Časopis pro pěstování matematiky

Jiří Novotný
Cardinal arithmetic of a certain class of monounary algebras

Časopis pro pěstování matematiky, Vol. 111 (1986), No. 4, 384--393

Persistent URL: `http://dml.cz/dmlcz/118286`

Časopis pro pěstování matematiky, roč. 111(1986), Praha

CARDINAL ARITHMETIC OF A CERTAIN CLASS OF MONOUNARY ALGEBRAS

JIŘÍ NOVOTNÝ, Brno

(Received November 1, 1983, in revised form October 5, 1984)

1. INTRODUCTION

In the thirties Birkhoff [1], [2], [3] defined and studied three operations on the class of partially ordered sets: the cardinal sum, the cardinal product and the cardinal power. Many authors considered properties of these operations – see for example M. Novotný, Fuchs, Jónsson, McKenzie [4], [5], [6], [7], [8] – even on other structures (e.g. Tarski [9]), among them monounary algebras. Marica, Bryant [10] studied the cancellation law for multiplication and Simerský [11] proved the basic rule for exponentiation. Hyman [12] described the group of automorphisms on an arbitrary monounary algebra. This description was used by Hyman and Nation [13] for constructing groups of automorphisms on a monounary algebra provided these groups belong to some special classes. Some properties of the group of automorphisms on a monounary algebra are also mentioned in Jónsson [14].

This paper is concerned with the cardinal arithmetic of a natural class of monounary algebras. Further, we consider endomorphisms and automorphisms on an arbitrary algebra of the given class of monounary algebras.

2. BASIC NOTIONS

The cardinal number of a set M is denoted by the symbol $|M|$.

The ordered pair $\mathbf{A} = (A, f)$, where A is a set and f a mapping of A into itself, is called a monounary algebra.

We put $f^0 = \text{id } A$, $f^n = f f^{n-1}$ for any positive integer n.

For arbitrary $x, y \in A$, we put $(x, y) \in \varrho A$ iff there exist nonnegative integers p, q such that $f^p(x) = f^q(y)$.

Clearly, ϱA is an equivalence on A. Each class of the equivalence ϱA is called a component of the algebra $\mathbf{A}$.

If $\mathbf{A}$ has exactly one component, then it is said to be a connected monounary algebra.

The set $\{x \in A;$ there exists $n(x) > 0$ such that $f^{n(x)}(x) = x\}$ is called a cycle of a connected algebra $\boldsymbol{A}$.

If $\boldsymbol{A} = (A, f)$, $\boldsymbol{B} = (B, g)$ are monounary algebras, then a mapping $\varphi: \boldsymbol{B} \to \boldsymbol{A}$ is said to be a homomorphism of $\boldsymbol{B}$ into $\boldsymbol{A}$ iff $\varphi(g(x)) = f(\varphi(x))$ for each $x \in B$.

Hom $(\boldsymbol{B}, \boldsymbol{A})$ denotes the set of all homomorphisms of $\boldsymbol{B}$ into $\boldsymbol{A}$.

The bijective homomorphism is called an isomorphism. We write $\boldsymbol{A} \cong \boldsymbol{B}$ if there exists at least one isomorphism of $\boldsymbol{A}$ onto $\boldsymbol{B}$.

To any algebra $\boldsymbol{A}$, we can assign an algebra $t(\boldsymbol{A})$ isomorphic to $\boldsymbol{A}$ such that $\boldsymbol{A} \cong \boldsymbol{B}$ implies $t(\boldsymbol{A}) = t(\boldsymbol{B})$. The algebra $t(\boldsymbol{A})$ is called the type of the algebra $\boldsymbol{A}$ (compare [15] axiom VIII).

We shall study the class of monounary algebras which includes the empty set and the algebras consisting of a finite number of components, each being a cycle. This class is denoted by the symbol $\mathfrak{A}$.

The type of empty algebra is defined to be $\mathbf{0}$, the type of any which is a cycle of k (>0) elements is denoted by $\boldsymbol{k}$.

3. SUM AND PRODUCT

1. By the sum $\boldsymbol{A} + \boldsymbol{B}$ of two algebras $\boldsymbol{A} = (A, f)$, $\boldsymbol{B} = (B, g) \in \mathfrak{A}$, $A \cap B = \emptyset$, we mean the algebra $\boldsymbol{C} = (C, h)$ such that $C = A \cup B$, $h = f \cup g$.

