatorname{doms}(n, k)$, then $\operatorname{len} f = k$.

(122) Let us consider finite sequences f, g. Suppose $f \in \operatorname{doms}(k, n)$ and $g \in \operatorname{doms}(k, m)$. Then $f \smallfrown g \in \operatorname{doms}(k, n+m)$.

(123) $\operatorname{doms}(k, n) \smallfrown \operatorname{doms}(k, m) = \operatorname{doms}(k, n+m)$. The theorem is a consequence of (122) and (120).

(124) Let us consider an enumeration E of F, a permutation p of $\operatorname{dom} E$, and a finite sequence s. Suppose $s \in \operatorname{doms}(m, \overline{\overline{F}})$. Then $s \cdot p \in \operatorname{doms}(m, \overline{\overline{F}})$. The theorem is a consequence of (109) and (121).

(125) If $k \leqslant n$, then $\operatorname{doms}(k, m) \subseteq \operatorname{doms}(n, m)$.

(126) Suppose A is commutative, associative, and unital and has inverse operation and M is associative, commutative, and unital and M is distributive w.r.t. A. Let us consider an enumeration E_1 of F_1, and an enumeration E_2 of F_2. Suppose $\bigcup F_1 \subseteq \operatorname{Seg}(1+m)$ and $\bigcup F_2 \subseteq \operatorname{Seg}(1+m)$. Let us consider an enumeration E_{17} of $\operatorname{ext}(F_1, 1+m, 2+m)$, and an enumeration E_{33} of $\operatorname{swap}(F_2, 1+m, 2+m)$.

Suppose $E_{17} = \operatorname{Ext}(E_1, 1+m, 2+m)$ and $E_{33} = \operatorname{Swap}(E_2, 1+m, 2+m)$. Let us consider an enumeration E_{21} of $\operatorname{ext}(F_1, 1+m, 2+m) \cup \operatorname{swap}(F_2, 1+m, 2+m)$. Suppose $E_{21} = E_{17} \smallfrown E_{33}$. Let us consider finite sequences s_1, s_2. Suppose $s_1 \in \operatorname{doms}(m+1, \overline{\overline{F_1}})$ and $s_2 \in \operatorname{doms}(m+1, \overline{\overline{F_2}})$ and $s_1 \smallfrown s_2$ has evenly repeated values and $\overline{\overline{{s_1}^{-1}(\{1+m\})}} = \overline{\overline{{s_2}^{-1}(\{1+m\})}}$. Then there exists a subset S of $\operatorname{doms}(m+2, \overline{\overline{F_1}} + \overline{\overline{F_2}})$ such that

- (i) if $\overline{\overline{{s_1}^{-1}(\{1+m\})}} = 0$, then $s_1 \smallfrown s_2 \in S$, and
- (ii) S is with evenly repeated values-member, and
- (iii) for every finite sequences C_4, C_7 of elements of D^* and for every f, d_1, and d_2 such that $\operatorname{len} f = m$ and $C_4 = (\operatorname{SignGenOp}(f \smallfrown \langle A(d_1, d_2) \rangle, A, F_1)) \cdot E_1$ and $C_7 = (\operatorname{SignGenOp}(f \smallfrown \langle A((\text{the inverse operation w.r.t. } A)(d_1), d_2) \rangle, A, F_2)) \cdot E_2$ for every non-empty, non empty finite sequence C_{17} of elements of D^* such that $C_{17} = (\operatorname{SignGenOp}((f \smallfrown \langle d_1 \rangle) \smallfrown \langle d_2 \rangle, A, \operatorname{ext}(F_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f) \cup \operatorname{swap}(F_2, 1 + \operatorname{len} f, 2 + \operatorname{len} f))) \cdot E_{21}$ for every element S_7 of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}(C_{17}))$ such that $S = S_7$ holds $M((M \odot \operatorname{App}(C_4))(s_1), (M \odot \operatorname{App}(C_7))(s_2)) = A\text{-}\sum_{S_7}(M \odot \operatorname{App}(C_{17}))$ and for every finite sequence h and for every i such that $h \in S_7$ and $i \in \operatorname{dom} h$ holds if $(s_1 \smallfrown s_2)(i) = 1 + \operatorname{len} f$, then $h(i) \in \{1 + \operatorname{len} f, 2 + \operatorname{len} f\}$ and if $(s_1 \smallfrown s_2)(i) \neq 1 + \operatorname{len} f$, then $h(i) = (s_1 \smallfrown s_2)(i)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every F_1 and F_2 for every enumeration E_1 of F_1 for every enumeration E_2 of F_2 such that $\bigcup F_1 \subseteq \operatorname{Seg}(1+m)$ and $\bigcup F_2 \subseteq \operatorname{Seg}(1+m)$ for every enumeration E_{17} of $\operatorname{ext}(F_1, 1+m, 2+m)$ for every enumeration E_{33} of $\operatorname{swap}(F_2, 1+m, 2+m)$ such that $E_{17} = \operatorname{Ext}(E_1, 1+m, 2+m)$ and $E_{33} = \operatorname{Swap}(E_2, 1+m, 2+m)$ for every enumeration E_{21} of $\operatorname{ext}(F_1, 1+m, 2+m) \cup \operatorname{swap}(F_2, 1+m, 2+m)$ such that $E_{21} = E_{17} \mathbin{^\frown} E_{33}$ for every finite sequences s_1, s_2 such that $s_1 \in \operatorname{doms}(m+1, \overline{\overline{F_1}})$ and $s_2 \in \operatorname{doms}(m+1, \overline{\overline{F_2}})$ and $s_1 \mathbin{^\frown} s_2$ has evenly repeated values and $\overline{\overline{{s_1}^{-1}(\{1+m\})}} = \$_1 = \overline{\overline{{s_2}^{-1}(\{1+m\})}}$ there exists a subset S of $\operatorname{doms}(m+2, \overline{\overline{F_1}} + \overline{\overline{F_2}})$ such that if $\overline{\overline{{s_1}^{-1}(\{1+m\})}} = 0$, then $s_1 \mathbin{^\frown} s_2 \in S$.

S is with evenly repeated values-member and for every finite sequences C_4, C_7 of elements of D^* and for every f, d_1, and d_2 such that $\operatorname{len} f = m$ and $C_4 = (\operatorname{SignGenOp}(f \mathbin{^\frown} \langle A(d_1, d_2)\rangle, A, F_1)) \cdot E_1$ and $C_7 = (\operatorname{SignGenOp}(f \mathbin{^\frown} \langle A((\text{the inverse operation w.r.t. } A)(d_1), d_2)\rangle, A, F_2)) \cdot E_2$ for every non-empty, non empty finite sequence C_{17} of elements of D^* such that $C_{17} = (\operatorname{SignGenOp}((f \mathbin{^\frown} \langle d_1\rangle) \mathbin{^\frown} \langle d_2\rangle, A, \operatorname{ext}(F_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f) \cup \operatorname{swap}(F_2, 1{+}\operatorname{len} f, 2{+}\operatorname{len} f))) \cdot E_{21}$ for every element S_7 of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}(C_{17}))$ such that $S = S_7$ holds $M((M \odot \operatorname{App}(C_4))(s_1), (M \odot \operatorname{App}(C_7))(s_2)) = A\text{-}\sum_{S_7}(M \odot \operatorname{App}(C_{17}))$ and for every finite sequence h and for every i such that $h \in S_7$ and $i \in \operatorname{dom} h$ holds if $(s_1 \mathbin{^\frown} s_2)(i) = 1 + \operatorname{len} f$, then $h(i) \in \{1 + \operatorname{len} f, 2 + \operatorname{len} f\}$ and if $(s_1 \mathbin{^\frown} s_2)(i) \neq 1 + \operatorname{len} f$, then $h(i) = (s_1 \mathbin{^\frown} s_2)(i)$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[0]$. $\mathcal{P}[n]$. □

(127) Suppose A is commutative, associative, and unital and has inverse operation and M is associative, commutative, and unital and M is distributive w.r.t. A. Let us consider an enumeration E_1 of F_1. Suppose $\bigcup F_1 \subseteq \operatorname{Seg}(1+m)$. Let us consider an enumeration E_{17} of $\operatorname{ext}(F_1, 1+m, 2+m)$. Suppose $E_{17} = \operatorname{Ext}(E_1, 1+m, 2+m)$. Then there exists a subset S of $\operatorname{doms}(m+2, \overline{\overline{F_1}})$ such that

(i) $S = \{1+m, 2+m\}^{\operatorname{len} E_1}$, and

(ii) for every non-empty, non empty finite sequence C_{16} of elements of D^* and for every f, d_1, and d_2 such that $\operatorname{len} f = m$ and $C_{16} = (\operatorname{SignGenOp}((f \mathbin{^\frown} \langle d_1\rangle) \mathbin{^\frown} \langle d_2\rangle, A, \operatorname{ext}(F_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f))) \cdot E_{17}$ for every element S_7 of $\operatorname{Fin} \operatorname{dom}(\operatorname{App}(C_{16}))$ such that $S_7 = S$ holds $(M \odot \operatorname{App}((\operatorname{SignGenOp}(f \mathbin{^\frown} \langle A(d_1, d_2)\rangle, A, F_1)) \cdot E_1))(\operatorname{len} E_1 \mapsto (1 + \operatorname{len} f)) = A\text{-}\sum_{S_7}(M \odot \operatorname{App}(C_{16}))$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every F_1 for every enumeration E_1 of F_1 such that $\bigcup F_1 \subseteq \operatorname{Seg}(1+m)$ and $\operatorname{len} E_1 = \$_1$ for every enumeration E_{17} of $\operatorname{ext}(F_1, 1+m, 2+m)$ such that $E_{17} = \operatorname{Ext}(E_1, 1+m, 2+m)$ there exists a subset S of $\operatorname{doms}(m+2, \overline{\overline{F_1}})$ such that $S = \{1{+}m, 2{+}m\}^{\operatorname{len} E_1}$ and for every non-empty, non empty finite sequence C_{16} of elements of D^* and for every f, d_1, and d_2 such that $\operatorname{len} f = m$ and $C_{16} = (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, A, \mathrm{ext}(F_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f))) \cdot E_{17}$ for every element S_7 of $\operatorname{Fin} \operatorname{dom}(\mathrm{App}(C_{16}))$ such that $S_7 = S$ holds $(M \odot \mathrm{App}((\mathrm{SignGenOp}(f \frown \langle A(d_1, d_2) \rangle, A, F_1)) \cdot E_1))(\operatorname{len} E_1 \mapsto (1 + \operatorname{len} f)) = A\text{-}\sum_{S_7}(M \odot \mathrm{App}(C_{16}))$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

(128) Suppose A is commutative, associative, and unital and has inverse operation. Let us consider an enumeration E_1 of F_1. Suppose $\bigcup F_1 \subseteq \mathrm{Seg}(1 + \operatorname{len} f)$. Let us consider an enumeration E_{17} of $\mathrm{ext}(F_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f)$, and an enumeration E_{33} of $\mathrm{swap}(F_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f)$. Suppose $E_{17} = \mathrm{Ext}(E_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f)$ and $E_{33} = \mathrm{Swap}(E_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f)$. Let us consider a non-empty, non empty finite sequence C_{16} of elements of D^*, and a non-empty, non empty finite sequence C_{20} of elements of D^*.

Suppose $C_{16} = (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, A, \mathrm{ext}(F_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f))) \cdot E_{17}$ and $C_{20} = (\mathrm{SignGenOp}((f \frown \langle (\text{the inverse operation w.r.t. } A)(d_1) \rangle) \frown \langle d_2 \rangle, A, \mathrm{swap}(F_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f))) \cdot E_{33}$. Let us consider an element S_1 of $\operatorname{Fin} \operatorname{dom}(\mathrm{App}(C_{16}))$, and an element S_2 of $\operatorname{Fin} \operatorname{dom}(\mathrm{App}(C_{20}))$. Suppose $S_1 = S_2$. Then $A\text{-}\sum_{S_1}(M \odot \mathrm{App}(C_{16})) = A\text{-}\sum_{S_2}(M \odot \mathrm{App}(C_{20}))$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every element S_1 of $\operatorname{Fin} \operatorname{dom}(\mathrm{App}(C_{16}))$ for every element S_2 of $\operatorname{Fin} \operatorname{dom}(\mathrm{App}(C_{20}))$ such that $S_1 = S_2$ and $\overline{\overline{S_1}} = \$_1$ holds $A\text{-}\sum_{S_1}(M \odot \mathrm{App}(C_{16})) = A\text{-}\sum_{S_2}(M \odot \mathrm{App}(C_{20}))$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

(129) Suppose A is commutative, associative, and unital and has inverse operation and M is associative, commutative, and unital and M is distributive w.r.t. A. Let us consider an enumeration E_1 of F_1. Suppose $\bigcup F_1 \subseteq \mathrm{Seg}(1 + m)$. Let us consider an enumeration E_{33} of $\mathrm{swap}(F_1, 1 + m, 2 + m)$. Suppose $E_{33} = \mathrm{Swap}(E_1, 1 + m, 2 + m)$. Then there exists a subset S of $\mathrm{doms}(m + 2, \overline{\overline{F_1}})$ such that

(i) $S = \{1 + m, 2 + m\}^{\operatorname{len} E_1}$, and

(ii) for every non-empty, non empty finite sequence C_{20} of elements of D^* and for every f, d_1, and d_2 such that $\operatorname{len} f = m$ and $C_{20} = (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, A, \mathrm{swap}(F_1, 1 + \operatorname{len} f, 2 + \operatorname{len} f))) \cdot E_{33}$ for every element S_7 of $\operatorname{Fin} \operatorname{dom}(\mathrm{App}(C_{20}))$ such that $S_7 = S$ holds $(M \odot \mathrm{App}((\mathrm{SignGenOp}(f \frown \langle A((\text{the inverse operation w.r.t. } A)(d_1), d_2) \rangle, A, F_1)) \cdot E_1))(\operatorname{len} E_1 \mapsto (1 + \operatorname{len} f)) = A\text{-}\sum_{S_7}(M \odot \mathrm{App}(C_{20}))$.

The theorem is a consequence of (28), (127), (80), (10), (11), (107), and (128).

(130) Suppose A is unital, associative, and commutative and has inverse operation and M is commutative and associative and $\operatorname{len} f \neq 0$. Then SignGenOp

$((f \frown \langle d_1\rangle) \frown \langle d_2\rangle, M, A, (\mathrm{Seg}(2+\mathrm{len}\, f)) \setminus \{1\}) = M(\mathrm{SignGenOp}(f \frown \langle A(d_1, d_2)\rangle, M, A, (\mathrm{Seg}(1+\mathrm{len}\, f)) \setminus \{1\}), \mathrm{SignGenOp}(f \frown \langle A((\text{the inverse operation w.r.t. } A)(d_1), d_2)\rangle, M, A, (\mathrm{Seg}(1+\mathrm{len}\, f)) \setminus \{1\}))$. The theorem is a consequence of (6), (117), and (64).

(131) Let us consider an enumeration E of F. Suppose $\bigcup F \subseteq \mathrm{Seg}(1+\mathrm{len}\, f)$. Let us consider an enumeration E_{17} of $\mathrm{ext}(F, 1+\mathrm{len}\, f, 2+\mathrm{len}\, f)$. Suppose $E_{17} = \mathrm{Ext}(E, 1+\mathrm{len}\, f, 2+\mathrm{len}\, f)$. Let us consider finite sequences C_4, C_9 of elements of D^*. Suppose $C_4 = (\mathrm{SignGenOp}(f \frown \langle d\rangle, A, F)) \cdot E$ and $C_9 = (\mathrm{SignGenOp}((f \frown \langle d_1\rangle) \frown \langle d_2\rangle, A, \mathrm{ext}(F, 1+\mathrm{len}\, f, 2+\mathrm{len}\, f))) \cdot E_{17}$. Let us consider a finite sequence s. Suppose $s \in \mathrm{dom}_\kappa\, C_4(\kappa)$ and $\mathrm{rng}\, s \subseteq \mathrm{dom}\, f$. Then

(i) $s \in \mathrm{dom}_\kappa\, C_9(\kappa)$, and

(ii) $(\mathrm{App}(C_4))(s) = (\mathrm{App}(C_9))(s)$.

Proof: $\mathrm{dom}_\kappa\, C_4(\kappa) \subseteq \mathrm{dom}_\kappa\, C_9(\kappa)$. $\mathrm{len}\, E = \mathrm{len}\, C_4 = \mathrm{len}\, s = \mathrm{len}\, C_9$. For every i such that $1 \leqslant i \leqslant \mathrm{len}\, s$ holds $(\mathrm{App}(C_4))(s)(i) = (\mathrm{App}(C_9))(s)(i)$. □

(132) Let us consider an enumeration E of F. Suppose $\bigcup F \subseteq \mathrm{Seg}(1+\mathrm{len}\, f)$. Let us consider an enumeration E_{33} of $\mathrm{swap}(F, 1+\mathrm{len}\, f, 2+\mathrm{len}\, f)$. Suppose $E_{33} = \mathrm{Swap}(E, 1+\mathrm{len}\, f, 2+\mathrm{len}\, f)$. Let us consider finite sequences C_4, C_{10} of elements of D^*. Suppose $C_4 = (\mathrm{SignGenOp}(f \frown \langle d\rangle, A, F)) \cdot E$ and $C_{10} = (\mathrm{SignGenOp}((f \frown \langle d_1\rangle) \frown \langle d_2\rangle, A, \mathrm{swap}(F, 1+\mathrm{len}\, f, 2+\mathrm{len}\, f))) \cdot E_{33}$. Let us consider a finite sequence s. Suppose $s \in \mathrm{dom}_\kappa\, C_4(\kappa)$ and $\mathrm{rng}\, s \subseteq \mathrm{dom}\, f$. Then

(i) $s \in \mathrm{dom}_\kappa\, C_{10}(\kappa)$, and

(ii) $(\mathrm{App}(C_4))(s) = (\mathrm{App}(C_{10}))(s)$.

Proof: $\mathrm{dom}_\kappa\, C_4(\kappa) \subseteq \mathrm{dom}_\kappa\, C_9(\kappa)$. $\mathrm{len}\, E = \mathrm{len}\, C_4 = \mathrm{len}\, s = \mathrm{len}\, C_9$. For every i such that $1 \leqslant i \leqslant \mathrm{len}\, s$ holds $(\mathrm{App}(C_4))(s)(i) = (\mathrm{App}(C_9))(s)(i)$. □

(133) Let us consider an enumeration E_1 of F_1, and (D^*)-valued finite sequences C_4, C_7. Suppose $C_4 = (\mathrm{SignGenOp}(f \frown \langle d_1\rangle, A, F_1)) \cdot E_1$ and $C_7 = (\mathrm{SignGenOp}(f \frown \langle d_2\rangle, A, F_1)) \cdot E_1$. Let us consider a finite sequence s. Suppose $s \in \mathrm{dom}_\kappa\, C_4(\kappa)$ and $1+\mathrm{len}\, f \notin \mathrm{rng}\, s$. Then

(i) $s \in \mathrm{dom}_\kappa\, C_7(\kappa)$, and

(ii) $(\mathrm{App}(C_4))(s) = (\mathrm{App}(C_7))(s)$.

