Mathematica Slovaca

Jiří Novotný

On the characterization of a certain class of monounary algebras

Mathematica Slovaca, Vol. 40 (1990), No. 2, 123--128

Persistent URL: http://dml.cz/dmlcz/136505

Math. Slovaca 40, 1990, No. 2, 123—128

ON THE CHARACTERIZATION OF A CERTAIN CLASS OF MONOUNARY ALGEBRAS

JIŘÍ NOVOTNÝ

1. Introduction

In literature we may observe a continual interest in monounary algebras, the simplicity of which enables relatively objective results even of advanced algebraic studies. Compare papers [13], [4] and monographs [5], [10]. Further, attempts have been carried out on arithmetic of types, first Birkhoff [1], [2] and others, e.g., [6], [7]. These questions were worked out for types of ordered sets. Analogical results were achieved for a certain class of monounary algebras [11], [12]. Here we continue in this study. We are concerned with the questions of cancellation and the algebraic characterization of the studied class of monounary algebras. There are described subclasses satisfying the cancellation law for multiplication. It is shown that the studied class forms a pseudovariety which, moreover, can be described in the terminology of usual algebraic structures.

2. Basic notions

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

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

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

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

If $\boldsymbol{A}$ has exactly one component, then $\boldsymbol{A}$ 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 the algebra $\boldsymbol{A}$.

We study the class of monounary algebras consisting of a finite number of components each being a cycle. This class is denoted by the symbol $\mathfrak{A}$.

The type $t(\boldsymbol{A})$ of any algebra $\boldsymbol{A}$ of the studied class $\mathfrak{A}$ can be expressed in the canonical form of a polynomial $a_1\boldsymbol{1} + a_2\boldsymbol{2} + \ldots + a_m\boldsymbol{m}$, which means that the algebra $\boldsymbol{A}$ consists of a_i i-element cycles, $1 \leqq i \leqq m$. The numbers a_i are determined uniquely by $\boldsymbol{A}$, $\boldsymbol{i}$ means the type of an i-element cycle.

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

By the product $\boldsymbol{A} \,.\, \boldsymbol{B}$ of the algebras $\boldsymbol{A} = (A, f)$, $\boldsymbol{B} = (B, g)$ we mean the algebra $\boldsymbol{C} = (C, h)$ such that $C = A \times B$, $h(a, b) = (f(a), g(b))$ for any $(a, b) \in C$. For $\underbrace{\boldsymbol{A} \,.\, \boldsymbol{A} \ldots \boldsymbol{A}}_{n \text{ times}}$ we write $\boldsymbol{A}^n$.

1. *For any positive integers i, j such that* $\boldsymbol{i} = t(\boldsymbol{A})$, $\boldsymbol{j} = t(\boldsymbol{B})$, $\boldsymbol{A}$, $\boldsymbol{B} \in \mathfrak{A}$ *we have*

$$\boldsymbol{i} \,.\, \boldsymbol{j} = \mathrm{g.c.d.}(i, j)\, \mathbf{l.c.m.}(i, j),$$

where g.c.d *means the greatest common divisor and* l.c.m *the least common multiple.*

Compare [11] 3.5.

3. Cancellation law

In this paragraph we shall consider the following cancellation law for multiplication:

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

Some results are known for arbitrary finite monounary algebras.

If $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ are finite, $\boldsymbol{C}$ contains one-element cycles, then $\boldsymbol{A} \,.\, \boldsymbol{C} \cong \boldsymbol{B} \,.\, \boldsymbol{C}$ implies $\boldsymbol{A} \cong \boldsymbol{B}$. Compare [7] 4.3.

If $\boldsymbol{A}$, $\boldsymbol{B}$ are finite and $\boldsymbol{A}^n \cong \boldsymbol{B}^n$ then $\boldsymbol{A} \cong \boldsymbol{B}$.
Compare [7] 4.2., or [6] and for $n = 2$ [9].
We shall study the problem in the class $\mathfrak{A}$.
By 2.1. (compare also [9], 6.3.) we have

1. *Let* $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C} \in \mathfrak{A}$ *be connected algebras. Then they satisfy the cancellation law:* $\boldsymbol{A} \,.\, \boldsymbol{C} \cong \boldsymbol{B} \,.\, \boldsymbol{C}$, $\boldsymbol{C} \neq \emptyset$ *implies* $\boldsymbol{A} \cong \boldsymbol{B}$.