2. By the product $\boldsymbol{A} \cdot \boldsymbol{B}$ of two algebras $\boldsymbol{A} = (A, f)$, $\boldsymbol{B} = (B, g)$ we mean the algebra $\boldsymbol{C} = (C, h)$ such that $C = A \times B$ and $h(a, b) = (f(a), g(b))$ for any $(a, b) \in C$.

3. The operation of addition is commutative and associative. The operation of multiplication is commutative and associative and distributive over addition.

4. If α is the type of an algebra $\boldsymbol{A}$, β the type of an algebra $\boldsymbol{B}$, then provided $A \cap B = \emptyset$ we define the sum of types $\alpha + \beta$ to be the type of the algebra $\boldsymbol{A} + \boldsymbol{B}$. Further, we define the product of types $\alpha \cdot \beta$ as the type of the algebra $\boldsymbol{A} \cdot \boldsymbol{B}$.

The operation $+$ and $.$ for types are, clearly, commutative and associative. This, above all, provides the possibility of making sums and products of a finite number of types.

Let $n > 0$, $k > 0$ be integers. The type of an algebra consisting of n cycles each having k elements is denoted by $n\boldsymbol{k}$.

We have, of course, $0\boldsymbol{k} = \mathbf{0}$.

Thus, the type of a nonempty algebra $\boldsymbol{A} \in \mathfrak{A}$ can be expressed in the form of a polynomial $a_1\mathbf{1} + a_2\mathbf{2} + \ldots + a_n\boldsymbol{n}$, where n is the cardinality of the largest cycle of the given algebra $\boldsymbol{A}$, $a_n \neq 0$.

If $p > n$ and we put $a_i = 0$ for $n < i \leqq p$, the same type can be expressed in the form $a_1\mathbf{1} + \ldots + a_p\mathbf{p}$. If $\alpha \neq \mathbf{0}$, $\alpha = a_1\mathbf{1} + \ldots + a_n\boldsymbol{n}$, where $a_n \neq 0$, we say that the type is expressed in the canonical form. Clearly, any type which differs from zero has exactly one canonical form.

5. For any integers $m, n > 0$ we have

$$\boldsymbol{m} \,.\, \boldsymbol{n} = g.c.d.(m, n)\ \boldsymbol{l.c.m.}(\boldsymbol{m}, \boldsymbol{n}),$$

where $g.c.d.$ means the greatest common divisor and $l.c.m.$ the lowest common multiple.

Proof. Let $\boldsymbol{M} = (M, f)$, $\boldsymbol{N} = (N, g)$, where $M = \{a_1, a_2, \ldots, a_m\}$, $f(a_i) = a_{i+1}$, $1 \leqq i < m$, $f(a_m) = a_1$; $N = \{b_1, b_2, \ldots, b_n\}$, $g(b_j) = b_{j+1}$, $1 \leqq j < n$, $g(b_n) = b_1$. The product $\boldsymbol{M} \,.\, \boldsymbol{N}$ will contain the elements (a_i, b_j), $1 \leqq i \leqq m$, $1 \leqq j \leqq n$ and its operation h satisfies

$$h(a_i, b_j) = \begin{cases} (a_{i+1}, b_{j+1}) & \text{for} \quad i < m\,, \quad j < n\,, \\ (a_1, b_{j+1}) & \text{for} \quad i = m\,, \quad j < n\,, \\ (a_{i+1}, b_1) & \text{for} \quad i < m\,, \quad j = n\,, \\ (a_1, b_1) & \text{for} \quad i = m\,, \quad j = n\,. \end{cases}$$

Clearly each element (a_i, b_j) lies in a cycle whose number of elements is $l.c.m.(m, n)$. Since the number of elements of the product considered is $m.n$ and $m.n = g.c.d.(m, n)$ $l.c.m.(m, n)$, the type of $\boldsymbol{M} \,.\, \boldsymbol{N}$ is $g.c.d.(m, n)$ $\boldsymbol{l.c.m.}(\boldsymbol{m}, \boldsymbol{n})$. □

If at least one of numbers m, n is equal to zero, then, clearly, $\boldsymbol{m} \,.\, \boldsymbol{n} = \mathbf{0}$.