Proof: $\mathrm{dom}_\kappa\, C_4(\kappa) \subseteq \mathrm{dom}_\kappa\, C_7(\kappa)$. $\mathrm{len}\, C_4 = \mathrm{len}\, s = \mathrm{len}\, C_7$. For every i such that $1 \leqslant i \leqslant \mathrm{len}\, s$ holds $(\mathrm{App}(C_4))(s)(i) = (\mathrm{App}(C_7))(s)(i)$. □

(134) Let us consider a finite sequence s. Suppose $\overline{\overline{s^{-1}(\{y\})}} = k$. Then there exists a permutation p of $\operatorname{dom} s$ and there exists a finite sequence s_1 such that $s \cdot p = s_1 \frown (k \mapsto y)$ and $y \notin \operatorname{rng} s_1$.

(135) Let us consider a finite sequence f of elements of D. Suppose A is commutative, associative, and unital and has inverse operation and M is associative, commutative, and unital and M is distributive w.r.t. A and $n \in \operatorname{dom} f$. Let us consider an enumeration E of F, and a subset D of $\operatorname{dom} E$. Suppose for every i, $i \in D$ iff $n \in E(i)$. Then

(i) if $\overline{\overline{D}}$ is even, then $(M \odot \operatorname{App}((\operatorname{SignGenOp}(f, A, F)) \cdot E))(\operatorname{len} E \mapsto n) = M \odot \operatorname{len} E \mapsto f_{/n}$, and

(ii) if $\overline{\overline{D}}$ is odd, then $(M \odot \operatorname{App}((\operatorname{SignGenOp}(f, A, F)) \cdot E))(\operatorname{len} E \mapsto n) =$ (the inverse operation w.r.t. A)$(M \odot \operatorname{len} E \mapsto f_{/n})$.

Proof: Set $I_1 =$ the inverse operation w.r.t. A. Define $\mathcal{P}[\text{natural number}] \equiv$ for every F such that $\overline{\overline{F}} = \$_1$ for every enumeration E of F for every subset I of $\operatorname{dom} E$ such that for every i, $i \in I$ iff $n \in E(i)$ holds if $\overline{\overline{I}}$ is even, then $(M \odot \operatorname{App}((\operatorname{SignGenOp}(f, A, F)) \cdot E))(\operatorname{len} E \mapsto n) = M \odot \operatorname{len} E \mapsto f_{/n}$ and if $\overline{\overline{I}}$ is odd, then $(M \odot \operatorname{App}((\operatorname{SignGenOp}(f, A, F)) \cdot E))(\operatorname{len} E \mapsto n) = I_1(M \odot \operatorname{len} E \mapsto f_{/n})$. $\mathcal{P}[0]$. If $\mathcal{P}[j]$, then $\mathcal{P}[j+1]$. $\mathcal{P}[j]$. □

(136) Suppose M is commutative, associative, and unital and A is commutative, associative, and unital and has inverse operation and M is distributive w.r.t. A. Let us consider a finite sequence f of elements of D, an enumeration E_1 of F_1, an enumeration E_2 of F_2, and finite sequences s_1, s_2. Suppose $s_1 \in \operatorname{dom}_\kappa(\operatorname{SignGenOp}(f \frown \langle d_1 \rangle, A, F_1)) \cdot E_1(\kappa)$ and $s_2 \in \operatorname{dom}_\kappa(\operatorname{SignGenOp}(f \frown \langle d_2 \rangle, A, F_2)) \cdot E_2(\kappa)$ and $\overline{\overline{{s_1}^{-1}(\{1 + \operatorname{len} f\})}} = \overline{\overline{{s_2}^{-1}(\{1 + \operatorname{len} f\})}}$. Then $M((M \odot \operatorname{App}((\operatorname{SignGenOp}(f \frown \langle d_1 \rangle, A, F_1)) \cdot E_1))(s_1), (M \odot \operatorname{App}((\operatorname{SignGenOp}(f \frown \langle d_2 \rangle, A, F_2)) \cdot E_2))(s_2)) = M((M \odot \operatorname{App}((\operatorname{SignGenOp}(f \frown \langle d_2 \rangle, A, F_1)) \cdot E_1))(s_1), (M \odot \operatorname{App}((\operatorname{SignGenOp}(f \frown \langle d_1 \rangle, A, F_2)) \cdot E_2))(s_2))$.

Proof: Set $L = 1 + \operatorname{len} f$. $\operatorname{dom}_\kappa(\operatorname{SignGenOp}(f \frown \langle d_1 \rangle, A, F_1)) \cdot E_1(\kappa) = \operatorname{dom}_\kappa(\operatorname{SignGenOp}(f \frown \langle d_2 \rangle, A, F_1)) \cdot E_1(\kappa)$ and $\operatorname{dom}_\kappa(\operatorname{SignGenOp}(f \frown \langle d_2 \rangle, A, F_2)) \cdot E_2(\kappa) = \operatorname{dom}_\kappa(\operatorname{SignGenOp}(f \frown \langle d_1 \rangle, A, F_2)) \cdot E_2(\kappa)$. Set $k = \overline{\overline{{s_1}^{-1}(\{L\})}}$. $\operatorname{len} s_1 = \operatorname{len}(\operatorname{SignGenOp}(f \frown \langle d_1 \rangle, A, F_1)) \cdot E_1 = \operatorname{len} E_1$ and $\operatorname{len} s_2 = \operatorname{len}(\operatorname{SignGenOp}(f \frown \langle d_2 \rangle, A, F_2)) \cdot E_2 = \operatorname{len} E_2$. Set $k_1 = k \mapsto L$. Consider p_1 being a permutation of $\operatorname{dom} s_1$, S_1 being a finite sequence such that $s_1 \cdot p_1 = S_1 \frown k_1$ and $L \notin \operatorname{rng} S_1$. Reconsider $E_4 = E_1 \cdot p_1$ as an enumeration of F_1. Set $e_3 = E_4 \restriction \operatorname{len} S_1$.

Consider e_2 being a finite sequence such that $E_4 = e_3 \frown e_2$. Set $F_4 = \operatorname{rng} e_3$. Set $F_3 = \operatorname{rng} e_2$. Reconsider $E_6 = e_3$ as an enumeration of F_4. Reconsider $E_5 = e_2$ as an enumeration of F_3. Consider p_2 being a permutation of $\operatorname{dom} s_2$, S_2 being a finite sequence such that $s_2 \cdot p_2 = S_2 \frown k_1$ and $L \notin \operatorname{rng} S_2$. Reconsider $E_8 = E_2 \cdot p_2$ as an enumeration of F_2. Set $e_5 = E_8 \restriction \operatorname{len} S_2$. Consider e_4 being a finite sequence such that $E_8 = e_5 \frown e_4$. Set $F_6 = \operatorname{rng} e_5$. Set $F_5 = \operatorname{rng} e_4$. Reconsider $E_{10} = e_5$ as an enumeration of F_6. Reconsider $E_9 = e_4$ as an enumeration of F_5. $(\mathrm{SignGenOp}(f \frown \langle d_1 \rangle, A, F_1)) \cdot E_4 = (\mathrm{SignGenOp}(f \frown \langle d_1 \rangle, A, F_4)) \cdot E_6 \frown (\mathrm{SignGenOp}(f \frown \langle d_1 \rangle, A, F_3)) \cdot E_5$ and $(\mathrm{SignGenOp}(f \frown \langle d_2 \rangle, A, F_2)) \cdot E_8 = (\mathrm{SignGenOp}(f \frown \langle d_2 \rangle, A, F_6)) \cdot E_{10} \frown (\mathrm{SignGenOp}(f \frown \langle d_2 \rangle, A, F_5)) \cdot E_9$. □

(137) Suppose M is commutative, associative, and unital and A is commutative, associative, and unital and has inverse operation and M is distributive w.r.t. A. Let us consider an enumeration E_1 of F_1. Suppose $\bigcup F_1 \subseteq \mathrm{Seg}(1+m)$ and $\operatorname{len} E_1$ is even. Let us consider an enumeration E_{17} of $\mathrm{ext}(F_1, 1+m, 2+m)$, and an enumeration E_{33} of $\mathrm{swap}(F_1, 1+m, 2+m)$. Suppose $E_{17} = \mathrm{Ext}(E_1, 1+m, 2+m)$ and $E_{33} = \mathrm{Swap}(E_1, 1+m, 2+m)$. Then there exist subsets s_6, s_8 of $\mathrm{doms}(m+2, \overline{\overline{F_1}})$ such that

(i) $s_6 \subseteq \{1+m, 2+m\}^{\operatorname{len} E_1}$, and

(ii) $s_8 \subseteq \{1+m, 2+m\}^{\operatorname{len} E_1}$, and

(iii) s_6 is with evenly repeated values-member, and

(iv) s_8 is with evenly repeated values-member, and

(v) for every non-empty, non empty finite sequences C_{16}, C_{20} of elements of D^* and for every f, d_1, and d_2 such that $\operatorname{len} f = m$ and $C_{16} = (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, A, \mathrm{ext}(F_1, 1+\operatorname{len} f, 2+\operatorname{len} f))) \cdot E_{17}$ and $C_{20} = (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, A, \mathrm{swap}(F_1, 1+\operatorname{len} f, 2+\operatorname{len} f))) \cdot E_{33}$ for every element S_8 of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_{16}))$ for every element S_{14} of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_{20}))$ such that $S_8 = s_6$ and $S_{14} = s_8$ holds $A((M \odot \mathrm{App}((\mathrm{SignGenOp}(f \frown \langle A(d_1, d_2) \rangle, A, F_1)) \cdot E_1))(\operatorname{len} E_1 \mapsto (1+\operatorname{len} f)), (M \odot \mathrm{App}((\mathrm{SignGenOp}(f \frown \langle A((\text{the inverse operation w.r.t. } A)(d_1), d_2) \rangle, A, F_1)) \cdot E_1))(\operatorname{len} E_1 \mapsto (1+\operatorname{len} f))) = A(A\text{-}\sum_{S_8}(M \odot \mathrm{App}(C_{16})), A\text{-}\sum_{S_{14}}(M \odot \mathrm{App}(C_{20})))$.

Proof: Set $I =$ the inverse operation w.r.t. A. Set $L_3 = \operatorname{len} E_1$. Set $L_1 = 1+m$. Set $L_2 = 2+m$. Consider s_6 being a subset of $\mathrm{doms}(m+2, \overline{\overline{F_1}})$ such that $s_6 = \{1+m, 2+m\}^{\operatorname{len} E_1}$ and for every non-empty, non empty finite sequence C_{16} of elements of D^* and for every f, d_1, and d_2 such that $\operatorname{len} f = m$ and $C_{16} = (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, A, \mathrm{ext}(F_1, 1+\operatorname{len} f, 2+\operatorname{len} f))) \cdot E_{17}$ for every element S_7 of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_{16}))$ such that $S_7 = s_6$ holds $(M \odot \mathrm{App}((\mathrm{SignGenOp}(f \frown \langle A(d_1, d_2) \rangle, A, F_1)) \cdot E_1))(\operatorname{len} E_1 \mapsto (1+\operatorname{len} f)) = A\text{-}\sum_{S_7}(M \odot \mathrm{App}(C_{16}))$.

Consider s_8 being a subset of $\mathrm{doms}(m+2, \overline{\overline{\overline{F_1}}})$ such that $s_8 = \{1+m, 2+m\}^{\mathrm{len}\, E_1}$ and for every non-empty, non empty finite sequence C_{20} of elements of D^* and for every f, d_1, and d_2 such that $\mathrm{len}\, f = m$ and $C_{20} = (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, A, \mathrm{swap}(F_1, 1 + \mathrm{len}\, f, 2 + \mathrm{len}\, f))) \cdot E_{33}$ for every element S_7 of $\mathrm{Fin}\, \mathrm{dom}(\mathrm{App}(C_{20}))$ such that $S_7 = s_8$ holds $(M \odot \mathrm{App}((\mathrm{SignGenOp}(f \frown \langle A(I(d_1), d_2) \rangle, A, F_1)) \cdot E_1))(\mathrm{len}\, E_1 \mapsto (1 + \mathrm{len}\, f)) = A\text{-}\sum_{S_7}(M \odot \mathrm{App}(C_{20}))$. Set $C = \mathrm{CFS}(\{1+m, 2+m\}^{L_3})$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant \mathrm{len}\, C$, then there exist subsets S_5, R_4, S_{15}, R_6 of $\mathrm{doms}(m+2, \overline{\overline{\overline{F_1}}})$ such that $S_5 \subseteq \mathrm{rng}(C \upharpoonright \$_1)$ and $R_4 = \mathrm{rng}(C \upharpoonright \$_1) = R_6$ and $S_{15} \subseteq \mathrm{rng}(C \upharpoonright \$_1)$ and S_5 is with evenly repeated values-member and S_{15} is with evenly repeated values-member and for every non-empty, non empty finite sequences C_{20}, C_{15} of elements of D^* and for every f, d_1, and d_2 such that $\mathrm{len}\, f = m$ and $C_{20} = (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, A, \mathrm{swap}(F_1, 1 + \mathrm{len}\, f, 2 + \mathrm{len}\, f))) \cdot E_{33}$ and $C_{15} = (\mathrm{SignGenOp}((f \frown \langle I(d_1) \rangle) \frown \langle d_2 \rangle, A, \mathrm{swap}(F_1, 1 + \mathrm{len}\, f, 2 + \mathrm{len}\, f))) \cdot E_{33}$ for every elements S_4, R_3 of $\mathrm{Fin}\, \mathrm{dom}(\mathrm{App}(C_{15}))$.

For every elements S_{14}, R_5 of $\mathrm{Fin}\, \mathrm{dom}(\mathrm{App}(C_{20}))$ such that $S_5 = S_4$ and $R_4 = R_3$ and $S_{15} = S_{14}$ and $R_6 = R_5$ holds $A(A\text{-}\sum_{S_4}(M \odot \mathrm{App}(C_{15})), A\text{-}\sum_{S_{14}}(M \odot \mathrm{App}(C_{20}))) = A(A\text{-}\sum_{R_3}(M \odot \mathrm{App}(C_{15})), A\text{-}\sum_{R_5}(M \odot \mathrm{App}(C_{20})))$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. Consider S_5, R_4, S_{15}, R_6 being subsets of $\mathrm{doms}(m+2, \overline{\overline{\overline{F_1}}})$ such that $S_5 \subseteq \mathrm{rng}(C \upharpoonright \mathrm{len}\, C)$ and $R_4 = \mathrm{rng}(C \upharpoonright \mathrm{len}\, C) = R_6$ and $S_{15} \subseteq \mathrm{rng}(C \upharpoonright \mathrm{len}\, C)$ and S_5 is with evenly repeated values-member and S_{15} is with evenly repeated values-member and for every non-empty, non empty finite sequences C_{20}, C_{15} of elements of D^*.

For every f, d_1, and d_2 such that $\mathrm{len}\, f = m$ and $C_{20} = (\mathrm{SignGenOp}((f \frown \langle d_1 \rangle) \frown \langle d_2 \rangle, A, \mathrm{swap}(F_1, 1 + \mathrm{len}\, f, 2 + \mathrm{len}\, f))) \cdot E_{33}$ and $C_{15} = (\mathrm{SignGenOp}((f \frown \langle I(d_1) \rangle) \frown \langle d_2 \rangle, A, \mathrm{swap}(F_1, 1 + \mathrm{len}\, f, 2 + \mathrm{len}\, f))) \cdot E_{33}$ for every elements S_4, R_3 of $\mathrm{Fin}\, \mathrm{dom}(\mathrm{App}(C_{15}))$ for every elements S_{14}, R_5 of $\mathrm{Fin}\, \mathrm{dom}(\mathrm{App}(C_{20}))$ such that $S_5 = S_4$ and $R_4 = R_3$ and $S_{15} = S_{14}$ and $R_6 = R_5$ holds $A(A\text{-}\sum_{S_4}(M \odot \mathrm{App}(C_{15})), A\text{-}\sum_{S_{14}}(M \odot \mathrm{App}(C_{20}))) = A(A\text{-}\sum_{R_3}(M \odot \mathrm{App}(C_{15})), A\text{-}\sum_{R_5}(M \odot \mathrm{App}(C_{20})))$. Set $C_{15} = (\mathrm{SignGenOp}((f \frown \langle I(d_1) \rangle) \frown \langle d_2 \rangle, A, \mathrm{swap}(F_1, L_1, L_2))) \cdot E_{33}$. For every x such that $x \in \mathrm{dom}\, C_{15}$ holds $C_{15}(x)$ is not empty. □

Let us consider an enumeration E of F, an enumeration E_{17} of $\mathrm{ext}(F, 1+m, 2+m)$, an enumeration E_{33} of $\mathrm{swap}(F, 1+m, 2+m)$, an enumeration E_{21} of $\mathrm{ext}(F, 1+m, 2+m) \cup \mathrm{swap}(F, 1+m, 2+m)$, and finite sequences s_1, s_2. Now we state the propositions:

(138) Suppose A is commutative, associative, and unital and has inverse ope-

ration and M is associative, commutative, and unital and M is distributive w.r.t. A. Then suppose $\bigcup F \subseteq \mathrm{Seg}(1+m)$. Then suppose $E_{17} = \mathrm{Ext}(E, 1+m, 2+m)$ and $E_{33} = \mathrm{Swap}(E, 1+m, 2+m)$. Then suppose $E_{21} = E_{17} \frown E_{33}$. Then suppose s_1, $s_2 \in \mathrm{doms}(m+1, \overline{\overline{F}})$ and s_1 has evenly repeated values and s_2 has evenly repeated values and $\overline{\overline{{s_1}^{-1}(\{1+m\})}} < \overline{\overline{{s_2}^{-1}(\{1+m\})}}$. Then there exist subsets D_1, D_2 of $\mathrm{doms}(m+2, \overline{\overline{F}} + \overline{\overline{F}})$ such that

(i) D_1 is with evenly repeated values-member, and

(ii) D_2 is with evenly repeated values-member, and

(iii) for every finite sequences C_4, C_7 of elements of D^* and for every f, d_1, and d_2 such that $\mathrm{len}\, f = m$ and $C_4 = (\mathrm{SignGenOp}(f \frown \langle A(d_1, d_2)\rangle, A, F)) \cdot E$ and $C_7 = (\mathrm{SignGenOp}(f \frown \langle A((\text{the inverse operation w.r.t. } A)(d_1), d_2)\rangle, A, F)) \cdot E$ for every non-empty, non empty finite sequence C_{17} of elements of D^* such that $C_{17} = (\mathrm{SignGenOp}((f \frown \langle d_1\rangle) \frown \langle d_2\rangle, A, \mathrm{ext}(F, 1+\mathrm{len}\, f, 2+\mathrm{len}\, f) \cup \mathrm{swap}(F, 1+\mathrm{len}\, f, 2+\mathrm{len}\, f))) \cdot E_{21}$ for every elements S_1, S_2 of $\mathrm{Fin}\, \mathrm{dom}(\mathrm{App}(C_{17}))$ such that $S_1 = D_1$ and $S_2 = D_2$ holds S_1 misses S_2 and $A(M((M \odot \mathrm{App}(C_4))(s_1), (M \odot \mathrm{App}(C_7))(s_2)), M((M \odot \mathrm{App}(C_4))(s_2), (M \odot \mathrm{App}(C_7))(s_1))) = A\text{-}\sum_{S_1 \cup S_2}(M \odot \mathrm{App}(C_{17}))$ and for every finite sequence h and for every i such that $h \in S_1$ and $i \in \mathrm{dom}(s_1 \frown s_2)$ holds if $(s_1 \frown s_2)(i) = 1+\mathrm{len}\, f$, then $h(i) \in \{1+\mathrm{len}\, f, 2+\mathrm{len}\, f\}$ and if $(s_1 \frown s_2)(i) \neq 1+\mathrm{len}\, f$, then $h(i) = (s_1 \frown s_2)(i)$ and for every finite sequence h and for every i such that $h \in S_2$ and $i \in \mathrm{dom}(s_2 \frown s_1)$ holds if $(s_2 \frown s_1)(i) = 1+\mathrm{len}\, f$, then $h(i) \in \{1+\mathrm{len}\, f, 2+\mathrm{len}\, f\}$ and if $(s_2 \frown s_1)(i) \neq 1+\mathrm{len}\, f$, then $h(i) = (s_2 \frown s_1)(i)$.