2. *If* $k = p \,.\, q$, *where* p, q *are positive integers, then* $\boldsymbol{k} \,.\, \boldsymbol{k} = q\boldsymbol{p} \,.\, \boldsymbol{k}$.

Proof: $\boldsymbol{k} \,.\, \boldsymbol{k} = k\boldsymbol{k}$, since $\mathrm{g.c.d.}(k, k) = \mathrm{l.c.m.}(k, k) = k$. Furthermore, $\boldsymbol{p} \,.\, \boldsymbol{k} = p \,.\, \boldsymbol{k}$ and thus $q\ \boldsymbol{p} \,.\, \boldsymbol{k} = qp\boldsymbol{k} = k\boldsymbol{k}$. □

As a consequence we obtain the assertion:

3. *Let* $\mathscr{B}$ *be a class of cyclic monounary algebras closed with respect to addition and multiplication (i.e. if* $\boldsymbol{A}$, $\boldsymbol{B} \in \mathscr{B}$, *then* $\boldsymbol{A} + \boldsymbol{B}$, $\boldsymbol{A} \,.\, \boldsymbol{B} \in \mathscr{B}$*) containing two different cycles. Then the cancellation law for multiplication is not satisfied in* $\mathscr{B}$.

Proof: Let p, q, r be positive integers, $p \neq rq$, $p > 1$, $q \geqq 1$. Then $\mathrm{g.c.d.}(p, q)\,\mathbf{l.c.m.}(\boldsymbol{p}, \boldsymbol{q}).\mathbf{l.c.m.}(\boldsymbol{p}, \boldsymbol{q}) = \mathrm{g.c.d.}(p, q)\,\mathrm{l.c.m.}(p, q)\,\mathbf{l.c.m.}(\boldsymbol{p}, \boldsymbol{q}) = pq\,\mathbf{l.c.m.}(\boldsymbol{p}, \boldsymbol{q})$ and also $p\boldsymbol{q}\mathbf{l.c.m.}(\boldsymbol{p}, \boldsymbol{q}) = pq\,\mathbf{l.c.m.}(\boldsymbol{p}, \boldsymbol{q})$. Thus, $\mathrm{g.c.d.}(p, q)\,\mathbf{l.c.m.}(\boldsymbol{p}, \boldsymbol{q}).\mathbf{l.c.m.}(\boldsymbol{p}, \boldsymbol{q}) = p\boldsymbol{q}.\mathbf{l.c.m.}(\boldsymbol{p}, \boldsymbol{q})$. After cancellation $\mathrm{g.c.d.}(p, q)\,\mathbf{l.c.m.}(\boldsymbol{p}, \boldsymbol{q}) = p\boldsymbol{q}$, which is a contradiction. □

4. *Any subclass of $\mathfrak{A}$ closed with respect to addition and multiplication satisfying the cancellation law for multiplication is of the form $\{n\boldsymbol{k};\ n \geqq 0\}$, where k is a positive integer. We denote this class by the symbol $\mathscr{K}(k)$.*

Proof: Let $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C} \in \mathscr{K}(k)$, $t(\boldsymbol{A}) = a\boldsymbol{k}$, $t(\boldsymbol{B}) = b\boldsymbol{k}$, $t(\boldsymbol{C}) = c\boldsymbol{k}$.
Then by [11] 3.7.

$$a\boldsymbol{k} + b\boldsymbol{k} = (a + b)\,\boldsymbol{k},\ (a\boldsymbol{k}).(b\boldsymbol{k}) = abk\boldsymbol{k}.$$

Further, if $\boldsymbol{A}.\boldsymbol{C} \cong \boldsymbol{B}.\boldsymbol{C}$, then $ack\boldsymbol{k} = bck\boldsymbol{k}$ and $a\boldsymbol{k} = b\boldsymbol{k}$, thus $\boldsymbol{A} \cong \boldsymbol{B}$. From this and 3.3. we obtain the assertion. □