6. By induction we can prove: For any integers $i_1 . i_2, \ldots, i_k > 0$ we have

$$\boldsymbol{i}_1 \,.\, \boldsymbol{i}_2 \ldots \boldsymbol{i}_k = \frac{i_1 \,.\, i_2 \ldots i_k}{[i_1, i_2, \ldots, i_k]}\ [\boldsymbol{i}_1, \boldsymbol{i}_2, \ldots, \boldsymbol{i}_k]\,,$$

where $[i_1, i_2, \ldots, i_k]$ denotes the l.c.m. of $i_1, i_2, \ldots, i_k$.

7. The class $\mathfrak{A}$ is closed with respect to addition and multiplication.

In more detail: If $t(\boldsymbol{A}) = a_1\mathbf{1} + a_2\mathbf{2} + \ldots + a_m\boldsymbol{m}$, $t(\boldsymbol{B}) = b_1\mathbf{1} + b_2\mathbf{2} + \ldots + b_n\boldsymbol{n}$, then we can write $t(\boldsymbol{A}) = a_1\mathbf{1} + \ldots + a_p\boldsymbol{p}$, $t(\boldsymbol{B}) = b_1\mathbf{1} + \ldots + b_p\boldsymbol{p}$, where $p = \max(m, n)$. Then

$$t(\boldsymbol{A} + \boldsymbol{B}) = \sum_{k=1}^{p} (a_k + b_k)\, \boldsymbol{k}$$

and

$$t(\boldsymbol{A} \,.\, \boldsymbol{B}) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j\ g.c.d.(i, j)\ \boldsymbol{l.c.m.}(\boldsymbol{i}, \boldsymbol{j})\,.$$

8. Since any algebra of the class $\mathfrak{A}$ has the uniquely defined type in the canonical form, it is clear that the following cancellation law for addition holds:

$$\boldsymbol{A} + \boldsymbol{B} \cong \boldsymbol{A} + \boldsymbol{C} \quad \text{implies} \quad \boldsymbol{B} \cong \boldsymbol{C}.$$

The cancellation law for multiplication:

$$\boldsymbol{A} \,.\, \boldsymbol{C} \cong \boldsymbol{B} \,.\, \boldsymbol{C} \quad \text{implies} \quad \boldsymbol{A} \cong \boldsymbol{B}$$

holds only for connected algebras $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in \mathfrak{A}$.

This is a direct consequence of 3.5.

The simplest example of its failure in the general case is the following: Let $\boldsymbol{A}$ be a two-cycle algebra and $\boldsymbol{B}$ the sum of two one-cycle algebras. In this case $\boldsymbol{A} \,.\, \boldsymbol{A} \cong \boldsymbol{B} \,.\, \boldsymbol{A}$ and $A \not\cong \boldsymbol{B}$.

Marica, Bryant [10] proved that

$$\boldsymbol{A} \,.\, \boldsymbol{A} \cong \boldsymbol{B} \,.\, \boldsymbol{B} \quad \text{implies} \quad \boldsymbol{A} \cong \boldsymbol{B}$$

for any finite monounary algebras $\boldsymbol{A}, \boldsymbol{B}$.

9. If α is the type of an algebra from the class $\mathfrak{A}$, $\alpha \neq \mathbf{0}$, then we define $\alpha^0 = \mathbf{1}$, $\alpha^{n+1} = \alpha^n \alpha$ for an arbitrary nonnegative integer n.

4. POWER

1. By the power of the base $\boldsymbol{A} = (A, f)$ with the exponent $\boldsymbol{B} = (B, g)$ we mean the algebra $\boldsymbol{C} = (C, h)$ such that $C = \operatorname{Hom}(\boldsymbol{B}, \boldsymbol{A})$ and $h(\varphi) = \varphi \,.\, g$ for each $\varphi \in C$.

2. Simerský [11] proved the following result: If $\boldsymbol{A}, \boldsymbol{B}$ are connected algebras such that $\operatorname{Hom}(\boldsymbol{B}, \boldsymbol{A}) \neq \emptyset$, then $\boldsymbol{A}^{\boldsymbol{B}} \cong \boldsymbol{A}$.

3. It can be proved that exponentiation satisfies similar rules as in arithmetic:

$$\boldsymbol{A}^{\boldsymbol{B}+\boldsymbol{C}} \cong \boldsymbol{A}^{\boldsymbol{B}} \,.\, \boldsymbol{A}^{\boldsymbol{C}}, \quad (\boldsymbol{A} \,.\, \boldsymbol{B})^{\boldsymbol{C}} \cong \boldsymbol{A}^{\boldsymbol{C}} \,.\, \boldsymbol{B}^{\boldsymbol{C}}$$

for arbitrary $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in \mathfrak{A}$.