(139) Suppose A is commutative, associative, and unital and has inverse operation and M is associative, commutative, and unital and M is distributive w.r.t. A. Then suppose $\bigcup F \subseteq \mathrm{Seg}(1+m)$. Then suppose $E_{17} = \mathrm{Ext}(E, 1+m, 2+m)$ and $E_{33} = \mathrm{Swap}(E, 1+m, 2+m)$. Then suppose $E_{21} = E_{17} \frown E_{33}$. Then suppose s_1, $s_2 \in \mathrm{doms}(m+1, \overline{\overline{F}})$ and s_1 has evenly repeated values and s_2 has evenly repeated values and $s_1 \neq s_2$. Then there exist subsets D_1, D_2 of $\mathrm{doms}(m+2, \overline{\overline{F}} + \overline{\overline{F}})$ such that

(i) D_1 is with evenly repeated values-member, and

(ii) D_2 is with evenly repeated values-member, and

(iii) for every finite sequences C_4, C_7 of elements of D^* and for every f, d_1, and d_2 such that $\mathrm{len}\, f = m$ and $C_4 = (\mathrm{SignGenOp}(f \frown \langle A(d_1, d_2)\rangle, A, F)) \cdot E$ and $C_7 = (\mathrm{SignGenOp}(f \frown \langle A((\text{the inverse operation w.r.t. } A)(d_1), d_2)\rangle, A, F)) \cdot E$ for every non-empty, non empty finite sequence C_{17} of elements of D^* such that $C_{17} = (\mathrm{SignGenOp}((f^\frown \langle d_1\rangle)^\frown\langle d_2\rangle, A, \mathrm{ext}(F, 1+\mathrm{len}\, f, 2+\mathrm{len}\, f)\cup\mathrm{swap}(F, 1+\mathrm{len}\, f, 2+\mathrm{len}\, f)))\cdot E_{21}$ for every elements S_1, S_2 of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_{17}))$ such that $S_1 = D_1$ and $S_2 = D_2$ holds S_1 misses S_2 and $A(M((M\odot\mathrm{App}(C_4))(s_1), (M\odot \mathrm{App}(C_7))(s_2)), M((M \odot \mathrm{App}(C_4))(s_2), (M \odot \mathrm{App}(C_7))(s_1))) = A\text{-}\sum_{S_1\cup S_2}(M \odot \mathrm{App}(C_{17}))$ and for every finite sequence h and for every i such that $h \in S_1$ and $i \in \mathrm{dom}(s_1 {}^\frown s_2)$ holds if $(s_1 {}^\frown s_2)(i) = 1+\mathrm{len}\, f$, then $h(i) \in \{1+\mathrm{len}\, f, 2+\mathrm{len}\, f\}$ and if $(s_1{}^\frown s_2)(i) \neq 1+\mathrm{len}\, f$, then $h(i) = (s_1{}^\frown s_2)(i)$ and for every finite sequence h and for every i such that $h \in S_2$ and $i \in \mathrm{dom}(s_2{}^\frown s_1)$ holds if $(s_2{}^\frown s_1)(i) = 1+\mathrm{len}\, f$, then $h(i) \in \{1 + \mathrm{len}\, f, 2 + \mathrm{len}\, f\}$ and if $(s_2 {}^\frown s_1)(i) \neq 1 + \mathrm{len}\, f$, then $h(i) = (s_2 {}^\frown s_1)(i)$.

The theorem is a consequence of (126), (40), (106), (47), (80), and (138).

(140) Suppose M is commutative and associative and $\mathrm{len}\, f = 2$. Then $\mathrm{SignGenOp}(f, M, A, \{2\}) = M(A(f(1), f(2)), A(f(1), (\text{the inverse operation w.r.t. } A)(f(2))))$. The theorem is a consequence of (71), (70), and (73).

Let us consider an enumeration E of $2^{\{2\}}$ and a non-empty, non empty finite sequence C_3 of elements of D^*. Now we state the propositions:

(141) Suppose M is commutative and associative and A is commutative, associative, and unital and has inverse operation and M is distributive w.r.t. A. Then suppose $C_3 = (\mathrm{SignGenOp}(f, A, 2^{\{2\}})) \cdot E$ and $\mathrm{len}\, f = 2$. Then there exists an element S of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_3))$ such that

(i) $S = \{\langle 1, 1\rangle, \langle 2, 2\rangle\}$, and

(ii) $\mathrm{SignGenOp}(f, M, A, \{2\}) = A\text{-}\sum_S(M \odot \mathrm{App}(C_3))$.

Proof: Set I = the inverse operation w.r.t. A. Reconsider $f_1 = f(1)$, $f_2 = f(2)$ as an element of D. $\{\langle 1, 1\rangle, \langle 2, 2\rangle\} \subseteq \mathrm{dom}_\kappa\, C_3(\kappa)$.
$\mathrm{SignGenOp}(f, M, A, \{2\}) = A(M(f_1, f_1), M(f_2, I(f_2)))$. □

(142) Suppose M is commutative and associative and A is commutative, associative, and unital and has inverse operation and M is distributive w.r.t. A. Then suppose $C_3 = (\mathrm{SignGenOp}(f, A, 2^{\{2\}})) \cdot E$ and $\mathrm{len}\, f = 2$. Then there exists an element S of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_3))$ such that

(i) S is with evenly repeated values-member, and

(ii) $\mathrm{SignGenOp}(f, M, A, \{2\}) = A\text{-}\sum_S(M \odot \mathrm{App}(C_3))$.

The theorem is a consequence of (141).

(143) Main Theorem:
Suppose A is commutative, associative, and unital and has inverse operation and M is associative, commutative, and unital and M is distributive w.r.t. A and $m > 1$ and for every d, $M(\mathbf{1}_A, d) = \mathbf{1}_A$.

Then there exists an enumeration E of $2^{(\mathrm{Seg}\, m)\setminus\{1\}}$ and there exists a subset S of $\mathrm{doms}(m, \overline{\overline{2^{(\mathrm{Seg}\, m)\setminus\{1\}}}})$ such that S is with evenly repeated values-member and $\overline{\overline{2^{(\mathrm{Seg}\, m)\setminus\{1\}}}} \mapsto 1 \in S$ and for every non-empty, non empty finite sequence C_3 of elements of D^* and for every f such that $C_3 = (\mathrm{SignGenOp}(f, A, 2^{(\mathrm{Seg}\, m)\setminus\{1\}})) \cdot E$ and $\mathrm{len}\, f = m$ for every element S_6 of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_3))$ such that $S_6 = S$ holds $\mathrm{SignGenOp}(f, M, A, (\mathrm{Seg}\, m) \setminus \{1\}) = A\text{-}\sum_{S_6}(M \odot \mathrm{App}(C_3))$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ there exists an enumeration E of $2^{(\mathrm{Seg}\,\$_1)\setminus\{1\}}$ and there exists a subset S of $\mathrm{doms}(\$_1, \overline{\overline{2^{(\mathrm{Seg}\,\$_1)\setminus\{1\}}}})$ such that S is with evenly repeated values-member and $\overline{\overline{2^{(\mathrm{Seg}\,\$_1)\setminus\{1\}}}} \mapsto 1 \in S$ and for every non-empty, non empty finite sequence C_3 of elements of D^* and for every f such that $C_3 = (\mathrm{SignGenOp}(f, A, 2^{(\mathrm{Seg}\,\$_1)\setminus\{1\}})) \cdot E$ and $\mathrm{len}\, f = \$_1$ for every element S_6 of $\mathrm{Fin}\,\mathrm{dom}(\mathrm{App}(C_3))$ such that $S_6 = S$ holds $\mathrm{SignGenOp}(f, M, A, (\mathrm{Seg}\,\$_1) \setminus \{1\}) = A\text{-}\sum_{S_6}(M \odot \mathrm{App}(C_3))$.

$\mathcal{P}[2]$. For every natural number j such that $2 \leqslant j$ holds if $\mathcal{P}[j]$, then $\mathcal{P}[j+1]$. For every natural number i such that $2 \leqslant i$ holds $\mathcal{P}[i]$. □

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] Marco B. Caminati. Preliminaries to classical first order model theory. *Formalized Mathematics*, 19(**3**):155–167, 2011. doi:10.2478/v10037-011-0025-2.

[4] Taneli Huuskonen. Polish notation. *Formalized Mathematics*, 23(**3**):161–176, 2015. doi:10.1515/forma-2015-0014.

[5] Yuri Matiyasevich and Julia Robinson. Reduction of an arbitrary diophantine equation to one in 13 unknowns. *Acta Arithmetica*, 27:521–553, 1975.

[6] Karol Pąk. Stirling numbers of the second kind. *Formalized Mathematics*, 13(**2**):337–345, 2005.

[7] 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.

Accepted September 30, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 3, Pages 199–207, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0014

sciendo.com/journal/forma

Artin's Theorem Towards the Existence of Algebraic Closures

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. This is the first part of a two-part article formalizing existence and uniqueness of algebraic closures using the Mizar system [1], [2]. Our proof follows Artin's classical one as presented by Lang in [3]. In this first part we prove 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 need 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 the 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_11`, version: `8.1.12 5.71.1431`

Let us consider ordinal numbers n, m and bags b_1, b_2 of n. Now we state the propositions:

(1) If $\operatorname{support} b_1 = \{m\}$ and $\operatorname{support} b_2 = \{m\}$, then $b_1 \leqslant b_2$ iff $b_1(m) \leqslant b_2(m)$.

(2) If $\operatorname{support} b_1 = \{m\}$, then $b_2 \mid b_1$ iff $b_2 = \operatorname{EmptyBag} n$ or $\operatorname{support} b_2 = \{m\}$ and $b_2(m) \leqslant b_1(m)$. The theorem is a consequence of (1).

(3) Let us consider a field F, ordinal numbers m, n, and a bag b of n. Suppose $\operatorname{support} b = \{m\}$. Then

(i) $\operatorname{len} \operatorname{divisors} b = b(m) + 1$, and

(ii) for every natural number k and for every finite subset S of n such that $S = \{m\}$ and $k \in \operatorname{dom}(\operatorname{divisors} b)$ holds $(\operatorname{divisors} b)(k) = (S, k -' 1)$-bag.

The theorem is a consequence of (1) and (2).

Let n be an ordinal number and L be a right zeroed, add-associative, right complementable, right unital, distributive, non degenerated double loop structure. Let us note that $\operatorname{PolyRing}(n, L)$ is non degenerated.

Now we state the proposition:

(4) Let us consider a non degenerated commutative ring R, a commutative ring extension S of R, and an ordinal number n. Then $\operatorname{PolyRing}(n, S)$ is a commutative ring extension of $\operatorname{PolyRing}(n, R)$.

Proof: Every polynomial of n,R is a polynomial of n,S. The carrier of $\operatorname{PolyRing}(n, R) \subseteq$ the carrier of $\operatorname{PolyRing}(n, S)$. For every polynomials p, q of n,R and for every polynomials p_1, q_1 of n,S such that $p = p_1$ and $q = q_1$ holds $p + q = p_1 + q_1$. The addition of $\operatorname{PolyRing}(n, R) =$ (the addition of $\operatorname{PolyRing}(n, S)$) $\restriction$ (the carrier of $\operatorname{PolyRing}(n, R)$). For every polynomials p, q of n,R and for every polynomials p_1, q_1 of n,S such that $p = p_1$ and $q = q_1$ holds $p * q = p_1 * q_1$. The multiplication of $\operatorname{PolyRing}(n, R) =$ (the multiplication of $\operatorname{PolyRing}(n, S)$) $\restriction$ (the carrier of $\operatorname{PolyRing}(n, R)$). □

Let R be a non degenerated ring, n be an ordinal number, and p be a polynomial of n,R. The functor Leading-Term(p) yielding a bag of n is defined by the term

$$\text{(Def. 1)} \quad \begin{cases} (\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p))(\operatorname{len} \operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p)), \\ \quad \textbf{if } p \neq 0_n R, \\ \operatorname{EmptyBag} n, \textbf{ otherwise}. \end{cases}$$

The leading coefficient of p yielding an element of R is defined by the term

$$\text{(Def. 2)} \quad p(\text{Leading-Term}(p)).$$

The functor Leading-Monomial p yielding a monomial of n,R is defined by the term

(Def. 3) Monom(the leading coefficient of p, Leading-Term(p)).

We introduce the notation LC p as a synonym of the leading coefficient of p and LT p as a synonym of Leading-Term(p) and LM(p) as a synonym of Leading-Monomial p.

Let us consider a non degenerated ring R, an ordinal number n, and a polynomial p of n,R. Now we state the propositions:

(5) $p = 0_n R$ if and only if Support $p = \emptyset$.

(6) LC $p = 0_R$ if and only if $p = 0_n R$. The theorem is a consequence of (5).

(7) Let us consider a non degenerated ring R, an ordinal number n, a polynomial p of n,R, and a bag b of n. Suppose $b \in$ Support p. Then $b =$ LT p if and only if for every bag b_1 of n such that $b_1 \in$ Support p holds $b_1 \leqslant b$. The theorem is a consequence of (5).

(8) Let us consider a non degenerated ring R, an ordinal number n, and a polynomial p of n,R. Then Support LM(p) $\subseteq$ Support p.

(9) Let us consider a field F, an ordinal number n, and a monomial p of n,F. Then

(i) LC $p =$ coefficient p, and

(ii) LT $p =$ term p.

The theorem is a consequence of (5).

Let us consider a non degenerated ring R, an ordinal number n, and a polynomial p of n,R. Now we state the propositions:

(10) (i) Support LM(p) $= \emptyset$, or

(ii) Support LM(p) $= \{$LT $p\}$.

The theorem is a consequence of (5), (8), and (6).

(11) LM(p) $= 0_n R$ if and only if $p = 0_n R$. The theorem is a consequence of (5), (8), and (6).

(12) (i) (LM(p))(LT p) $=$ LC p, and

(ii) for every bag b of n such that $b \neq$ LT p holds (LM(p))(b) $= 0_R$.

(13) (i) LT LM(p) $=$ LT p, and

(ii) LC LM(p) $=$ LC p.

Let us consider an ordinal number n, a non degenerated ring R, and elements a, b of R. Now we state the propositions:

(14) $(a\restriction(n,R)) + (b\restriction(n,R)) = a + b\restriction(n,R)$.

(15) $(a\restriction(n,R)) * (b\restriction(n,R)) = a \cdot b\restriction(n,R)$.

Let R, S be non degenerated commutative rings, n be an ordinal number, p be a polynomial of n,R, and x be a function from n into S. The functor $\mathrm{ExtEval}(p, x)$ yielding an element of S is defined by

(Def. 4) there exists a finite sequence y of elements of S such that $it = \sum y$ and $\mathrm{len}\, y = \mathrm{len}\,\mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p)$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y$ holds $y(i) = (p \cdot (\mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p)))(i)(\in S) \cdot (\mathrm{eval}((\mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p))_{/i}, x))$.

Let us consider non degenerated commutative rings R, S, an ordinal number n, and a function x from n into S. Now we state the propositions:

(16) $\mathrm{ExtEval}(0_n R, x) = 0_S$. The theorem is a consequence of (5).

(17) If R is a subring of S, then $\mathrm{ExtEval}(1\_(n, R), x) = 1_S$.

(18) Let us consider non degenerated commutative rings R, S, an ordinal number n, a polynomial p of n,R, and a bag b of n. Suppose $\mathrm{Support}\, p = \{b\}$. Let us consider a function x from n into S. Then $\mathrm{ExtEval}(p, x) = p(b)(\in S) \cdot (\mathrm{eval}(b, x))$.

PROOF: Reconsider $s_2 = \mathrm{Support}\, p$ as a finite subset of $\mathrm{Bags}\, n$. Set $s_1 = \mathrm{SgmX}(\mathrm{BagOrder}\, n, s_2)$. For every object u such that $u \in \mathrm{dom}\, s_1$ holds $u \in \{1\}$. Consider y being a finite sequence of elements of the carrier of S such that $\mathrm{ExtEval}(p, x) = \sum y$ and $\mathrm{len}\, y = \mathrm{len}\,\mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p)$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y$ holds $y(i) = (p \cdot (\mathrm{SgmX}(\mathrm{BagOrder}\, n, s_2)))(i)(\in S) \cdot (\mathrm{eval}((\mathrm{SgmX}(\mathrm{BagOrder}\, n, s_2))_{/i}, x))$. □

Let us consider non degenerated commutative rings R, S, an ordinal number n, polynomials p, q of n,R, and a function x from n into S. Now we state the propositions:

(19) If R is a subring of S, then $\mathrm{ExtEval}(p + q, x) = \mathrm{ExtEval}(p, x) + \mathrm{ExtEval}(q, x)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every polynomial p of n,R such that $\overline{\overline{\mathrm{Support}\, p}} = \$_1$ holds $\mathrm{ExtEval}(p+q, x) = \mathrm{ExtEval}(p, x) + \mathrm{ExtEval}(q, x)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k + 1]$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. □

(20) If R is a subring of S, then $\mathrm{ExtEval}(p * q, x) = (\mathrm{ExtEval}(p, x)) \cdot (\mathrm{ExtEval}(q, x))$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every polynomial p of n,R such that $\overline{\overline{\mathrm{Support}\, p}} = \$_1$ holds $\mathrm{ExtEval}(p * q, x) = (\mathrm{ExtEval}(p, x)) \cdot (\mathrm{ExtEval}(q, x))$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k + 1]$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. □

Let F be a field. The functor $\mathrm{nCP}(F)$ yielding a non empty subset of the carrier of $\mathrm{PolyRing}(F)$ is defined by the term

(Def. 5) the set of all p where p is a non constant element of the carrier of $\mathrm{PolyRing}(F)$.