Proofs are analogous to those for ordered sets. If we denote $R = \sum_{1 \leq j \leq n} \boldsymbol{B}_j$, these formulas yield by induction

$$\boldsymbol{A}^{\boldsymbol{R}} \cong \prod_{1 \leq j \leq n} \boldsymbol{A}^{\boldsymbol{B}_j}, \quad \Big(\prod_{1 \leq i \leq m} \boldsymbol{A}_i\Big)^{\boldsymbol{B}} \cong \prod_{1 \leq i \leq m} \boldsymbol{A}_i^{\boldsymbol{B}}$$

for arbitrary $\boldsymbol{A}, \boldsymbol{A}_i, \boldsymbol{B}_j \in \mathfrak{A}$, $m \geq 1$, $n \geq 1$, $1 \leq i \leq m$, $1 \leq j \leq n$.

Further, we have: $(\boldsymbol{A} + \boldsymbol{B})^{\boldsymbol{C}} \cong \boldsymbol{A}^{\boldsymbol{C}} + \boldsymbol{B}^{\boldsymbol{C}}$ for $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in \mathfrak{A}$, $\boldsymbol{C}$ connected.

Proof. Since C is connected, we have $\operatorname{Hom}(C, A + B) = \operatorname{Hom}(C, A) \cup \cup \operatorname{Hom}(C, B)$. The union is disjoint because C is mapped either to A, or to B. This implies the assertion. $\square$

We can prove by induction that

$$\left(\sum_{1 \leqq i \leqq m} A_i\right)^C \cong \sum_{1 \leqq i \leqq m} A_i^C \quad \text{for} \quad m \geqq 1\,, \quad \text{arbitrary } A_i\,,$$

$1 \leqq i \leqq m$, C connected.

4. If α is the type of an algebra A, β is the type of an algebra B, then we define the power of the types α^β to be the type of the algebra A^B.

Clearly, we have $\mathbf{1}^\alpha = \mathbf{1}$ for any type α . $\alpha^0 = \mathbf{1}$, $\mathbf{0}^\alpha = \mathbf{0}$ for any $\alpha \neq \mathbf{0}$.

5. Any integers $m, n > 0$ satisfy

$$\mathbf{m}^{\mathbf{n}} = \begin{cases} \mathbf{0} & \text{if} \quad m \nmid n\,, \\ \mathbf{m} & \text{if} \quad m \mid n\,. \end{cases}$$

Proof. Let $t(M) = \mathbf{m}$, $t(N) = \mathbf{n}$, then $\operatorname{Hom}(N, M) \neq \emptyset$ iff m is a divisor of n. The assertion follows from 4.2. $\square$

6. For any integers $a, b, m, n, >0$ we have

$$(a\mathbf{m})^{(b\mathbf{n})} = \begin{cases} \mathbf{0} & \text{if} \quad m \nmid n\,, \\ a^b m^{b-1} \mathbf{m} & \text{if} \quad m \mid n\,. \end{cases}$$

Proof.

$$(a\mathbf{m})^{(b\mathbf{n})} = (a\mathbf{m})^{(\mathbf{n}+\mathbf{n}+\ldots+\mathbf{n})} = (a\mathbf{m})^{\mathbf{n}} \,.\, (a\mathbf{m})^{\mathbf{n}} \ldots (a\mathbf{m})^{\mathbf{n}}\,,$$

where the dots indicated that the term repeats b-times. Now, if m is not a divisor of n, we obtain $\mathbf{0}$ and otherwise $(a\mathbf{m})^b$. The assertion follows by induction with respect to b. $\square$

7. The class $\mathfrak{A}$ is closed with respect to exponentiation. In more detail: We transform

$$(a_1\mathbf{1} + a_2\mathbf{2} + \ldots + a_m\mathbf{m})^{(b_1\mathbf{1} + b_2\mathbf{2} + \ldots + b_n\mathbf{n})}$$

to the canonical form.

Let us proceed via 4.3 and 4.6 in the following way, denoting $S = \left(\sum_{1 \leqq j \leqq n} b_j\mathbf{j}\right)$

$$\left(\sum_{1 \leqq i \leqq m} a_i\mathbf{i}\right)^S = \prod_{1 \leqq j \leqq n} \left(\sum_{1 \leqq i \leqq m} a_i\mathbf{i}\right)^{b_j\mathbf{j}} =$$

$$= \prod_{1 \leqq j \leqq n} \left(\left(\sum_{1 \leqq i \leqq m} a_i\mathbf{i}\right)^{\mathbf{j}}\right)^{b_j} = \prod_{1 \leqq j \leqq n} \left(\sum_{\substack{1 \leqq i \leqq m \\ i/j}} a_i\mathbf{i}\right)^{b_j}.$$

Put: $D(j, m) = \{i;\ 1 \leqq i \leqq m,\ i/j\}$. We are to compute $\left(\sum_{i \in D(j,m)} a_i\mathbf{i}\right)^{b_j}$.

Let D be a finite nonempty set of positive integers. We prove that for $k > 0$,

$$(\sum_{i\in D} a_i \boldsymbol{i})^k = \sum_{i_1\dots i_k \in D^k} a_{i_1} \dots a_{i_k} \frac{i_1 \dots i_k}{[i_1, \dots, i_k]} [\boldsymbol{i}_1, \dots, \boldsymbol{i}_k] .$$

The proof will proceed by induction with respect to the exponent k. The formula clearly holds for $k = 1$. Let us admit that it holds for some k and let us compute:

$$(\sum_{i\in D} a_i \boldsymbol{i})^{k+1} = (\sum_{i\in D} a_i \boldsymbol{i})^k (\sum_{i\in D} a_i \boldsymbol{i}) =$$

$$= \left(\sum_{i_1\dots i_k \in D^k} a_{i_1} \dots a_{i_k} \frac{i_1 \dots i_k}{[i_1, \dots, i_k]} [\boldsymbol{i}_1, \dots, \boldsymbol{i}_k] \right) . (\sum_{i\in D} a_i \boldsymbol{i}) =$$

$$= \left(\sum_{i_1\dots i_{k+1} \in D^{k+1}} a_{i_1} \dots a_{i_k} . a_{i_{k+1}} \frac{i_1 \dots i_k}{[i_1, \dots, i_k]} [\boldsymbol{i}_1, \dots, \boldsymbol{i}_k] \right) . \boldsymbol{i}_{k+1} =$$

$$= \sum_{i_1\dots i_{k+1} \in D^{k+1}} a_{i_1} \dots a_{i_{k+1}} \frac{i_1 \dots i_{k+1}}{[i_1, \dots, i_{k+1}]} [\boldsymbol{i}_1, \dots, \boldsymbol{i}_{k+1}] .$$

Thus, the formula is proved. In the case $k = 0$, the result is $\mathbf{1}$ by 3.9.

We write the result in a better arranged form. Clearly, $i_1 \dots i_k$ is a word from the set $D^k = D \times D \times \dots \times D$. Now, a can be considered as the mapping which assigns $a_i = a(i)$ to any $i \in D$. Then $a_{i_1} \dots a_{i_k} = a(i_1) \dots a(i_k) = a(w)$ can be considered as the image of the word w. Moreover, let us put $[w] = [i_1, \dots, i_k]$. Then we can write

$$(\sum_{i\in D} a_i \boldsymbol{i})^k = \sum_{w\in D^k} a(w) \frac{w}{[w]} [\boldsymbol{w}] ,$$

where w denotes at the same time also the unmultiplied product formed by the elements of the word w which can be dealt with as a word.

The above mentioned relation includes also the case $k = 0$ if to the usual conventions for the empty chain we add another one, $[\Lambda] = 1$.

Thus, if we return to the beginning, we have

$$(\sum_{1\leq i\leq m} a_i \boldsymbol{i})^S = \prod_{1\leq j\leq n} \left(\sum_{w\in D^{b_j}(j,m)} a(w) \frac{w}{[w]} [\boldsymbol{w}] \right) =$$

$$= \sum_{\substack{w\in D^{b_j}(j,m) \\ 1\leq j\leq n}} a(w_1) \dots a(w_n) \frac{w_1 \dots w_n}{[w_1] \dots [w_n]} [\boldsymbol{w}_1] \dots [\boldsymbol{w}_n] .$$