One can verify that $\overline{\overline{\mathrm{nCP}(F)}}$ is non empty and there exists a function from $\mathrm{nCP}(F)$ into $\overline{\overline{\mathrm{nCP}(F)}}$ which is bijective.

Let g be a function from $\mathrm{nCP}(F)$ into $\overline{\overline{\mathrm{nCP}(F)}}$ and p be a non constant element of the carrier of $\mathrm{PolyRing}(F)$. Observe that the functor $g(p)$ yields an ordinal number. Let m be an ordinal number and p be a polynomial over F. The functor $\mathrm{Poly}(m,p)$ yielding a polynomial of $\overline{\overline{\mathrm{nCP}(F)}}$,$F$ is defined by

(Def. 6) $it(\mathrm{EmptyBag}\,\overline{\overline{\mathrm{nCP}(F)}}) = p(0)$ and for every bag b of $\overline{\overline{\mathrm{nCP}(F)}}$ such that $\mathrm{support}\,b = \{m\}$ holds $it(b) = p(b(m))$ and for every bag b of $\overline{\overline{\mathrm{nCP}(F)}}$ such that $\mathrm{support}\,b \neq \emptyset$ and $\mathrm{support}\,b \neq \{m\}$ holds $it(b) = 0_F$.

Let g be a bijective function from $\mathrm{nCP}(F)$ into $\overline{\overline{\mathrm{nCP}(F)}}$. The functor $\mathrm{nCP}(g, F)$ yielding a non empty subset of $\mathrm{PolyRing}(\overline{\overline{\mathrm{nCP}(F)}}, F)$ is defined by the term

(Def. 7) the set of all $\mathrm{Poly}(g(p),p)$ where p is a non constant element of the carrier of $\mathrm{PolyRing}(F)$.

Let m be an ordinal number and p be a polynomial over F. Observe that $\mathrm{Poly}(m, \mathrm{LM}(p))$ is monomial-like. Now we state the propositions:

(21) Let us consider a field F, and an ordinal number m. Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Let us consider a polynomial p over F. Then $\mathrm{Poly}(m,p) = 0_{\overline{\overline{\mathrm{nCP}(F)}}}F$ if and only if $p = \mathbf{0}.F$. The theorem is a consequence of (5).

(22) Let us consider a field F, and an ordinal number m. Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Let us consider a polynomial p over F, and an element a of F. Then $\mathrm{Poly}(m,p) = a\restriction(\overline{\overline{\mathrm{nCP}(F)}}, F)$ if and only if $p = a\restriction F$.

(23) Let us consider a field F, and an ordinal number m. Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Let us consider a non zero element p of the carrier of $\mathrm{PolyRing}(F)$. Then $\mathrm{Support}\,\mathrm{Poly}(m,p) = \{\mathrm{EmptyBag}\,\overline{\overline{\mathrm{nCP}(F)}}\}$ if and only if p is constant. The theorem is a consequence of (22) and (21).

(24) Let us consider a field F, and ordinal numbers m_1, m_2. Suppose m_1, $m_2 \in \overline{\overline{\mathrm{nCP}(F)}}$. Let us consider non constant polynomials p_1, p_2 over F. Suppose $\mathrm{Poly}(m_1,p_1) = \mathrm{Poly}(m_2,p_2)$. Then

(i) $m_1 = m_2$, and

(ii) $p_1 = p_2$.

The theorem is a consequence of (21), (23), and (5).

(25) Let us consider a field F, and an ordinal number m. Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Let us consider a constant polynomial p over F. Then

(i) $\mathrm{LT}\,\mathrm{Poly}(m,p) = \mathrm{EmptyBag}\,\overline{\overline{\mathrm{nCP}(F)}}$, and

(ii) $\mathrm{LC}\,\mathrm{Poly}(m,p) = p(0)$.

The theorem is a consequence of (22).

(26) Let us consider a field F, and an ordinal number m. Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Let us consider a non constant polynomial p over F. Then

(i) $(\mathrm{LT}\,\mathrm{Poly}(m,p))(m) = \deg(p)$, and

(ii) for every ordinal number o such that $o \neq m$ holds $(\mathrm{LT}\,\mathrm{Poly}(m,p))(o) = 0$.

Proof: Set $n = \overline{\overline{\mathrm{nCP}(F)}}$. Set $q = \mathrm{Poly}(m,p)$. Reconsider $S = \{m\}$ as a finite subset of n. Reconsider $d = \deg(p)$ as a non zero element of $\mathbb{N}$. Set $b = (S,d)$-bag. $b \in \mathrm{Support}\,q$. For every bag b_1 of n such that $b_1 \in \mathrm{Support}\,q$ holds $b_1 \leqslant b$ by [4, (7),(6)]. $b = \mathrm{LT}\,q$. □

Let us consider a field F, an ordinal number m, and a polynomial p over F. Now we state the propositions:

(27) Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Then

(i) $\mathrm{LC}\,\mathrm{Poly}(m,\mathrm{LM}(p)) = \mathrm{LC}\,\mathrm{Poly}(m,p)$, and

(ii) $\mathrm{LT}\,\mathrm{Poly}(m,\mathrm{LM}(p)) = \mathrm{LT}\,\mathrm{Poly}(m,p)$.

The theorem is a consequence of (25) and (26).

(28) Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Then $\mathrm{Poly}(m,\mathrm{LM}(p)) = \mathrm{Monom}(\mathrm{LC}\,\mathrm{Poly}(m,p), \mathrm{LT}\,\mathrm{Poly}(m,p))$. The theorem is a consequence of (9) and (27).

(29) If $m \in \overline{\overline{\mathrm{nCP}(F)}}$, then $\mathrm{LM}(\mathrm{Poly}(m,p)) = \mathrm{Poly}(m,\mathrm{LM}(p))$.

(30) Let us consider a field F, an ordinal number m, and polynomials p, q over F. Then $\mathrm{Poly}(m,p+q) = \mathrm{Poly}(m,p) + \mathrm{Poly}(m,q)$.

(31) Let us consider a field F, an ordinal number m, and a polynomial p over F. Then $\mathrm{Poly}(m,-p) = -\mathrm{Poly}(m,p)$.

(32) Let us consider a field F, a non zero element a of F, a natural number i, and an ordinal number m. Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Then $\mathrm{Poly}(m,\mathrm{anpoly}(a, 0)) * \mathrm{Poly}(m,\mathrm{anpoly}(1_F,i)) = \mathrm{Poly}(m,\mathrm{anpoly}(a,i))$. The theorem is a consequence of (22).

(33) Let us consider a field F, an element i of $\mathbb{N}$, and an ordinal number m. Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Then $\mathrm{Poly}(m,\mathrm{anpoly}(1_F,1)) * \mathrm{Poly}(m,\mathrm{anpoly}(1_F, i)) = \mathrm{Poly}(m,\mathrm{anpoly}(1_F,i+1))$. The theorem is a consequence of (22) and (3).

(34) Let us consider a field F, a natural number i, and an ordinal number m. Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Then $\mathrm{power}_{\mathrm{PolyRing}(\overline{\overline{\mathrm{nCP}(F)}},F)}(\mathrm{Poly}(m,\mathrm{anpoly}(1_F,$

1)), i) = Poly(m, anpoly(1_F, i)).

PROOF: Set f = $\text{power}_{\text{PolyRing}(\overline{\overline{\text{nCP}(F)}},F)}$. Define $\mathcal{P}$[natural number] $\equiv$ f(Poly(m, anpoly(1_F, 1)), $\$_1$) = Poly($m$, anpoly($1_F$, $\$_1$)). $\mathcal{P}[0]$ by [5, (7)], (22). For every natural number k, $\mathcal{P}[k]$. □

(35) Let us consider a field F, a non constant element p of the carrier of PolyRing(F), and an ordinal number m. Suppose $m \in \overline{\overline{\text{nCP}(F)}}$. Then Poly($m$, anpoly(LC p, deg(p))) = LM(Poly(m, p)). The theorem is a consequence of (28).

(36) Let us consider a field F, and a finite subset P of the carrier of PolyRing (F). Then there exists an extension E of F such that for every non constant element p of the carrier of PolyRing(F) such that $p \in P$ holds p has a root in E.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every field F for every finite subset P of the carrier of PolyRing(F) such that $\overline{\overline{P}} = \$_1$ there exists an extension E of F such that for every non constant element p of the carrier of PolyRing(F) such that $p \in P$ holds p has a root in E. $\mathcal{P}[0]$ by [6, (6)]. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{P}} = n$. □

(37) Let us consider a field F, an extension E of F, and an ordinal number m. Suppose $m \in \overline{\overline{\text{nCP}(F)}}$. Let us consider a polynomial p over F, and a function x from $\overline{\overline{\text{nCP}(F)}}$ into E. Then ExtEval(Poly(m, p), x) = ExtEval(p, $x_{/m}$).

PROOF: Set q = Poly(m, p). Set $n = \overline{\overline{\text{nCP}(F)}}$. Define $\mathcal{P}$[natural number] $\equiv$ for every polynomial p over F for every function x from n into E such that $\overline{\overline{\text{Support}\,\text{Poly}(m,p)}} = \$_1$ holds ExtEval(Poly(m, p), x) = ExtEval(p, $x_{/m}$). For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{\text{Support}\,q}} = n$. □

(38) Let us consider a non degenerated commutative ring R, a non empty subset M of R, and an object o. Then $o \in M$–ideal if and only if there exists a non empty, finite subset P of R and there exists a linear combination L of P such that $P \subseteq M$ and $o = \sum L$.

Let F be a field and g be a bijective function from nCP(F) into $\overline{\overline{\text{nCP}(F)}}$. Let us observe that (nCP(g, F))–ideal is proper.

Let R be a non degenerated, commutative ring and I be a proper ideal of R.

A maximal ideal of I is an ideal of R defined by

(Def. 8) $I \subseteq$ *it* and *it* is maximal.

Observe that every maximal ideal of I is maximal.

Let F be a field, g be a bijective function from $\mathrm{nCP}(F)$ into $\overline{\overline{\mathrm{nCP}(F)}}$, and I be a maximal ideal of $(\mathrm{nCP}(g,F))$–ideal. The functor KroneckerField(F,g,I) yielding a field is defined by the term

(Def. 9) $\frac{\mathrm{PolyRing}(\overline{\overline{\mathrm{nCP}(F)}},F)}{I}$.

Let n be an ordinal number and R be a non degenerated ring. The functor $\pi_{n\to n/R}$ yielding a function from R into PolyRing(n,R) is defined by

(Def. 10) for every element a of R, $it(a) = a\restriction(n,R)$.

Let R be a non degenerated commutative ring. One can check that $\pi_{n\to n/R}$ is additive, multiplicative, and unity-preserving and $\pi_{n\to n/R}$ is monomorphic.

Let F be a field, g be a bijective function from $\mathrm{nCP}(F)$ into $\overline{\overline{\mathrm{nCP}(F)}}$, and I be a maximal ideal of $(\mathrm{nCP}(g,F))$–ideal. The functor emb(F,I,g) yielding a function from F into KroneckerField(F,g,I) is defined by the term

(Def. 11) (the canonical homomorphism of I into quotient field)$\cdot$
$(\pi_{\overline{\overline{\mathrm{nCP}(F)}}\to\overline{\overline{\mathrm{nCP}(F)}}/F})$.

Note that emb(F,I,g) is additive, multiplicative, and unity-preserving and emb(F,I,g) is monomorphic and KroneckerField(F,g,I) is F-monomorphic and F-homomorphic.

Let m be an ordinal number. The functor KrRoot(I,m) yielding an element of KroneckerField(F,g,I) is defined by the term

(Def. 12) $[\mathrm{Poly}(m,\langle 0_F,1_F\rangle)]_{\mathrm{EqRel}(\mathrm{PolyRing}(\overline{\overline{\mathrm{nCP}(F)}},F),I)}$.

Now we state the propositions:

(39) Let us consider a field F, a bijective function g from $\mathrm{nCP}(F)$ into $\overline{\overline{\mathrm{nCP}(F)}}$, a maximal ideal I of $(\mathrm{nCP}(g,F))$–ideal, and an element a of F. Then $(\mathrm{emb}(F,I,g))(a) = [a\restriction(\overline{\overline{\mathrm{nCP}(F)}},F)]_{\mathrm{EqRel}(\mathrm{PolyRing}(\overline{\overline{\mathrm{nCP}(F)}},F),I)}$.

(40) Let us consider a field F, a bijective function g from $\mathrm{nCP}(F)$ into $\overline{\overline{\mathrm{nCP}(F)}}$, a maximal ideal I of $(\mathrm{nCP}(g,F))$–ideal, an element p of the carrier of PolyRing(F), and an element n of $\mathbb{N}$. Then $(\mathrm{PolyHom}(\mathrm{emb}(F,I,g)))$ $(p)(n) = [p(n)\restriction(\overline{\overline{\mathrm{nCP}(F)}},F)]_{\mathrm{EqRel}(\mathrm{PolyRing}(\overline{\overline{\mathrm{nCP}(F)}},F),I)}$.
The theorem is a consequence of (39).

(41) Let us consider a field F, a bijective function g from $\mathrm{nCP}(F)$ into $\overline{\overline{\mathrm{nCP}(F)}}$, a maximal ideal I of $(\mathrm{nCP}(g,F))$–ideal, an element p of the carrier of PolyRing(F), and an ordinal number m. Suppose $m \in \overline{\overline{\mathrm{nCP}(F)}}$. Then $\mathrm{eval}((\mathrm{PolyHom}(\mathrm{emb}(F,I,g)))(p),\mathrm{KrRoot}(I,m)) =$
$[\mathrm{Poly}(m,p)]_{\mathrm{EqRel}(\mathrm{PolyRing}(\overline{\overline{\mathrm{nCP}(F)}},F),I)}$.

(42) Let us consider a field F, a bijective function g from $\mathrm{nCP}(F)$ into

$\overline{\overline{\mathrm{nCP}(F)}}$, a maximal ideal I of $(\mathrm{nCP}(g, F))$–ideal, and a non constant element p of the carrier of PolyRing(F). Then KrRoot$(I, g(p))$ is a root of $(\mathrm{PolyHom}(\mathrm{emb}(F, I, g)))(p)$. The theorem is a consequence of (41).

(43) Let us consider a field F. Then there exists an extension E_1 of F such that for every non constant element p of the carrier of PolyRing(F), p has a root in E_1. The theorem is a consequence of (42), (39), and (40).

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] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**): 49–58, 2004.

[5] Christoph Schwarzweller. On roots of polynomials over $F[X]/\langle p\rangle$. *Formalized Mathematics*, 27(**2**):93–100, 2019. doi:10.2478/forma-2019-0010.

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

Accepted September 30, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 3, Pages 209–210, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0015

sciendo
sciendo.com/journal/forma

The Divergence of the Sum of Prime Reciprocals[1]

Mario Carneiro
Carnegie Mellon University
Pittsburgh PA, USA

Summary. This is Erdős's proof of the divergence of the sum of prime reciprocals, using the Mizar system [2], [3], as reported in "Proofs from THE BOOK" [1].

MSC: 11N05 11A41 68V20

Keywords: primes; asymptotics

MML identifier: `PRIMRECI`, version: `8.1.12 5.71.1431`

From now on i, j, k, k_0, m, n, N denote natural numbers, x, y denote real numbers, and p denotes a prime number. Now we state the propositions:

(1) k is not zero if and only if $1 \leqslant k$.

(2) If $x^{\mathbf{2}} \leqslant y$, then $x \leqslant \sqrt{y}$.

(3) If $x^{\mathbf{2}} < y$, then $x < \sqrt{y}$.

(4) If $0 \leqslant x$ and $0 \leqslant y$ and $x \leqslant y^{\mathbf{2}}$, then $\sqrt{x} \leqslant y$.

(5) If $0 \leqslant x$ and $0 \leqslant y$ and $x < y^{\mathbf{2}}$, then $\sqrt{x} < y$.

Let x be a non negative real number. Let us note that the functor $\lfloor x \rfloor$ yields a natural number. In the sequel s denotes a sequence of real numbers. Now we state the propositions:

(6) If for every n, $0 \leqslant s(n)$, then $0 \leqslant ((\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa \in \mathbb{N}})(n)$.

(7) If s is summable and for every n, $0 \leqslant s(n)$, then $((\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa \in \mathbb{N}})(i) \leqslant \sum s$.

(8) If s is summable and for every n, $0 \leqslant s(n)$ and $i \leqslant j$, then $\sum(s \uparrow j) \leqslant \sum(s \uparrow i)$. The theorem is a consequence of (6).

[1] Work performed while visiting the Czech Institute for Informatics, Robotics and Cybernetics.

(9) If s is summable and for every n, $0 \leqslant s(n)$, then $\sum(s \uparrow i) \leqslant \sum s$. The theorem is a consequence of (8).

(10) If $p < n$, then $\overline{\overline{\mathbb{P}(p)}} + 1 \leqslant \overline{\overline{\mathbb{P}(n)}}$.

(11) $n \leqslant \mathrm{pr}(n)$.

(12) If $p < \mathrm{pr}(n+1)$, then $p \leqslant \mathrm{pr}(n)$. The theorem is a consequence of (10).

From now on N denotes a non zero natural number. Now we state the proposition:

(13) **Main Result** THE SUM OF THE RECIPROCALS OF THE PRIMES DIVERGES:

$\mathrm{inv}_{\mathbb{P}}$ is not summable.

PROOF: Define $\mathcal{P}$[non zero natural number, natural number, natural number] $\equiv \$_1 \leqslant \$_3$ and for every p such that $p \mid \$_1$ holds $p \leqslant \mathrm{pr}(\$_2)$. Define $\mathcal{M}$(natural number, natural number) $= \{n$, where n is a non zero natural number : $\mathcal{P}[n, \$_1, \$_2]\}$.