If we put here $W = w_1 \dots w_n$, then $W \in D^{b_1}(1, m) \dots D^{b_n}(n, m)$ and $a(w_1) \dots a(w_n)$ can be denoted by $a(W)$. Further,

$$[w_1] \dots [w_n] = \frac{[w_1] \dots [w_n]}{[[w_1], \dots, [w_n]]} [[w_1], \dots, [w_n]] \quad \text{by 3.6 ;}$$

thus we obtain

$$(\sum_{1\leq i\leq m} a_i i)^S =$$

$$= \sum_{W\in D^{b}{}_1(1,m)\dots D^{b}{}_n(n,m)} a(W) \frac{W}{[[w_1], \dots, [w_n]]} [[w_1], \dots, [w_n]] \,.$$

Now, evidently, $W = w_1 \dots w_n$ and each w_j is a word from $D^{b_j}(j, m)$. We put $[W] = [[w_1], \dots, [w_n]]$; clearly, it is the least common multiple of all elements contained in $w_1, \dots, w_n$. Then we can put

$$(\sum_{1\leq i\leq m} a_i i)^S = \sum_{W\in D^{b}{}_1(1,m)\dots D^{b}{}_n(n,m)} a(W) \frac{W}{[W]} [W] \,.$$

8. The computation of a power is illustrated by the following example:

$(32 + 23 + 45 + 16)^{(34+26)} =$

$= (32 + 23 + 45 + 16)^{34} \,.\, (32 + 23 + 45 + 16)^{26} =$

$= (32)^3 \,.\, (32 + 23 + 16)^2 \,.$

$(32)^3 = 3^3 2^2 2$ by 4.6.

$$(32 + 23 + 16)^2 = \sum_{W\in D^2(6,6)} a(w) \frac{w}{[w]} w \,,$$

$D(6, 6) = \{1, 2, 3, 6\}\,, \quad w = i_1 i_2 \,,$

$$\begin{aligned} D^2(6, 6) = \{&(1, 1); (1, 2); (1, 3); (1, 6);\\ &(2, 1); (2, 2); (2, 3); (2, 6);\\ &(3, 1); (3, 2); (3, 3); (3, 6);\\ &(6, 1); (6, 2); (6, 3); (6, 6)\}\,, \end{aligned}$$

$a(1) = 0\,, \quad a(2) = 3\,, \quad a(3) = 2\,, \quad a(6) = 1\,,$

$$\begin{aligned} \{a(w);\ w \in D^2(6, 6)\} = \{&0;\ 0;\ 0;\ 0;\\ &0;\ 3\,.\,3;\ 3\,.\,2;\ 3\,.\,1;\\ &0;\ 1\,.\,3;\ 1\,.\,2;\ 1\,.\,1\}\,, \end{aligned}$$

$$\begin{aligned} \{[w];\ w \in D^2(6, 6)\} = \{&1;\ 2;\ 3;\ 6;\\ &2;\ 2;\ 6;\ 6;\\ &3;\ 6;\ 3;\ 6;\\ &6;\ 6;\ 6;\ 6\}\,. \end{aligned}$$

Thus

$$\sum_{w\in D^2(6,6)} a(w)\frac{w}{[w]}[w] = 3\,.\,3\frac{2\,.\,2}{2}\mathbf{2} + 3\,.\,2\frac{2\,.\,3}{6}\mathbf{6} +$$

$$+ 3\,.\,1\frac{2\,.\,6}{6}\mathbf{6} + 2\,.\,3\frac{3\,.\,2}{6}\mathbf{6} + 2\,.\,2\frac{3\,.\,3}{3}\mathbf{3} + 2\,.\,1\frac{3\,.\,6}{6}\mathbf{6} +$$

$$+ 1\,.\,3\frac{6\,.\,2}{6}\mathbf{6} + 1\,.\,2\frac{6\,.\,3}{6}\mathbf{6} + 1\,.\,1\frac{6\,.\,6}{6}\mathbf{6} =$$

$$= 2\,.\,3^2\mathbf{2} + 2^2\mathbf{3}\mathbf{3} + 2\,.\,3\,.\,7\mathbf{6}\,.$$

Together,

$$(\mathbf{3}\mathbf{2})^3\,.\,(\mathbf{3}\mathbf{2} + \mathbf{2}\mathbf{3} + \mathbf{1}\mathbf{6})^2 = 3^3\,.\,2^2\mathbf{2}(2\,.\,3^2\mathbf{2} + 2^2\,.\,\mathbf{3}\mathbf{3} + 2\,.\,3\,.\,7\mathbf{6}) =$$
$$= 2^4\,.\,3^5\mathbf{2} + 2^4\,.\,3^4\mathbf{6} + 2^4\,.\,3^4\,.\,7\mathbf{6} = 2^4\,.\,3^5\mathbf{2} + 2^7\,.\,3^4\mathbf{6}\,.$$