For every k and N, $\mathcal{M}(k, N)$ is finite and $\overline{\overline{\mathcal{M}(k, N)}} \subseteq 2^{\mathrm{pr}(k)} \cdot \lfloor \sqrt{N} \rfloor$ by (1), (2), [4, (47)]. For every k and N, $N \cdot ((\sum_{\alpha=0}^{\kappa} (\mathrm{inv}_{\mathbb{P}})(\alpha))_{\kappa \in \mathbb{N}})(k) + \overline{\overline{(\mathrm{Seg}\, N) \setminus \mathcal{M}(k, N)}} \leqslant N \cdot ((\sum_{\alpha=0}^{\kappa} (\mathrm{inv}_{\mathbb{P}})(\alpha))_{\kappa \in \mathbb{N}})(k+N)$. Consider k being an element of $\mathbb{N}$ such that $\sum(\mathrm{inv}_{\mathbb{P}} \uparrow k) < \frac{1}{2}$. Set $p = \mathrm{pr}(k)$. For every N, $\frac{N}{2} < 2^p \cdot \lfloor \sqrt{N} \rfloor$ by (8), (7), [5, (3)]. □

Observe that $\mathrm{inv}_{\mathbb{P}}$ is non summable as a sequence of real numbers.

REFERENCES

[1] Martin Aigner and Günter M. Ziegler. *Proofs from THE BOOK.* Springer-Verlag, Berlin Heidelberg New York, 2004.

[2] 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.

[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] Adam Grabowski. Sequences of prime reciprocals. Preliminaries. *Formalized Mathematics*, 26(**1**):69–79, 2018. doi:10.2478/forma-2018-0006.

[5] Christoph Schwarzweller. Renamings and a condition-free formalization of Kronecker's construction. *Formalized Mathematics*, 28(**2**):129–135, 2020. doi:10.2478/forma-2020-0012.

Accepted September 30, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 3, Pages 211–221, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0016

sciendo
sciendo.com/journal/forma

Ring of Endomorphisms and Modules over a Ring

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

Summary. We formalize in the Mizar system [3], [4] some basic properties on left module over a ring such as constructing a module via a ring of endomorphism of an abelian group and the set of all homomorphisms of modules form a module [1] along with Ch. 2 set. 1 of [2].

The formalized items are shown in the below list with notations: M_{ab} for an Abelian group with a suffix "$_{ab}$" and M without a suffix is used for left modules over a ring.

1. The endomorphism ring of an abelian group denoted by $\mathbf{End}(M_{ab})$.
2. A pair of an Abelian group M_{ab} and a ring homomorphism $R \xrightarrow{\rho} \mathbf{End}(M_{ab})$ determines a left R-module, formalized as a function $\mathbf{AbGrLMod}(M_{ab}, \rho)$ in the article.
3. The set of all functions from M to N form R-module and denoted by $\mathbf{Func\_Mod}_R(M, N)$.
4. The set R-module homomorphisms of M to N, denoted by $\mathbf{Hom}_R(M, N)$, forms R-module.
5. A formal proof of $\mathbf{Hom}_R(\bar{R}, M) \cong M$ is given, where the $\bar{R}$ denotes the regular representation of R, i.e. we regard R itself as a left R-module.
6. A formal proof of $\mathbf{AbGrLMod}(M'_{ab}, \rho') \cong M$ where M'_{ab} is an abelian group obtained by removing the scalar multiplication from M, and ρ' is obtained by currying the scalar multiplication of M.

The removal of the multiplication from M has been done by the forgettable functor defined as **AbGr** in the article.

MSC: 13C05 13C60 68V20

Keywords: module; endomorphism ring

MML identifier: LMOD_XX1, version: 8.1.12 5.71.1431

Let M, N be Abelian groups. The functor $\mathrm{ADD}(M,N)$ yielding a binary operation on (the carrier of $N)^{(\text{the carrier of } M)}$ is defined by

(Def. 1) for every elements f, g of (the carrier of $N)^{\alpha}$, $it(f,g) =$ (the addition of $N)^{\circ}(f, g)$, where α is the carrier of M.

Now we state the propositions:

(1) Let us consider Abelian groups M, N, and elements f, g, h of (the carrier of $N)^{\alpha}$. Then $h = (\mathrm{ADD}(M,N))(f,g)$ if and only if for every element x of the carrier of M, $h(x) = f(x) + g(x)$, where α is the carrier of M.

(2) Let us consider Abelian groups M, N, and homomorphisms f, g from M to N. Then $(\mathrm{ADD}(M,N))(f,g)$ is a homomorphism from M to N. The theorem is a consequence of (1).

Let M be an Abelian group. The functor $\mathrm{set\_End}(M)$ yielding a non empty subset of (the carrier of $M)^{(\text{the carrier of } M)}$ is defined by the term

(Def. 2) $\{f$, where f is a function from M into $M : f$ is an endomorphism of $M\}$.

The functor $\mathrm{add\_End}(M)$ yielding a binary operation on $\mathrm{set\_End}(M)$ is defined by the term

(Def. 3) $\mathrm{ADD}(M,M){\restriction}(\mathrm{set\_End}(M) \times \mathrm{set\_End}(M))$.

Now we state the proposition:

(3) Let us consider an Abelian group M, and endomorphisms f, g of M. Then

(i) f, $g \in$ (the carrier of $M)^{\alpha}$, and

(ii) $(\mathrm{add\_End}(M))(\langle f, g\rangle) = (\mathrm{ADD}(M,M))(f,g)$, and

(iii) $(\mathrm{ADD}(M,M))(f,g)$ is an endomorphism of M,

where α is the carrier of M. The theorem is a consequence of (2).

From now on M, N denote Abelian groups. Let M be an Abelian group and f, g be elements of (the carrier of $M)^{(\text{the carrier of } M)}$. Let us note that the functor $g \cdot f$ yields an element of (the carrier of $M)^{(\text{the carrier of } M)}$.

We prepare composition of homomorphisms.

Let M be an Abelian group. The functor $\mathrm{FuncComp}(M)$ yielding a binary operation on (the carrier of $M)^{(\text{the carrier of } M)}$ is defined by

(Def. 4) for every elements f, g of (the carrier of $M)^{\alpha}$, $it(f,g) = f \cdot g$, where α is the carrier of M.

(4) Let us consider Abelian groups M, N, and elements f, g of (the carrier of $N)^{\alpha}$. Then $(\mathrm{ADD}(M,N))(f,g) = (\mathrm{ADD}(M,N))(g,f)$, where α is the carrier of M. The theorem is a consequence of (1).

(5) Endomorphism of M is closed under Composition:
Let us consider an Abelian group M, and endomorphisms f, g of M. Then $(\mathrm{FuncComp}(M))(f,g)$ is an endomorphism of M.
Proof: Reconsider $F = (\mathrm{FuncComp}(M))(f,g)$ as an element of (the carrier of $M)^{(\text{the carrier of } M)}$. F is additive. □

Let M be an Abelian group. The functor mult_End(M) yielding a binary operation on set_End(M) is defined by the term

(Def. 5) $\mathrm{FuncComp}(M) \restriction (\mathrm{set\_End}(M) \times \mathrm{set\_End}(M))$.

Now we state the proposition:

(6) Let us consider an Abelian group M, and endomorphisms f, g of M. Then

(i) f, $g \in$ (the carrier of $M)^{\alpha}$, and

(ii) $(\mathrm{mult\_End}(M))(\langle f, g\rangle) = (\mathrm{FuncComp}(M))(f,g)$, and

(iii) $(\mathrm{FuncComp}(M))(f,g)$ is an endomorphism of M,

where α is the carrier of M. The theorem is a consequence of (5).

Let M be an Abelian group. The functors: 0_End(M) and 1_End(M) yielding elements of set_End(M) are defined by terms

(Def. 6) $\mathrm{ZeroMap}(M, M)$,

(Def. 7) id_M,

respectively. Let f be an element of set_End(M). The functor Inv f yielding an element of set_End(M) is defined by

(Def. 8) for every element x of M, $it(x) = f(-x)$.

Now we state the proposition:

(7) Let us consider an Abelian group M, and an element f of set_End(M). Then $(\mathrm{ADD}(M, M))(f, \mathrm{Inv}\, f) = \mathrm{ZeroMap}(M, M)$.
Proof: Consider f_1 being a function from the carrier of M into the carrier of M such that $f_1 = f$ and f_1 is an endomorphism of M. Consider g_1 being a function from the carrier of M into the carrier of M such that $g_1 = \mathrm{Inv}\, f$ and g_1 is an endomorphism of M. For every element x of the carrier of M, $(\mathrm{ADD}(M, M))(f_1, g_1)(x) = (\mathrm{ZeroMap}(M, M))(x)$. □

We define the Ring of Endomorphism of M as a structure.

Let M be an Abelian group. The functor End_Ring(M) yielding a strict, non empty double loop structure is defined by the term

(Def. 9) $\langle \mathrm{set\_End}(M), \mathrm{add\_End}(M), \mathrm{mult\_End}(M), 1\_\mathrm{End}(M), 0\_\mathrm{End}(M)\rangle$.

Now we state the proposition:

(8) The structure of End-Ring(M) turns to be a Ring:
Let us consider an Abelian group M. Then End_Ring(M) is a ring.

Let M be an Abelian group. One can verify that End_Ring(M) is Abelian, add-associative, right zeroed, right complementable, associative, well unital, and distributive and End_Ring(M) is strict.

In the sequel R denotes a ring and r denotes an element of R.

Let us consider R. Let M, N be left modules over R.

A homomorphism from M to N by R is a function from M into N defined by

(Def. 10) *it* is additive and homogeneous.

Now we state the proposition:

(9) Let us consider left modules M, N over R, and a homomorphism f from M to N by R. Suppose f is one-to-one and onto. Then f^{-1} is a homomorphism from N to M by R.
PROOF: Reconsider $g = f^{-1}$ as a function from N into M. For every elements a, b of the carrier of N, $g(a+b) = g(a)+g(b)$. For every element r of R and for every element a of the carrier of N, $g(r \cdot a) = r \cdot g(a)$. □

Let us consider R. Let M, N be left modules over R. We say that $M \cong N$ if and only if

(Def. 11) there exists a homomorphism f from M to N by R such that f is one-to-one and onto.

Let M be a left module over R.

An endomorphism of R and M is a homomorphism from M to M by R. Now we state the propositions:

(10) Let us consider a left module M over R. Then $M \cong M$.

(11) Let us consider left modules M, N over R. If $M \cong N$, then $N \cong M$.
The theorem is a consequence of (9).

Let us consider R. Let M, N be left modules over R. Observe that the predicate $M \cong N$ is reflexive and symmetric. Now we state the propositions:

(12) Let us consider left modules L, M, N over R. If $L \cong M$ and $M \cong N$, then $L \cong N$.
PROOF: Consider f being a homomorphism from L to M by R such that f is one-to-one and onto. Consider g being a homomorphism from M to N by R such that g is one-to-one and onto. Reconsider $G = g \cdot f$ as a function from L into N. For every elements x, y of L, $G(x+y) = G(x)+G(y)$. For every element x of L and for every element a of R, $G(a \cdot x) = a \cdot G(x)$. □

(13) Let us consider left modules M, N over R, and a homomorphism f from M to N by R. Then f is one-to-one if and only if $\ker f = \{0_M\}$.
PROOF: If f is one-to-one, then $\ker f = \{0_M\}$. For every objects x_1, x_2 such that $x_1, x_2 \in \operatorname{dom} f$ and $f(x_1) = f(x_2)$ holds $x_1 = x_2$. □

Let us consider R. Let M be an Abelian group and s be a function from R into End_Ring(M). The functor LModlmult(M, s) yielding a function from (the carrier of R) × (the carrier of M) into the carrier of M is defined by

(Def. 12) for every element x of the carrier of R and for every element y of the carrier of M, there exists an endomorphism h of M such that $h = s(x)$ and $it(x, y) = h(y)$.

The functor AbGrLMod(M, s) yielding a strict, non empty vector space structure over R is defined by the term

(Def. 13) $\langle$the carrier of M, the addition of M, 0_M, LModlmult$(M, s)\rangle$.

Now we state the proposition:

(14) Let us consider an Abelian group M, and a function s from R into End_Ring(M). Suppose s inherits ring homomorphism.
Then AbGrLMod(M, s) is a left module over R.
PROOF: AbGrLMod(M, s) is Abelian. AbGrLMod(M, s) is add-associative. AbGrLMod(M, s) is right zeroed. AbGrLMod(M, s) is right complementable. AbGrLMod(M, s) is scalar unital. □

The set of all functions from R-module M into R-module N form R-module.

In the sequel M, N denote left modules over R.

Let us consider R, M, and N. The functor 0_Funcs(M, N) yielding an element of (the carrier of N)$^{(\text{the carrier of } M)}$ is defined by the term

(Def. 14) ZeroMap(M, N).

The functor ADD(M, N) yielding a binary operation on (the carrier of N)$^{(\text{the carrier of } M)}$ is defined by

(Def. 15) for every elements f, g of (the carrier of $N)^{\alpha}$, $it(f, g) =$ (the addition of $N)^{\circ}(f, g)$, where α is the carrier of M.

From now on f, g, h denote elements of (the carrier of N)$^{(\text{the carrier of } M)}$.

Now we state the proposition:

(15) $h = (\text{ADD}(M, N))(f, g)$ if and only if for every element x of the carrier of M, $h(x) = f(x) + g(x)$.

Let us consider R, M, and N. Let F be a function from (the carrier of R) × (the carrier of N) into the carrier of N, a be an element of the carrier of R, and f be a function from M into N. Observe that the functor $F^{\circ}(a, f)$ yields an element of (the carrier of N)$^{(\text{the carrier of } M)}$. The functor LMULT($M, N$) yielding a function from (the carrier of R) × (the carrier of N)$^{(\text{the carrier of } M)}$ into (the carrier of N)$^{(\text{the carrier of } M)}$ is defined by

(Def. 16) for every element a of the carrier of R and for every element f of (the carrier of $N)^{\alpha}$ and for every element x of the carrier of M, $it(\langle a, f\rangle)(x) = a \cdot f(x)$, where α is the carrier of M.

The functor Func_Mod(R, M, N) yielding a non empty vector space structure over R is defined by the term

(Def. 17) $\langle(\text{the carrier of } N)^{\alpha}, \mathrm{ADD}(M, N), 0\_\mathrm{Funcs}(M, N), \mathrm{LMULT}(M, N)\rangle$, where α is the carrier of M.

Now we state the proposition:

(16) Let us consider an element a of the carrier of R, and elements f, h of (the carrier of $N)^{\alpha}$. Then $h = (\mathrm{LMULT}(M, N))(\langle a, f\rangle)$ if and only if for every element x of M, $h(x) = a \cdot f(x)$, where α is the carrier of M.

In the sequel a, b denote elements of the carrier of R.

Let us consider R, M, and N. Note that Func_Mod(R, M, N) is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital. Now we state the proposition:

(17) Func_Mod(R, M, N) is a left module over R.

From now on R denotes a commutative ring and M, M_1, N, N_1 denote left modules over R. Now we state the proposition:

(18) HOM(M, N) THE SET OF ALL R HOMOMORPHISMS FORM LEFT R-MODULE:
Let us consider homomorphisms f, g from M to N by R.
Then $(\mathrm{ADD}(M, N))(f, g)$ is a homomorphism from M to N by R. The theorem is a consequence of (15).

Let us consider R, M_1, M, and N. Let f be an element of (the carrier of $M)^{(\text{the carrier of } M_1)}$ and g be an element of (the carrier of $N)^{(\text{the carrier of } M)}$. Let us observe that the functor $g \cdot f$ yields an element of (the carrier of $N)^{(\text{the carrier of } M_1)}$. Now we state the propositions:

(19) Let us consider left modules M, N, M_1 over R, a homomorphism f from M to N by R, and a homomorphism u from M_1 to M by R. Then $f \cdot u$ is a homomorphism from M_1 to N by R.
PROOF: For every elements x_1, y_1 of the carrier of M_1 and for every element a of R, $(f \cdot u)(x_1 + y_1) = (f \cdot u)(x_1) + (f \cdot u)(y_1)$ and $a \cdot (f \cdot u)(x_1) = a \cdot (f \cdot u)(x_1)$. For every element x_1 of the carrier of M_1 and for every element a of R, $(f \cdot u)(a \cdot x_1) = a \cdot (f \cdot u)(x_1)$. □

(20) Let us consider an element a of the carrier of R, and a homomorphism g from M to N by R. Then $(\mathrm{LMULT}(M, N))(\langle a, g\rangle)$ is a homomorphism from M to N by R.

Let us consider R, M, and N. The functor set_Hom(M, N) yielding a non empty subset of (the carrier of $N)^{(\text{the carrier of } M)}$ is defined by the term

(Def. 18) $\{f$, where f is a function from M into N : f is a homomorphism from M to N by $R\}$.

The functor add_Hom(M, N) yielding a binary operation on set_Hom(M, N) is defined by the term

(Def. 19) ADD$(M, N) \restriction ($set_Hom$(M, N) \times$ set_Hom$(M, N))$.

Let F be a function from (the carrier of R)$\times$(the carrier of N) into the carrier of N, a be an element of the carrier of R, and f be a function from M into N. One can verify that the functor $F^{\circ}(a, f)$ yields an element of (the carrier of $N)^{(\text{the carrier of } M)}$. The functor lmult_Hom$(M, N)$ yielding a function from (the carrier of R) $\times$ set_Hom(M, N) into set_Hom(M, N) is defined by the term

(Def. 20) LMULT$(M, N) \restriction (($the carrier of $R) \times$ set_Hom$(M, N))$.

The functor 0_Hom(M, N) yielding an element of set_Hom(M, N) is defined by the term

(Def. 21) ZeroMap(M, N).

The functor Hom(R, M, N) yielding a non empty vector space structure over R is defined by the term

(Def. 22) $\langle$set_Hom(M, N), add_Hom(M, N), 0_Hom(M, N), lmult_Hom$(M, N)\rangle$.

Let us note that Hom(R, M, N) is non empty. Now we state the propositions:

(21) Let us consider homomorphisms f, g from M to N by R. Then

(i) f, $g \in$ (the carrier of $N)^{\alpha}$, and

(ii) (add_Hom$(M, N))(\langle f, g\rangle) = (ADD(M, N))(f, g)$, and

(iii) (ADD$(M, N))(f, g)$ is a homomorphism from M to N by R,

where α is the carrier of M. The theorem is a consequence of (18).

(22) Let us consider an element a of the carrier of R, and a homomorphism f from M to N by R. Then

(i) (lmult_Hom$(M, N))(\langle a, f\rangle) = ($LMULT$(M, N))(\langle a, f\rangle)$, and

(ii) (LMULT$(M, N))(\langle a, f\rangle)$ is a homomorphism from M to N by R.

The theorem is a consequence of (20).

(23) Let us consider elements f_1, g_1 of Func_Mod(R, M, N), and elements f, g of Hom(R, M, N). If $f_1 = f$ and $g_1 = g$, then $f + g = f_1 + g_1$. The theorem is a consequence of (21).

(24) Hom(R, M, N) is a left module over R. The theorem is a consequence of (23).

Let us consider R, M, and N. Note that Hom(R, M, N) is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

Let us consider M_1. Let u be a homomorphism from M_1 to M by R. The functor $\tau(N, u)$ yielding a function from Hom(R, M, N) into Hom(R, M_1, N) is defined by

(Def. 23) for every element f of $\mathrm{Hom}(R, M, N)$, there exists a homomorphism f_1 from M to N by R such that $f = f_1$ and $it(f) = f_1 \cdot u$.

Let us note that $\tau(N, u)$ is additive and homogeneous. Now we state the proposition:

(25) Let us consider a homomorphism u from M_1 to M by R. Then $\tau(N, u)$ is a homomorphism from $\mathrm{Hom}(R, M, N)$ to $\mathrm{Hom}(R, M_1, N)$ by R.

Let us consider R, M, N, and N_1. Let u be a homomorphism from N to N_1 by R. The functor $\phi(M, u)$ yielding a function from $\mathrm{Hom}(R, M, N)$ into $\mathrm{Hom}(R, M, N_1)$ is defined by

(Def. 24) for every element f of $\mathrm{Hom}(R, M, N)$, there exists a homomorphism f_1 from M to N by R such that $f = f_1$ and $it(f) = u \cdot f_1$.

Let us observe that $\phi(M, u)$ is additive and homogeneous. Now we state the propositions:

(26) Let us consider a homomorphism u from N to N_1 by R. Then $\phi(M, u)$ is a homomorphism from $\mathrm{Hom}(R, M, N)$ to $\mathrm{Hom}(R, M, N_1)$ by R.

(27) $\mathrm{Hom}(R, \mathrm{LeftMod}(R), M) \cong M$.

PROOF: Reconsider $R_1 = \mathrm{LeftMod}(R)$ as a left module over R. Reconsider $m_1 = 1_R$ as an element of R_1. Define $\mathcal{F}$(element of (the carrier of $M)^{(\text{the carrier of } R_1)}) = \$_1(m_1)$. Consider G being a function from (the carrier of $M)^{(\text{the carrier of } R_1)}$ into M such that For every element x of (the carrier of $M)^{\alpha}$, $G(x) = \mathcal{F}(x)$, where α is the carrier of R_1. For every elements f, g of (the carrier of $M)^{\alpha}$, $G((\mathrm{ADD}(R_1, M))(f, g)) = G(f) + G(g)$, where α is the carrier of R_1.

For every element f of (the carrier of $M)^{\alpha}$ and for every element a of R, $G((\mathrm{LMULT}(R_1, M))(\langle\!\langle a, f\rangle\!\rangle)) = a \cdot G(f)$, where α is the carrier of R_1. Set $c =$ the carrier of $\mathrm{Hom}(R, R_1, M)$. Set $G_1 = G{\restriction}c$. For every object y such that $y \in \mathrm{rng}\, G_1$ holds $y \in$ the carrier of M. For every elements f, g of $\mathrm{Hom}(R, R_1, M)$, $G_1(f + g) = G_1(f) + G_1(g)$. For every element f of $\mathrm{Hom}(R, R_1, M)$ and for every element a of R, $G_1(a \cdot f) = a \cdot G_1(f)$. $\ker G_1 = \{0_{\mathrm{Hom}(R, R_1, M)}\}$. For every object y such that $y \in$ the carrier of M holds $y \in \mathrm{rng}\, G_1$. □

Correspondence between Abelian Group (AbGr) and left R-module.

Let us consider R and M. The functor $\mathrm{AbGr}(M)$ yielding a non empty, strict Abelian group is defined by the term

(Def. 25) $\langle$the carrier of M, the addition of $M, 0_M\rangle$.

Let us consider N. Let f be a homomorphism from M to N by R. The functor $\mathrm{AbGr}(f)$ yielding a function from $\mathrm{AbGr}(M)$ into $\mathrm{AbGr}(N)$ is defined by

(Def. 26) for every object x such that $x \in$ the carrier of AbGr(M) holds $it(x) = f(x)$.

Now we state the proposition:

(28) Let us consider a homomorphism f from M to N by R. Then AbGr(f) is a homomorphism from AbGr(M) to AbGr(N).

Let us consider endomorphisms f, g, h of R and M. Now we state the propositions:

(29) AbGr(h) $=$ (FuncComp(AbGr(M)))(AbGr(f), AbGr(g)) if and only if for every element x of the carrier of AbGr(M), (AbGr(h))(x) $=$ ((AbGr(f))$\cdot$ (AbGr(g)))(x).

(30) If $h = f \cdot g$, then AbGr(h) $=$ (AbGr(f)) $\cdot$ (AbGr(g)).

Proof: For every element x of the carrier of AbGr(M), (AbGr(h))(x) $=$ ((AbGr(f)) $\cdot$ (AbGr(g)))(x). □

(31) AbGr(h) $=$ (ADD(AbGr(M), AbGr(M)))(AbGr(f), AbGr(g)) if and only if for every element x of the carrier of AbGr(M), (AbGr(h))(x) $=$ (AbGr(f))(x) $+$ (AbGr(g))(x).

Proof: If AbGr(h) $=$ (ADD(AbGr(M), AbGr(M)))(AbGr(f), AbGr(g)), then for every element x of the carrier of AbGr(M), (AbGr(h))(x) $=$ (AbGr(f))(x) $+$ (AbGr(g))(x). AbGr(h) $=$ (ADD(AbGr(M), AbGr(M))) (AbGr(f), AbGr(g)). □

(32) If $h = (\mathrm{ADD}(M, M))(f, g)$, then AbGr($h$) $=$ (ADD(AbGr(M), AbGr(M)))(AbGr(f), AbGr(g)). The theorem is a consequence of (15) and (31).

(33) Let us consider a ring R, a left module M over R, an element a of R, and an element m of M. Then (curry(the left multiplication of M))(a)(m) $=$ $a \cdot m$.

(34) Let us consider a commutative ring R, a left module M over R, and an element a of R. Then (curry(the left multiplication of M))(a) is an endomorphism of R and M.

Proof: Set $f =$ (curry(the left multiplication of M))(a). For every elements m_1, m_2 of M, $f(m_1 + m_2) = f(m_1) + f(m_2)$. For every element b of R and for every element m of M, $f(b \cdot m) = b \cdot f(m)$. □

(35) Let us consider endomorphisms f, g, h of R and M. Suppose $h = f \cdot g$. Then AbGr(h) $=$ (FuncComp(AbGr(M)))(AbGr(f), AbGr(g)). The theorem is a consequence of (30) and (29).

Let R be a commutative ring and M be a left module over R. The canonical homomorphism of M into quotient field yielding a function from R into End_Ring(AbGr(M)) is defined by

(Def. 27) for every object x such that $x \in$ the carrier of R there exists an endomorphism f of R and M such that $f =$ (curry(the left multiplication of M))(x) and $it(x) = \mathrm{AbGr}(f)$.

Observe that the canonical homomorphism of M into quotient field is additive. Now we state the proposition:

(36) Let us consider a commutative ring R, a left module M over R, and an element a of R. Then (the canonical homomorphism of M into quotient field)(a) is a homomorphism from $\mathrm{AbGr}(M)$ to $\mathrm{AbGr}(M)$.

Let R be a commutative ring and M be a left module over R. One can verify that the canonical homomorphism of M into quotient field is linear and AbGrLMod(AbGr(M), the canonical homomorphism of M into quotient field) is non empty, Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

Now we state the propositions:

(37) Let us consider a commutative ring R, and a left module M over R. Then LModlmult(AbGr(M), the canonical homomorphism of M into quotient field) = the left multiplication of M.

PROOF: Set $F =$ LModlmult(AbGr(M), the canonical homomorphism of M into quotient field). For every object z such that $z \in$ (the carrier of R) × (the carrier of M) holds $F(z) =$ (the left multiplication of M)(z). □

(38) Let us consider a commutative ring R, and a strict left module M over R. Then AbGrLMod(AbGr(M), the canonical homomorphism of M into quotient field) $= M$.

PROOF: AbGrLMod(AbGr(M), the canonical homomorphism of M into quotient field) is a submodule of M. □

Let R be a commutative ring and M be a left module over R. The functor $\rho(M)$ yielding a function from M into AbGrLMod(AbGr(M), the canonical homomorphism of M into quotient field) is defined by the term

(Def. 28) id_M.

Now we state the proposition:

(39) Let us consider a commutative ring R, and a left module M over R. Then $\rho(M)$ is additive and homogeneous.

PROOF: For every element x of the carrier of M and for every element a of R, $\rho(M)(a \cdot x) = a \cdot \rho(M)(x)$ by [5, (7)]. □

Let R be a commutative ring and M be a left module over R. Observe that $\rho(M)$ is additive and homogeneous.

Let us consider a commutative ring R and a left module M over R. Now we state the propositions:

(40) $\rho(M)$ is one-to-one and onto.

(41) $M \cong \mathrm{AbGrLMod}(\mathrm{AbGr}(M),$ the canonical homomorphism of M into quotient field). The theorem is a consequence of (40).

References

[1] Frank W. Anderson and Kent R. Fuller. *Rings and Categories of Modules, Second Edition*. Springer-Verlag, 1992.

[2] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to Commutative Algebra*, volume 2. Addison-Wesley Reading, 1969.

[3] 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.

[4] 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.

[5] Kazuhisa Nakasho, Yuichi Futa, and Yasunari Shidama. Continuity of bounded linear operators on normed linear spaces. *Formalized Mathematics*, 26(**3**):231–237, 2018. doi:10.2478/forma-2018-0021.

Accepted September 30, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 3, Pages 223–228, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0017

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part IV

Artur Korniłowicz
Institute of Computer Science
University of Białystok
Poland

Summary. In this paper problems 17, 18, 26, 27, 28, and 98 from [9] are formalized, using the Mizar formalism [8], [2], [3], [6].

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes

MML identifier: NUMBER04, version: 8.1.12 5.71.1431

1. Preliminaries

From now on X denotes a set, a, b, c, k, m, n denote natural numbers, i denotes an integer, r denotes a real number, and p denotes a prime number.

Let p be a prime number. One can verify that 1 mod p reduces to 1.

Let us consider n. One can verify that $\varepsilon_{\mathbb{N}}$ mod n reduces to $\varepsilon_{\mathbb{N}}$ and $\varepsilon_{\mathbb{Z}}$ mod n reduces to $\varepsilon_{\mathbb{Z}}$. Now we state the proposition:

(1) Let us consider a non empty, natural-membered set X. Suppose for every a such that $a \in X$ there exists b such that $b > a$ and $b \in X$. Then X is infinite.

Let us note that $\mathbb{N}_{\mathrm{even}}$ is infinite and $\mathbb{N}_{\mathrm{odd}}$ is infinite and every element of $\mathbb{N}_{\mathrm{even}}$ is even and every element of $\mathbb{N}_{\mathrm{odd}}$ is odd. Now we state the propositions:

(2) $n \bmod (k+1) = 0$ or ... or $n \bmod (k+1) = k$.

(3) Let us consider integers a, b, c. If $a \cdot b \mid c$, then $a \mid c$ and $b \mid c$.

(4) Let us consider integers a, b, m. If $a \equiv b \pmod{m}$, then $m \nmid a$ or $m \mid b$.

(5) If k is odd, then $(-1)^k \equiv -1 \pmod{n}$.

(6) Let us consider integers a, b. Suppose $k \neq 0$ and $a \equiv b \pmod{n^k}$. Then $a \equiv b \pmod{n}$.

(7) $2^{4 \cdot n} \equiv 1 \pmod{5}$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv 2^{4 \cdot \$_1} \equiv 1 \pmod{5}$. $\mathcal{P}[0]$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(8) $2^{12 \cdot n} \equiv 1 \pmod{13}$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv 2^{12 \cdot \$_1} \equiv 1 \pmod{13}$. $\mathcal{P}[0]$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(9) $\langle i \rangle \bmod n = \langle i \bmod n \rangle$.

(10) If $n \neq 0$, then for every integer-valued finite sequence f, $\sum f \equiv \sum (f \bmod n) \pmod{n}$.
Proof: Define $\mathcal{P}[\text{finite sequence of elements of } \mathbb{Z}] \equiv \sum \$_1 \equiv \sum (\$_1 \bmod n) \pmod{n}$. For every finite sequence p of elements of $\mathbb{Z}$ and for every element x of $\mathbb{Z}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle x \rangle]$. For every finite sequence p of elements of $\mathbb{Z}$, $\mathcal{P}[p]$. □

(11) If ($a \neq 0$ or $b \neq 0$) and $c \neq 0$ and a, b, c are mutually coprime, then $a \cdot b$ and c are relatively prime.

(12) If ($a \neq 0$ or $b \neq 0$) and $c \neq 0$ and a, b, c are mutually coprime and $a \mid n$ and $b \mid n$ and $c \mid n$, then $a \cdot b \cdot c \mid n$.

(13) If k is odd, then $a^n + 1 \mid a^{n \cdot k} + 1$.

(14) Let us consider an even natural number n. Suppose $n \mid 2^n + 2$. Then there exists a non zero, odd natural number k such that $2^n + 2 = n \cdot k$.

2. Main Problems

Now we state the propositions:

(15) Let us consider an even natural number n. Suppose $n \mid 2^n + 2$ and $n - 1 \mid 2^n + 1$. Let us consider a natural number n_1. If $n_1 = 2^n + 2$, then $n_1 - 1 \mid 2^{n_1} + 1$ and $n_1 \mid 2^{n_1} + 2$. The theorem is a consequence of (14) and (13).

(16) $\{n$, where n is a non zero, even natural number : $n \mid 2^n + 2$ and $n - 1 \mid 2^n + 1\}$ is infinite.
Proof: Set $X = \{n$, where n is a non zero, even natural number : $n \mid 2^n + 2$ and $n - 1 \mid 2^n + 1\}$. X is natural-membered. For every a such that $a \in X$ there exists b such that $b > a$ and $b \in X$. □

Let i be an integer. We say that i is double odd if and only if

(Def. 1) there exists an odd integer j such that $i = 2 \cdot j$.

Let i be a natural number. Let us observe that i is double odd if and only if the condition (Def. 2) is satisfied.

(Def. 2) there exists an odd natural number j such that $i = 2 \cdot j$.

Note that there exists an integer which is double odd and every integer which is double odd is also even. Let i be an odd integer. Observe that $i^2 + 1$ is double odd and $i^{\mathbf{2}} + 1$ is double odd.

Let r be a complex number and n be a natural number. The functor OddEvenPowers(r, n) yielding a complex-valued finite sequence is defined by

(Def. 3) len $it = n$ and for every natural number i such that $1 \leqslant i \leqslant n$ for every natural number m such that $m = n - i$ holds if i is odd, then $it(i) = r^m$ and if i is even, then $it(i) = -r^m$.

Let r be a real number. Let us observe that OddEvenPowers(r, n) is real-valued. Let r be an integer. Let us observe that OddEvenPowers(r, n) is $\mathbb{Z}$-valued. Let us consider a complex number r. Now we state the propositions:

(17) OddEvenPowers$(r, 1) = \langle 1 \rangle$.

(18) $\sum$ OddEvenPowers$(r, 1) = 1$. The theorem is a consequence of (17).

(19) OddEvenPowers$(r, 2 \cdot (k+1)+1) = \langle r^{2 \cdot k+2}, -r^{2 \cdot k+1} \rangle ^\frown$OddEvenPowers$(r, 2 \cdot k + 1)$.

PROOF: Set $n = 2 \cdot (k+1)+1$. Set $N = 2 \cdot k+1$. Set $f =$ OddEvenPowers(r, n). Set $p = \langle r^{2 \cdot k+2}, -r^{2 \cdot k+1} \rangle$. Set $q =$ OddEvenPowers(r, N). For every natural number x such that $x \in \operatorname{dom} p$ holds $f(x) = p(x)$. For every natural number x such that $x \in \operatorname{dom} q$ holds $f(\operatorname{len} p + x) = q(x)$. □

(20) $\sum$ OddEvenPowers$(r, 2 \cdot k+3) = r^{2 \cdot k+2} - r^{2 \cdot k+1} + \sum$ OddEvenPowers$(r, 2 \cdot k + 1)$. The theorem is a consequence of (19).

(21) $r^{2 \cdot n+1} + 1 = (r + 1) \cdot (\sum$ OddEvenPowers$(r, 2 \cdot n + 1))$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv r^{2 \cdot \$_1+1} + 1 = (r+1) \cdot (\sum$ OddEvenPowers$(r, 2 \cdot \$_1 + 1))$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k + 1]$. $\mathcal{P}[k]$. □

Let us consider an odd prime number p. Now we state the propositions:

(22) If $p^{k+1} \mid a^{p^k} + 1$, then $p^{k+2} \mid a^{p^{k+1}} + 1$.

PROOF: Set $b = a^{p^k}$. $b \equiv -1 \pmod{p}$. For every natural number L, $b^{2 \cdot L} \equiv 1 \pmod{p}$. For every natural number L, $b^{2 \cdot L+1} \equiv -1 \pmod{p}$ by [1, (34)]. Reconsider $F =$ OddEvenPowers(b, p) as a $\mathbb{Z}$-valued finite sequence. Reconsider $M = F \bmod p$ as a $\mathbb{Z}$-valued finite sequence. For every natural number x such that $1 \leqslant x \leqslant \operatorname{len} F$ holds $M(x) = 1$. Set $P = p \mapsto 1$. For every k such that $k \in \operatorname{dom} P$ holds $M(k) = P(k)$. $\sum F \equiv \sum M \pmod{p}$. □

(23) If $p \mid a + 1$, then $p^{k+1} \mid a^{p^k} + 1$ and $p^k \mid a^{p^k} + 1$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv p^{\$_1+1} \mid a^{p^{\$_1}} + 1$. For every natural number x such that $\mathcal{P}[x]$ holds $\mathcal{P}[x+1]$. For every natural number x, $\mathcal{P}[x]$. □

(24) Let us consider an odd natural number a. Suppose $a > 1$. Let us consider a natural number s. Suppose s is double odd and a^s+1 is double odd and $s \mid a^s + 1$. Then

(i) $a^s + 1 > s$, and

(ii) $a^s + 1$ is double odd, and

(iii) $a^{a^s+1} + 1$ is double odd, and

(iv) $a^s + 1 \mid a^{a^s+1} + 1$.

(25) Let us consider a natural number a. If $a > 1$, then $\{n$, where n is a natural number : $n \mid a^n + 1\}$ is infinite. The theorem is a consequence of (24) and (1).

(26) $\{n$, where n is a natural number : $n \mid 2^n + 2\}$ is infinite. The theorem is a consequence of (16).