9. For exponentiation the cancellation law for exponents:

$$\boldsymbol{A}^{\boldsymbol{C}} \cong \boldsymbol{B}^{\boldsymbol{C}} \quad \text{implies} \quad \boldsymbol{A} \cong \boldsymbol{B}$$

holds only for connected algebras $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in \mathfrak{A}$ such that $\operatorname{Hom}(C, A) \neq \emptyset$. Indeed, then $\boldsymbol{A} \cong \boldsymbol{A}^{\boldsymbol{C}} \cong \boldsymbol{B}^{\boldsymbol{C}} \cong \boldsymbol{B}$.

For disconnected algebras the law does not hold in general. For example:

$$(\mathbf{2} + \mathbf{3})^{\mathbf{4}} = \mathbf{2}^{\mathbf{4}} = \mathbf{2}\,, \quad (\mathbf{2} + \mathbf{5})^{\mathbf{4}} = \mathbf{2}^{\mathbf{4}} = \mathbf{2}$$

and at the same time $\mathbf{2} + \mathbf{3} \neq \mathbf{2} + \mathbf{5}$.

The cancellation law for bases:

$$\boldsymbol{A}^{\boldsymbol{B}} \cong \boldsymbol{A}^{\boldsymbol{C}} \quad \text{implies} \quad \boldsymbol{B} \cong \boldsymbol{C}$$

does not hold even for connected algebras.

Indeed, $\boldsymbol{A}^{\boldsymbol{B}} \cong \boldsymbol{A}$ whenever $\operatorname{Hom}(\boldsymbol{B}, \boldsymbol{A}) \neq \emptyset$.

5. ENDOMORPHISMS AND AUTOMORPHISMS

A homomorphism of $\boldsymbol{A}$ into $\boldsymbol{A}$ is called an endomorphism. End $\boldsymbol{A}$ denotes the set of all endomorphisms of the algebra $\boldsymbol{A} = (A, f)$.

1. Let $\boldsymbol{A} \in \mathfrak{A}$, $t(\boldsymbol{A}) = a_1\mathbf{1} + a_2\mathbf{2} + \ldots + a_m\boldsymbol{m}$. Then

$$|\operatorname{End} \boldsymbol{A}| = \prod_{i=1}^{m}\Big(\sum_{j/i} j\,.\,a_j\Big)^{a_i}\,.$$

Proof. By 4.7, denoting $T = \sum_{1\leq i\leq m} a_i\boldsymbol{i}$ we have

$$\Big(\sum_{1\leq i\leq m} a_i\boldsymbol{i}\Big)^{T} = \sum_{W\in D^{a_1}(1,m)\ldots D^{a_m}(m,m)} a(W)\frac{W}{[W]}[W]\,.$$

Thus, the number of endomorphisms is

$$\sum_{W \in D^{a_1}(1,m)\dots D^{a_m}(m,m)} a(W) \,.\, W = \prod_{1 \leqq i \leqq m} \Big(\sum_{w \in D^{a_i}(i,m)} a(w) \,.\, w \Big) =$$

$$\prod_{1 \leqq i \leqq m} \Big(\sum_{j_1 \dots j_{a_i} \in D^{b_j}(i,m)} a_{j_1} \dots a_{j_{a_i}} j_1 \dots j_{a_i} \Big) = \prod_{1 \leqq i \leqq m} \Big(\sum_{j/i} j \,.\, a_j \Big)^{a_i} . \square$$

An isomorphism of A onto A is called an automorphism. Aut A denotes the set of all automorphisms on the algebra A.

2. Let $A \in \mathfrak{A}$ be such that $t(A) = a_1\mathbf{1} + a_2\mathbf{2} + \dots + a_m\mathbf{m}$. Then an arbitrary automorphism F of the algebra A can be expressed in the form

$$F = \prod_{i=1}^{m} \begin{pmatrix} \sigma_i(1) & \dots & \sigma_i(a_i) \\ o_1^i & \dots & o_{a_i}^i \end{pmatrix},$$

where σ_i is a permutation on the set $\{1, \dots, a_i\}$ of i-element cycles, which expresses that the k-th component is mapped onto the $\sigma_i(k)$-th component of the algebra A by the automorphism F, and where o^i are numbers from the set $\{0, 1, \dots, i - 1\}$ expressing the rotation of these cycles with regard to identity. This form is called the canonical description of the automorphism.