(27) $\{n$, where n is a natural number : $5 \mid 2^n - 3\}$ is infinite.
Proof: Set $A = \{n$, where n is a natural number : $5 \mid 2^n - 3\}$. Define $\mathcal{F}(\text{natural number}) = 4 \cdot \$_1 + 3$. Consider f being a many sorted set indexed by $\mathbb{N}$ such that for every element d of $\mathbb{N}$, $f(d) = \mathcal{F}(d)$. $\operatorname{rng} f \subseteq A$. f is one-to-one. □

(28) $\{n$, where n is a natural number : $13 \mid 2^n - 3\}$ is infinite.
Proof: Set $A = \{n$, where n is a natural number : $13 \mid 2^n - 3\}$. Define $\mathcal{F}(\text{natural number}) = 12 \cdot \$_1 + 4$. Consider f being a many sorted set indexed by $\mathbb{N}$ such that for every element d of $\mathbb{N}$, $f(d) = \mathcal{F}(d)$. $\operatorname{rng} f \subseteq A$. f is one-to-one. □

(29) $2^{n+12} \equiv 2^n \pmod{65}$.

(30) $2^n \equiv 2^{n \bmod 12} \pmod{65}$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv 2^{\$_1} \equiv 2^{\$_1 \bmod 12} \pmod{65}$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$ by [7, (11)], [4, (4)]. $\mathcal{P}[k]$. □

(31) $65 \nmid 2^n - 3$. The theorem is a consequence of (30) and (2).

(32) 341 is composite.

(33) 561 is composite.

(34) 645 is composite.

(35) 1105 is composite.

(36) $341 \mid 2^{341} - 2$.

(37) $3 \mid 2^{561} - 2$.

(38) $11 \mid 2^{561} - 2$.

(39) $17 \mid 2^{561} - 2$.

(40) $561 \mid 2^{561} - 2$. The theorem is a consequence of (37), (38), (39), and (12).

(41) $3 \mid 2^{645} - 2$.

(42) $5 \mid 2^{645} - 2$.

(43) $43 \mid 2^{645} - 2$.

(44) $645 \mid 2^{645} - 2$. The theorem is a consequence of (41), (42), (43), and (12).

(45) $5 \mid 2^{1105} - 2$.

(46) $13 \mid 2^{1105} - 2$.

(47) $17 \mid 2^{1105} - 2$.

(48) $1105 \mid 2^{1105} - 2$. The theorem is a consequence of (45), (46), (47), and (12).

(49) Let us consider a composite natural number n. If $n \leqslant 1105$ and $n \mid 2^n - 2$, then $n \in \{341, 561, 645, 1105\}$.

(50) $341 \nmid 3^{341} - 3$. The theorem is a consequence of (4) and (3).

(51) $3 \mid 3^{561} - 3$.

(52) $11 \mid 3^{561} - 3$.

(53) $17 \mid 3^{561} - 3$.

(54) $561 \mid 3^{561} - 3$. The theorem is a consequence of (51), (52), (53), and (12).

Now we state the propositions:

(55) $43 \nmid 3^{645} - 3$.

(56) $645 \nmid 3^{645} - 3$. The theorem is a consequence of (55).

Now we state the propositions:

(57) $5 \mid 3^{1105} - 3$.

(58) $13 \mid 3^{1105} - 3$.

(59) $17 \mid 3^{1105} - 3$.

(60) $1105 \mid 3^{1105} - 3$. The theorem is a consequence of (57), (58), (59), and (12).

(61) If $n \leqslant 1105$ and n is composite and $n \mid 2^n - 2$ and $n \mid 3^n - 3$, then $n \in \{561, 1105\}$. The theorem is a consequence of (49), (50), and (56).

(62) If $n \mid 2^n - 2$ and $n \nmid 3^n - 3$, then n is composite.

(63) If $n \leqslant 341$ and $n \mid 2^n - 2$ and $n \nmid 3^n - 3$, then $n = 341$. The theorem is a consequence of (62) and (49).

(64) If m and n are relatively prime, then $a \cdot n + m$ and n are relatively prime.

(65) $7 \mid 10^{6 \cdot k + 4} + 3$. The theorem is a consequence of (64).

(66) $10^{6 \cdot k + 4} + 3$ is composite. The theorem is a consequence of (65).

(67) $\{10^n + 3$, where n is a natural number : $10^n + 3$ is composite$\}$ is infinite.

PROOF: Set $X = \{10^n+3$, where n is a natural number : 10^n+3 is composite$\}$. Set $z = 10^{6 \cdot 0+4} + 3$. z is composite. X is natural-membered. For every a such that $a \in X$ there exists b such that $b > a$ and $b \in X$ by [5, (66)]. □

References

[1] Kenichi Arai and Hiroyuki Okazaki. Properties of primes and multiplicative group of a field. *Formalized Mathematics*, 17(**2**):151–155, 2009. doi:10.2478/v10037-009-0017-7.

[2] 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.

[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] Yoshinori Fujisawa and Yasushi Fuwa. Definitions of radix-2^k signed-digit number and its adder algorithm. *Formalized Mathematics*, 9(**1**):71–75, 2001.

[5] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.

[6] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[7] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(**4**):181–187, 2007. doi:10.2478/v10037-007-0022-7.

[8] Adam Naumowicz. Dataset description: Formalization of elementary number theory in Mizar. In Christoph Benzmüller and Bruce R. Miller, editors, *Intelligent Computer Mathematics – 13th International Conference, CICM 2020, Bertinoro, Italy, July 26–31, 2020, Proceedings*, volume 12236 of *Lecture Notes in Computer Science*, pages 303–308. Springer, 2020. doi:10.1007/978-3-030-53518-6_22.

[9] Wacław Sierpiński. *250 Problems in Elementary Number Theory.* Elsevier, 1970.

Accepted September 30, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 3, Pages 229–234, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0018

sciendo.com/journal/forma

Elementary Number Theory Problems. Part V[1]

Artur Korniłowicz
Institute of Computer Science
University of Białystok
Poland

Adam Naumowicz
Institute of Computer Science
University of Białystok
Poland

Summary. This paper reports on the formalization of ten selected problems from W. Sierpinski's book "250 Problems in Elementary Number Theory" [5] using the Mizar system [4], [1], [2]. Problems 12, 13, 31, 32, 33, 35 and 40 belong to the chapter devoted to the divisibility of numbers, problem 47 concerns relatively prime numbers, whereas problems 76 and 79 are taken from the chapter on prime and composite numbers.

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes

MML identifier: `NUMBER05`, version: `8.1.12 5.71.1431`

1. Problem 12

Now we state the proposition:

(1) Let us consider natural numbers n, k. If $n \uparrow\uparrow k = 0$, then $n = 0$.

Let x be an odd natural number and i be a natural number. Let us note that $x \uparrow\uparrow i$ is odd.

Let x be a non zero, even natural number and i be a non zero natural number. One can verify that $x \uparrow\uparrow i$ is even. Now we state the proposition:

(2) Let us consider a non zero natural number n. Then there exists a non zero natural number x such that for every natural number i, $n \mid x \uparrow\uparrow (i+1) + 1$.

[1] The Mizar processing has been performed using the infrastructure of the University of Bialystok High Performance Computing Center.

2. Problem 13

Now we state the proposition:

(3) Let us consider natural numbers n, k. Suppose $n = 4 \cdot k + 3$. Then there exist natural numbers p, q such that

(i) $p = 4 \cdot q + 3$, and

(ii) p is prime, and

(iii) $p \mid n$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if there exists a natural number k such that $\$_1 = 4 \cdot k + 3$, then there exist natural numbers p, q such that $p = 4 \cdot q + 3$ and p is prime and $p \mid \$_1$. For every natural number m such that for every natural number l such that $l < m$ holds $\mathcal{P}[l]$ holds $\mathcal{P}[m]$ by [3, (28)], [6, (29)]. For every natural number n, $\mathcal{P}[n]$. Consider p, q being natural numbers such that $p = 4 \cdot q + 3$ and p is prime and $p \mid n$. □

The functor 4k + 3_Primes yielding a subset of $\mathbb{N}$ is defined by

(Def. 1) for every natural number n, $n \in$ *it* iff there exists a natural number k such that $n = 4 \cdot k + 3$ and n is prime.

Now we state the proposition:

(4) Let us consider a natural number n. If $n \in$ 4k + 3_Primes, then $n \geqslant 3$.

Let us observe that 4k + 3_Primes is infinite. Now we state the proposition:

(5) Let us consider a natural number n. Suppose $n \in$ 4k + 3_Primes. Let us consider an even natural number x, and a natural number i. Then $n \nmid x \uparrow\uparrow (i + 2) + 1$. The theorem is a consequence of (4).

3. Problem 31

Now we state the propositions:

(6) Let us consider an integer a. If $3 \nmid a$, then $a^3 \bmod 9 = 1$ or $a^3 \bmod 9 = 8$.

(7) Let us consider integers a, b, c. If $9 \mid a^3 + b^3 + c^3$, then $3 \mid a$ or $3 \mid b$ or $3 \mid c$. The theorem is a consequence of (6).

4. Problem 32

Now we state the propositions:

(8) Let us consider integers a, b, c, n. Then $a + b + c \bmod n = (a \bmod n) + (b \bmod n) + (c \bmod n) \bmod n$.

(9) Let us consider integers a, b, c, d, n. Then $a+b+c+d \bmod n = (a \bmod n)+(b \bmod n)+(c \bmod n)+(d \bmod n) \bmod n$. The theorem is a consequence of (8).

(10) Let us consider integers a, b, c, d, e, n. Then $a+b+c+d+e \bmod n = (a \bmod n)+(b \bmod n)+(c \bmod n)+(d \bmod n)+(e \bmod n) \bmod n$. The theorem is a consequence of (9).

(11) Let us consider integers a_1, a_2, a_3, a_4, a_5. Suppose $9 \mid {a_1}^3+{a_2}^3+{a_3}^3+{a_4}^3+{a_5}^3$. Then $3 \mid a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5$. The theorem is a consequence of (6) and (10).

5. Problem 33

From now on a, b, c, k, m, n denote natural numbers and p denotes a prime number. Now we state the propositions:

(12) $n \bmod (k+1) = 0$ or ... or $n \bmod (k+1) = k$.

(13) Let us consider natural numbers x, y, z. If x and y are relatively prime and $x^2+y^2=z^4$, then $7 \mid x \cdot y$.

(14) (i) 15 and 20 are not relatively prime, and

(ii) $15^2+20^2=5^4$, and

(iii) $7 \nmid 15 \cdot 20$.

6. Problem 35

Let x, y be natural numbers. We say that x and y satisfy Sierpiński Problem 35 if and only if

(Def. 2) $x \cdot (x+1) \mid y \cdot (y+1)$ and $x \nmid y$ and $x+1 \nmid y$ and $x \nmid y+1$ and $x+1 \nmid y+1$.

Now we state the propositions:

(15) Let us consider natural numbers x, y. Suppose $x = 36 \cdot k + 14$ and $y = (12 \cdot k + 5) \cdot (18 \cdot k + 7)$. Then x and y satisfy Sierpiński Problem 35.

(16) $\{\langle x, y\rangle$, where x, y are natural numbers : x and y satisfy Sierpiński Problem 35$\}$ is infinite.

Proof: Set $A = \{\langle x, y\rangle$, where x, y are natural numbers : x and y satisfy Sierpiński Problem 35$\}$. Define $\mathcal{F}$(natural number) $= \langle 36 \cdot \$_1 + 14, (12 \cdot \$_1+5)\cdot(18\cdot\$_1+7)\rangle$. Consider f being a many sorted set indexed by $\mathbb{N}$ such that for every element d of $\mathbb{N}$, $f(d) = \mathcal{F}(d)$. $\operatorname{rng} f \subseteq A$. f is one-to-one. □

(17) 14 and 35 satisfy Sierpiński Problem 35.

(18) There exist no natural numbers x, y such that $x < 14$ and $y < 35$ and x and y satisfy Sierpiński Problem 35.

7. Problem 40

Now we state the propositions:

(19) If $a \mid b$, then $n^a - 1 \mid n^b - 1$.

(20) $2^{2^n} + 1 \mid 2^{2^{2^n}+1} - 2$. The theorem is a consequence of (19).

8. Problem 47

Now we state the propositions:

(21) If $n \mid 4$, then $n = 1$ or $n = 2$ or $n = 4$.

(22) If $n > 6$, then there exist natural numbers a, b such that $a > 1$ and $b > 1$ and $n = a + b$ and a and b are relatively prime. The theorem is a consequence of (21).

9. Problem 76

Let n be a natural number. We say that n satisfies Sierpiński Problem 76a if and only if

(Def. 3) for every natural number x such that $n < x < n + 10$ holds x is not prime.

Let m be a natural number. We say that m satisfies Sierpiński Problem 76b if and only if

(Def. 4) for every natural number x such that $10 \cdot m < x < 10 \cdot (m + 1)$ holds x is not prime.

Now we state the propositions:

(23) 113 satisfies Sierpiński Problem 76a.

(24) 114 satisfies Sierpiński Problem 76a.

(25) 115 satisfies Sierpiński Problem 76a.

(26) 116 satisfies Sierpiński Problem 76a.

(27) 117 satisfies Sierpiński Problem 76a.

(28) 139 satisfies Sierpiński Problem 76a.

(29) 181 satisfies Sierpiński Problem 76a.

(30) If n satisfies Sierpiński Problem 76a and $n \leqslant 181$, then $n \in \{113, 114, 115, 116, 117, 139, 181\}$.

(31) 20 satisfies Sierpiński Problem 76b.

(32) 32 satisfies Sierpiński Problem 76b.

(33) 51 satisfies Sierpiński Problem 76b.

(34) 53 satisfies Sierpiński Problem 76b.

(35) 62 satisfies Sierpiński Problem 76b.

(36) If m satisfies Sierpiński Problem 76b and $m \leqslant 62$, then $m \in \{20, 32, 51, 53, 62\}$.

10. Problem 79

Now we state the propositions:

(37) If $c \neq 0$ and $c < b$, then $\frac{a \cdot b + c}{b}$ is not integer.

(38) There exist no positive natural numbers m, n such that $m^{\mathbf{2}} - n^{\mathbf{2}} = 1$.

(39) There exist no positive natural numbers m, n such that $m^{\mathbf{2}} - n^{\mathbf{2}} = 4$. The theorem is a consequence of (38).

(40) $(2 \cdot n + 1)^{\mathbf{2}} \bmod 8 = 1$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv (2 \cdot \$_1 + 1)^{\mathbf{2}} \bmod 8 = 1$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(41) If n is odd, then $n^{\mathbf{2}} \bmod 8 = 1$. The theorem is a consequence of (40).

(42) Let us consider prime numbers q, s, t. Suppose $q^{\mathbf{2}} = s^{\mathbf{2}} + t^{\mathbf{2}}$. Then

(i) s is even and t is odd, or

(ii) s is odd and t is even.

The theorem is a consequence of (39).

(43) There exist no prime numbers q, s, t such that $q^{\mathbf{2}} = s^{\mathbf{2}} + t^{\mathbf{2}}$. The theorem is a consequence of (42) and (39).

(44) Let us consider prime numbers p, q, r, s, t. Suppose $p^{\mathbf{2}} + q^{\mathbf{2}} = r^{\mathbf{2}} + s^{\mathbf{2}} + t^{\mathbf{2}}$. Then

(i) p is even, or

(ii) q is even, or

(iii) r is even, or

(iv) s is even, or

(v) t is even.

(45) There exist no prime numbers p, q, r, s, t such that $p^{\mathbf{2}} + q^{\mathbf{2}} = r^{\mathbf{2}} + s^{\mathbf{2}} + t^{\mathbf{2}}$. The theorem is a consequence of (43) and (41).

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] Robert Milewski. Natural numbers. *Formalized Mathematics*, 7(**1**):19–22, 1998.

[4] Adam Naumowicz. Dataset description: Formalization of elementary number theory in Mizar. In Christoph Benzmüller and Bruce R. Miller, editors, *Intelligent Computer Mathematics – 13th International Conference, CICM 2020, Bertinoro, Italy, July 26–31, 2020, Proceedings*, volume 12236 of *Lecture Notes in Computer Science*, pages 303–308. Springer, 2020. doi:10.1007/978-3-030-53518-6_22.

[5] Wacław Sierpiński. *250 Problems in Elementary Number Theory*. Elsevier, 1970.

[6] Rafał Ziobro. Prime factorization of sums and differences of two like powers. *Formalized Mathematics*, 24(**3**):187–198, 2016. doi:10.1515/forma-2016-0015.

Accepted September 30, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 3, Pages 235–244, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0019

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part VI

Adam Grabowski
Institute of Computer Science
University of Białystok
Poland

Summary. This paper reports on the formalization in Mizar system [1], [2] of ten selected problems from W. Sierpinski's book "250 Problems in Elementary Number Theory" [7] (see [6] for details of this concrete dataset). This article is devoted mainly to arithmetic progressions: problems 52, 54, 55, 56, 60, 64, 70, 71, and 73 belong to the chapter "Arithmetic Progressions", and problem 50 is from "Relatively Prime Numbers".

MSC: 11B25 03B35 68V20

Keywords: number theory; arithmetic progression; prime number

MML identifier: NUMBER06, version: 8.1.12 5.71.1431

1. Preliminaries

Now we state the proposition:

(1) Let us consider a prime number p. If $3 \mid p$, then $p = 3$.

Note that there exists a prime number which is even.

Now we state the propositions:

(2) Let us consider an even prime number p. Then $p = 2$.

(3) Let us consider prime numbers p, q. If $p \neq q$, then p and q are relatively prime.

Let f be an integer-valued function. We say that f is with all coprime terms if and only if

(Def. 1) for every natural numbers i, j such that i, $j \in \operatorname{dom} f$ and $i \neq j$ holds $f(i)$ and $f(j)$ are relatively prime.

Now we state the proposition:

(4) Let us consider a sequence f of $\mathbb{R}$, and a natural number n. Then $f{\restriction}n$ is a finite 0-sequence.

2. Arithmetic Progressions

Let f be a real-valued function. We say that f is AP-like if and only if

(Def. 2) for every natural numbers i, k such that i, $i+1$, k, $k+1 \in \operatorname{dom} f$ holds $f(i+1) - f(i) = f(k+1) - f(k)$.

Let f be a real-valued finite sequence. We say that f is finite arithmetic progression-like if and only if

(Def. 3) for every natural number i such that i, $i+1$, $i+2 \in \operatorname{dom} f$ holds $f(i+2) - f(i+1) = f(i+1) - f(i)$.

One can check that every real-valued finite sequence which is constant is also finite arithmetic progression-like and every sequence of $\mathbb{R}$ which is constant is also AP-like and $\mathrm{id}_{\mathbb{N}}$ is AP-like and $\mathrm{id}_{\mathbb{R}}$ is AP-like and there exists a sequence of $\mathbb{R}$ which is AP-like and there exists a real-valued function which is AP-like and there exists an integer-valued, real-valued finite 0-sequence which is AP-like.

Let f be an AP-like, real-valued function and n be a natural number. Let us note that $f{\restriction}n$ is AP-like.

An arithmetic progression is an AP-like sequence of $\mathbb{R}$. Let a, r be real numbers. The functor $\mathrm{ArProg}(a, r)$ yielding a sequence of $\mathbb{R}$ is defined by

(Def. 4) $it(0) = a$ and for every natural number i, $it(i+1) = it(i) + r$.

Let us observe that $\mathrm{ArProg}(a, r)$ is AP-like. Now we state the proposition:

(5) Let us consider an arithmetic progression f, and a natural number i. Then $f(i+1) - f(i) = f(1) - f(0)$.

Let f be an arithmetic progression. The functor difference(f) yielding a real number is defined by the term

(Def. 5) $f(1) - f(0)$.

Now we state the propositions:

(6) Let us consider an arithmetic progression f.
Then $f = \mathrm{ArProg}(f(0), \mathrm{difference}(f))$.
Proof: Set $a = f(0)$. Set $r = f(1) - f(0)$. Define $\mathcal{P}[\text{natural number}] \equiv f(\$_1) = (\mathrm{ArProg}(a, r))(\$_1)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number n, $\mathcal{P}[n]$. □

(7) Let us consider real numbers a, r, and a natural number i. Then $(\mathrm{ArProg}(a,r))(i) = a + i \cdot r$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (\mathrm{ArProg}(a,r))(\$_1) = a + \$_1 \cdot r$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number n, $\mathcal{P}[n]$. □

Let a, r be integers. Let us note that $\mathrm{ArProg}(a,r)$ is integer-valued and there exists an arithmetic progression which is integer-valued.

Let a be an integer and r be a non zero integer. Let us observe that $\mathrm{ArProg}(a,r)$ is non constant.

Let a be a real number and r be a positive real number. Let us observe that $\mathrm{ArProg}(a,r)$ is increasing.

Let r be a non positive real number. One can verify that $\mathrm{ArProg}(a,r)$ is non-increasing.

Let r be a negative real number. Note that $\mathrm{ArProg}(a,r)$ is decreasing.

Let r be a non negative real number. Let us note that $\mathrm{ArProg}(a,r)$ is non-decreasing and $\mathrm{ArProg}(a,0)$ is constant and there exists an arithmetic progression which is constant and there exists an arithmetic progression which is increasing and non-decreasing and there exists an arithmetic progression which is decreasing and non-increasing.

Let f be an increasing arithmetic progression. One can verify that difference(f) is positive.

Let f be a decreasing arithmetic progression. Note that difference(f) is negative.

Let f be a non-increasing arithmetic progression. Observe that difference(f) is non positive.

Let f be a non-decreasing arithmetic progression. Let us observe that difference(f) is non negative.

Let f be a constant arithmetic progression. One can verify that difference(f) is zero. Now we state the proposition:

(8) Let us consider an arithmetic progression f. Suppose there exists a natural number i such that $f(i)$ is an integer and difference(f) is an integer. Then f is integer-valued.

PROOF: Consider i being a natural number such that $f(i)$ is an integer and difference(f) is an integer. Define $\mathcal{P}[\text{natural number}] \equiv f(\$_1)$ is integer. 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 $\mathcal{P}[n]$. $\mathcal{P}[0]$. For every object n such that $n \in \mathrm{dom}\, f$ holds $f(n)$ is integer. □

3. Problem 50

Let n be a natural number. We say that n is Fibonacci if and only if

(Def. 6) there exists a natural number k such that $n = \mathrm{Fib}(k)$.

Let us note that there exists a natural number which is Fibonacci.

Now we state the propositions:

(9) Let us consider a natural number n. If $\mathrm{Fib}(n) > 1$, then $n > 2$.

(10) Let us consider a natural number k. If $k > 0$, then $\mathrm{Fib}(k) > 0$.

(11) Let us consider natural numbers k, m. Suppose $\mathrm{Fib}(k) < \mathrm{Fib}(m+1)$ and $1 < k$. Then $\mathrm{Fib}(k) \leqslant \mathrm{Fib}(m)$.

(12) Let us consider natural numbers k, n. Suppose $n \neq 1$ and $k \neq 0$ and $k \neq 1$. If $\mathrm{Fib}(k) = \mathrm{Fib}(n)$, then $k = n$. The theorem is a consequence of (10).

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

(13) If $n > 2$, then $\mathrm{Fib}(n) \geqslant 2$.

(14) If $n > 3$, then $\mathrm{Fib}(n) \geqslant 3$.

Let us consider natural numbers m, n. Now we state the propositions:

(15) If $m < n$ and $m > 3$, then $\mathrm{Fib}(n) - \mathrm{Fib}(m) > 1$. The theorem is a consequence of (13).

(16) If $m < n$ and $m > 4$, then $\mathrm{Fib}(n) - \mathrm{Fib}(m) > 2$. The theorem is a consequence of (14).

Let f be a sequence of $\mathbb{R}$. We say that f is Fibonacci-valued if and only if

(Def. 7) for every natural number n, there exists a natural number f_4 such that $f_4 = f(n)$ and f_4 is Fibonacci.

Let us observe that every sequence of $\mathbb{R}$ which is Fibonacci-valued is also integer-valued and there exists a sequence of $\mathbb{R}$ which is Fibonacci-valued.

Let n be a natural number. One can verify that $\mathrm{Fib}(n)$ is Fibonacci.

Now we state the proposition:

(17) There exists a Fibonacci-valued sequence f of $\mathbb{R}$ such that f is increasing and with all coprime terms.

Proof: Define $\mathcal{F}(\text{natural number}) = \mathrm{Fib}(\mathrm{pr}(\$_1))$. Consider f being a sequence of $\mathbb{R}$ such that for every natural number n, $f(n) = \mathcal{F}(n)$. For every natural number n, $f(n) < f(n+1)$ by [5, (46)]. For every natural number n, there exists a natural number f_4 such that $f_4 = f(n)$ and f_4 is Fibonacci. For every natural numbers i, j such that $i, j \in \operatorname{dom} f$ and $i \neq j$ holds $f(i)$ and $f(j)$ are relatively prime by [3, (21)], (3), [8, (5)]. □

Let us observe that there exists an integer-valued sequence of $\mathbb{R}$ which is Fibonacci-valued, increasing, and with all coprime terms.

4. TRIANGULAR NUMBERS

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

(18) (i) $3 \mid n$, or

(ii) $3 \mid n+1$, or

(iii) $3 \mid n+2$.

PROOF: $3 \mid n-1$ iff $3 \mid n+2$. □

(19) (i) $4 \mid n$, or

(ii) $4 \mid n+1$, or

(iii) $4 \mid n+2$, or

(iv) $4 \mid n+3$.

(20) Let us consider natural numbers n, k, l. Then $3 \mid n+l$ if and only if $3 \mid n+l+3 \cdot k$.

Let f be a function. We say that f is triangular-valued if and only if

(Def. 8) for every object n, $f(n)$ is triangular.

One can check that every number which is triangular is also integer and every sequence of $\mathbb{R}$ which is triangular-valued is also integer-valued and there exists an integer-valued sequence of $\mathbb{R}$ which is triangular-valued and $\langle 0 \rangle$ is triangular-valued as a finite sequence.

5. PROBLEM 52

Now we state the propositions:

(21) Let us consider natural numbers m, k, l. Suppose $k \neq l$ and $1 \leqslant k \leqslant m$ and $1 \leqslant l \leqslant m$. Then $m! \cdot k+1$ and $m! \cdot l+1$ are relatively prime.

(22) Let us consider a natural number n. Then there exists an AP-like, integer-valued finite 0-sequence f such that

(i) $\operatorname{dom} f \geqslant n$, and

(ii) f is with all coprime terms.

PROOF: Set $f = \operatorname{ArProg}(n!+1, n!)$. Reconsider $f_3 = f \restriction n$ as an integer-valued finite 0-sequence. For every natural number k, $f(k) = n! \cdot (k+1)+1$. For every natural number k such that $k+1 \leqslant n$ holds $f_3(k) = n! \cdot (k+1)+1$. For every natural numbers i, j such that i, $j \in \operatorname{dom} f_3$ and $i \neq j$ holds $f_3(i)$ and $f_3(j)$ are relatively prime. □

6. Problem 54

Let x, y, z be real numbers. We say that x, y and z form an arithmetic progression if and only if

(Def. 9) $y - x = z - y$.

Now we state the propositions:

(23) Let us consider natural numbers x, y, z. Suppose $y = 5 \cdot x + 2$ and $z = 7 \cdot x + 3$. Then

(i) $x \cdot (x + 1)$, $y \cdot (y + 1)$ and $z \cdot (z + 1)$ form an arithmetic progression, and

(ii) $x < y < z$.

(24) $\{\langle x, y, z\rangle$, where x is a real number, y is a real number, z is a real number : $x \cdot (x + 1)$, $y \cdot (y + 1)$ and $z \cdot (z + 1)$ form an arithmetic progression$\}$ is infinite.

Proof: Set $A_1 = \{\langle x, y, z\rangle$, where x is a real number, y is a real number, z is a real number : $x \cdot (x+1)$, $y \cdot (y+1)$ and $z \cdot (z+1)$ form an arithmetic progression$\}$. Reconsider $x = 1$ as a natural number. Reconsider $y = 5 \cdot x + 2$ as a natural number. Define $\mathcal{P}[$element of $\mathbb{R}$, element of $A_1] \equiv \$_2 = \langle \$_1, 5 \cdot \$_1 + 2, 7 \cdot \$_1 + 3\rangle$. For every element x of $\mathbb{R}$, there exists an element y of A_1 such that $\mathcal{P}[x, y]$. Consider f being a function from $\mathbb{R}$ into A_1 such that for every element x of $\mathbb{R}$, $\mathcal{P}[x, f(x)]$. For every objects x_1, x_2 such that x_1, $x_2 \in \mathbb{R}$ and $f(x_1) = f(x_2)$ holds $x_1 = x_2$. □

7. Problem 55

Now we state the proposition:

(25) Let us consider natural numbers a, b, c. Suppose $a^{\mathbf{2}} + b^{\mathbf{2}} = c^{\mathbf{2}}$ and a, b and c form an arithmetic progression. Then there exists an integer i such that

(i) $a = 3 \cdot i$, and

(ii) $b = 4 \cdot i$, and

(iii) $c = 5 \cdot i$.

8. Problem 56

Let k be a natural number. Observe that $\mathrm{Triangle}(4 \cdot k + 1)$ is odd and $\mathrm{Triangle}\,4 \cdot k$ is even.

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

(26) $3 \mid \mathrm{Triangle}(3 \cdot n + 2)$.

(27) $3 \mid \mathrm{Triangle}\,3 \cdot n$.

(28) $3 \mid \mathrm{Triangle}(3 \cdot n + 1) - 1$.

(29) Let us consider a natural number i. Then $3 \nmid (\mathrm{ArProg}(2, 3))(i)$. The theorem is a consequence of (7).

(30) $\{i$, where i is a natural number : $(\mathrm{ArProg}(0, 1))(i)$ is triangular$\}$ is infinite.

Proof: Set $X = \{i$, where i is a natural number : $(\mathrm{ArProg}(0, 1))(i)$ is triangular$\}$. For every natural number m, there exists a natural number n such that $n \geqslant m$ and $n \in X$ by [4, (19)], (7). □

(31) $\{i$, where i is a natural number : $(\mathrm{ArProg}(0, 2))(i)$ is triangular$\}$ is infinite.

Proof: Set $X = \{i$, where i is a natural number : $(\mathrm{ArProg}(0, 2))(i)$ is triangular$\}$. For every natural number m, there exists a natural number n such that $n \geqslant m$ and $n \in X$. □

(32) $\{i$, where i is a natural number : $(\mathrm{ArProg}(1, 2))(i)$ is triangular$\}$ is infinite.

Proof: Set $X = \{i$, where i is a natural number : $(\mathrm{ArProg}(1, 2))(i)$ is triangular$\}$. For every natural number m, there exists a natural number n such that $n \geqslant m$ and $n \in X$. □

(33) Let us consider a natural number i. Then $3 \nmid (\mathrm{ArProg}(2, 3))(i) - 1$. The theorem is a consequence of (7).

(34) Let us consider a natural number i. Then $(\mathrm{ArProg}(2, 3))(i)$ is not triangular. The theorem is a consequence of (28), (33), (29), (26), and (27).

9. Problem 60

Let n be a natural number. We say that n is perfect power if and only if

(Def. 10) there exists a natural number x and there exists a natural number k such that $k > 1$ and $n = x^k$.

Now we state the proposition:

(35) There exists a natural number n such that

(i) n is perfect power, and

(ii) $n+1$ is perfect power.

Let us note that there exists a natural number which is even and perfect power. Now we state the propositions:

(36) Let us consider an even natural number n, and a natural number k. If $k > 1$, then $4 \mid n^k$.

(37) Let us consider an even, perfect power natural number n. Then $4 \mid n$. The theorem is a consequence of (36).

(38) Let us consider a natural number k. Then $4 \cdot k + 2$ is not perfect power. The theorem is a consequence of (37).

(39) Let us consider a prime number p. Then p is not perfect power.

One can verify that every natural number which is prime is also non perfect power and every natural number which is a square is also perfect power.

Now we state the proposition:

(40) There exists no natural number n such that n is perfect power and $n+1$ is perfect power and $n+2$ is perfect power and $n+3$ is perfect power. The theorem is a consequence of (38).

10. Problem 64

Now we state the propositions:

(41) Let us consider natural numbers k, l, m. Suppose $0 < k < l < m$ and it is not true that $k = 2$ and $l = 3$ and $m = 4$ and it is not true that $k = 1$ and $l = 4$ and $m = 5$ and $\mathrm{Fib}(m) - \mathrm{Fib}(l) = \mathrm{Fib}(l) - \mathrm{Fib}(k)$ and $\mathrm{Fib}(l) - \mathrm{Fib}(k) > 0$. Then

(i) $l > 2$, and

(ii) $k = l - 2$, and

(iii) $m = l + 1$.

Proof: Set $u_2 = \mathrm{Fib}(l)$. Set $u_3 = \mathrm{Fib}(m)$. $\mathrm{Fib}(l) > 1$. $l > 2$. $u_3 < u_2 + u_2$. $\mathrm{Fib}(m) \leqslant \mathrm{Fib}(l+1)$. □

(42) $\mathrm{Fib}(1) - \mathrm{Fib}(0) \neq \mathrm{Fib}(2) - \mathrm{Fib}(1)$.

(43) $\mathrm{Fib}(1) - \mathrm{Fib}(0) = \mathrm{Fib}(3) - \mathrm{Fib}(1)$.

(44) $\mathrm{Fib}(2) - \mathrm{Fib}(0) = \mathrm{Fib}(3) - \mathrm{Fib}(2)$.

(45) $\mathrm{Fib}(3) - \mathrm{Fib}(2) = \mathrm{Fib}(4) - \mathrm{Fib}(3)$.

(46) $\mathrm{Fib}(5) = 5$.

(47) $\mathrm{Fib}(5) - \mathrm{Fib}(4) = \mathrm{Fib}(4) - \mathrm{Fib}(1)$.

(48) There exist no natural numbers k, l, m, n such that $0 < k < l < m < n$ and $\mathrm{Fib}(m) - \mathrm{Fib}(l) = \mathrm{Fib}(l) - \mathrm{Fib}(k) = \mathrm{Fib}(n) - \mathrm{Fib}(m)$ and $\mathrm{Fib}(l) - \mathrm{Fib}(k) > 0$. The theorem is a consequence of (41), (15), and (16).

11. Problem 70

Now we state the propositions:

(49) Let us consider an arithmetic progression f, and prime numbers p_1, p_2, p_3. Suppose $\mathrm{difference}(f) = 10$ and there exists a natural number i such that $p_1 = f(i)$ and $p_2 = f(i+1)$ and $p_3 = f(i+2)$. Then $p_1 = 3$. The theorem is a consequence of (20), (5), and (18).

(50) There exists no arithmetic progression f such that $\mathrm{difference}(f) = 10$ and there exist prime numbers p_1, p_2, p_3, p_4 and there exists a natural number i such that p_1, p_2, p_3, p_4 are mutually different and $p_1 = f(i)$ and $p_2 = f(i+1)$ and $p_3 = f(i+2)$ and $p_4 = f(i+3)$. The theorem is a consequence of (8), (5), (20), (18), and (1).

12. Problem 71

Now we state the propositions:

(51) There exists no arithmetic progression f such that $\mathrm{difference}(f) = 100$ and there exist prime numbers p_1, p_2, p_3 and there exists a natural number i such that p_1, p_2, p_3 are mutually different and $p_1 = f(i)$ and $p_2 = f(i+1)$ and $p_3 = f(i+2)$. The theorem is a consequence of (8), (5), (20), (1), and (18).

(52) There exists no arithmetic progression f such that $\mathrm{difference}(f) = 1000$ and there exist prime numbers p_1, p_2, p_3 and there exists a natural number i such that p_1, p_2, p_3 are mutually different and $p_1 = f(i)$ and $p_2 = f(i+1)$ and $p_3 = f(i+2)$. The theorem is a consequence of (8), (5), (20), (1), and (18).

13. Problem 73

Let k be an integer. We say that k is not representable by a sum or a difference of two primes if and only if

(Def. 11) there exist no prime numbers p_1, p_2 such that $k = p_1 + p_2$ or $k = p_1 - p_2$.

Let f be an integer-valued sequence of $\mathbb{R}$. We say that f is with terms not representable by a sum or a difference of two primes if and only if

(Def. 12) for every natural number i, $f(i)$ is not representable by a sum or a difference of two primes.

Now we state the propositions:

(53) Let us consider an integer k. Then $30 \cdot k + 7$ is odd.

(54) Let us consider a natural number k. Suppose $k \geqslant 1$. Then $30 \cdot k + 7$ is not representable by a sum or a difference of two primes. The theorem is a consequence of (53).

Note that ArProg$(37, 30)$ is with terms not representable by a sum or a difference of two primes.

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] Adam Grabowski. On square-free numbers. *Formalized Mathematics*, 21(**2**):153–162, 2013. doi:10.2478/forma-2013-0017.

[4] Adam Grabowski. Polygonal numbers. *Formalized Mathematics*, 21(**2**):103–113, 2013. doi:10.2478/forma-2013-0012.

[5] Magdalena Jastrzębska and Adam Grabowski. Some properties of Fibonacci numbers. *Formalized Mathematics*, 12(**3**):307–313, 2004.

[6] Adam Naumowicz. Dataset description: Formalization of elementary number theory in Mizar. In Christoph Benzmüller and Bruce R. Miller, editors, *Intelligent Computer Mathematics – 13th International Conference, CICM 2020, Bertinoro, Italy, July 26–31, 2020, Proceedings*, volume 12236 of *Lecture Notes in Computer Science*, pages 303–308. Springer, 2020. doi:10.1007/978-3-030-53518-6_22.

[7] Wacław Sierpiński. *250 Problems in Elementary Number Theory.* Elsevier, 1970.

[8] Robert M. Solovay. Fibonacci numbers. *Formalized Mathematics*, 10(**2**):81–83, 2002.

Accepted September 30, 2022