3. By 5.1, taking into account that any endomorphism of a connected algebra $A \in \mathfrak{A}$ is an automorphism, we obtain:

Let $A \in \mathfrak{A}$ be a connected algebra. Then

$$|\mathrm{Aut}\, A| = |\mathrm{End}\, A| = |A| .$$

4. For any integers $m, n, a > 0$, $m \neq n$, we have

a) $|\mathrm{Aut}\,(\mathbf{m} + \mathbf{n})| = m \,.\, n$,
b) $|\mathrm{Aut}\,(a\mathbf{m})| = a!\, m^a$.

Proof. a) follows from 5.3. An arbitrary automorphism of the algebra A whose type is $t(A) = a\mathbf{m}$, has the canonical description

$$\begin{pmatrix} \sigma(1) & \dots & \sigma(a) \\ o_1 & \dots & o_a \end{pmatrix}.$$

(Compare 5.2.) Thus, for a fixed σ, we obtain m^a words of the form $o_1 \dots o_a$ $(0 \leqq o_i \leqq m - 1)$; the number of permutations σ is $a!$. Hence, we obtain the assertion b). $\square$

5. Let $A \in \mathfrak{A}$, $t(A) = a_1\mathbf{1} + a_2\mathbf{2} + \dots + a_m\mathbf{m}$. Then

$$|\mathrm{Aut}\, A| = \prod_{i=1}^{m} a_i!\, i^{a_i} .$$

Proof. An arbitrary automorphism of the algebra A can be expressed in the canonical form

$$\prod_{i=1}^{m} \begin{pmatrix} \sigma_i(1) & \ldots & \sigma_i(a_i) \\ o_1^i & \ldots & o_{a_i}^i \end{pmatrix}.$$

(Compare 5.2.) Now, the assertion follows from 5.4. □

6. CONCLUSION

The studied arithmetic is the simplest extension of the usual arithmetic of natural numbers for the special class of monounary algebras. In the case when the algebra A consists of m and algebra B of n one-element cycles, the operations $m + n$, $m \cdot n$ and m^n have their current sense and the numbers $|\text{End}\, m|$ and $|\text{Aut}\, m|$ reach well-known values.

References

[1] *G. Birkhoff:* Lattice Theory, rev. ed. New York 1948.
[2] *G. Birkhoff:* Extended arithmetic, Duke Math. J. *3* (1937), 312—316.
[3] *K. Birkhoff:* Generalized arithmetic, Duke Math. J. *9* (1942), 283—302.
[4] *M. Novotný:* Über gewisse Eigenschaften von Kardinaloperationen, Spisy Přírod. Fak. Univ. Brno, No *418* (1960), 465—484.
[5] *E. Fuchs:* Isomorphismus der Kardinalpotenzen, Arch. Math. Brno, *1* (1965), 83—93.
[6] *M. Novotný:* Über Isomorphismen gewisser Kardinalpotenzen, Ann. Mat. Pura Appl., (4) *54* (1961), 301—310.
[7] *B. Jónsson, R. McKenzie:* Powers of partially ordered sets: Cancellation and refinement properties, Math. Scand. *51* (1982), 87—220.
[8] *B. Jónsson:* The aritmetic of ordered sets, In: Ordered sets (ed. I. Rival), 3—41, D. Reidel Publishing Company, Dordrecht 1982.
[9] *A. Tarski:* Cardinal Algebras, New York 1949.
[10] *J. C. Marica, S. J. Bryant:* Unary algebras, Pac. Math. J., *10* (1960), 1347—1359.
[11] *M. Simerský:* Arithmetic of monounary algebras (Czech), Thesis, Brno 1979.
[12] *J. Hyman:* Automorphisms of 1-unary algebras I, Algebra Univ. *4* (1974), No 1, 61—77.
[13] *J. Hyman, J. B. Nation:* Automorphisms of 1-unary algebras II., ibid, 127—131.
[14] *B. Jónsson:* Topics in Universal Algebra, Lecture Notes Math. 250, Berlin, Springer 1972.
[15] *K. Kuratowski, A. Mostowski:* Set Theory, Amsterdam 1967.

Author's address: 625 00 Brno, Voroněžské nám. 15.