5. *For $k > 1$ the class $\mathscr{K}(k)$ is not isomorphic to the set of natural numbers ($\boldsymbol{N}$, $+$, .).*

Proof: Let i be an isomorphism of N onto $\mathscr{K}(k)$. N contains the unique zero element 0 and $\mathscr{K}(k)$ has the zero element $0\boldsymbol{k} = \boldsymbol{0}$. Thus $i(0) = \boldsymbol{0}$. Further, $1 \neq 0$ implies $i(1) \neq \boldsymbol{0}$. From this $i(1) = n\boldsymbol{k}$ for some $n > 0$. Now, we have $n\boldsymbol{k} = i(1) = i(1.1) = i(1).i(1) = (n\boldsymbol{k}).(n\boldsymbol{k}) = n^2k\boldsymbol{k}$. From the uniqueness of the type we have $n = n^2k$, thus $1 = nk$, which is not possible for $k > 1$. Thus, there is no isomorphism of N onto $\mathscr{K}(k)$. □

4. Algebraic structure of extension

Let $\mathscr{V}$ be a family of algebras. According to the usual definition in universal algebra $\mathscr{V}$ is a variety if it satisfies the following conditions:
(1) *If* $\mathrm{S} \in \mathscr{V}$ and T is a subalgebra of S, then $\mathrm{T} \in \mathscr{V}$.
(2) *If $S \in \mathscr{V}$ and T is a quotientalgebra of S, then $T \in \mathscr{V}$.*
(3) *The direct product of any family in $\mathscr{V}$ is in $\mathscr{V}$.*

Since we are concerned only with finite monounary algebras it will be natural to restrict (3) to finite direct products. Such a family $\mathscr{V}$ is sometimes called a pseudovariety. Compare [3] p. 109.

1. $\mathfrak{A}$ *is, clearly, a pseudovariety of monounary algebras.*

Let $\boldsymbol{A}_i$ be a two-element cycle for any $i \in \mathrm{N}$. Then $\boldsymbol{A}_i \in \mathfrak{A}$ and the direct product of all $\boldsymbol{A}_i$, clearly, contains infinite many elements, therefore $\Pi \boldsymbol{A}_i \notin \mathfrak{A}$. Thus, $\mathfrak{A}$ is not a variety.

2. *Let us define the relation $\equiv$ on $\mathfrak{A} \times \mathfrak{A}$ in the following way: $[\boldsymbol{A}_1, \boldsymbol{A}_2] \equiv [\boldsymbol{B}_1, \boldsymbol{B}_2]$ iff $t(\boldsymbol{A}_1) + t(\boldsymbol{B}_2) = t(\boldsymbol{A}_2) + t(\boldsymbol{B}_1)$. Then the relation $\equiv$ is an equivalence on the set $\mathfrak{A} \times \mathfrak{A} = \mathfrak{A}^2$.*

Proof: The assertion follows from the commutativity and the associativity of the addition of types. See [11] 3.4. □

The factor set $\mathfrak{A}^2/\equiv$ is denoted by the symbol $\mathfrak{A}^*$. If $a \in \mathfrak{A}^*$, $[\boldsymbol{A}_1, \boldsymbol{A}_2] \in a$, we write $a = T[\boldsymbol{A}_1, \boldsymbol{A}_2]$.

3. $\mathfrak{A}^*$ *is a commutative group if we define the addition on classes of* $\equiv$ *in the following way. If* $a = T[\boldsymbol{A}_1, \boldsymbol{A}_2]$, $b = T[\boldsymbol{B}_1, \boldsymbol{B}_2]$ *we set* $a + b = T[\boldsymbol{A}_1 + \boldsymbol{B}_1, \boldsymbol{A}_2 + \boldsymbol{B}_2]$.

Proof: $\mathfrak{A}$ is a commutative semigroup with cancellation, which can be isomorphically embedded into a commutative group. In this group $\mathfrak{A}^*$ $0 = T[\boldsymbol{A}, \boldsymbol{A}]$ is a zero element and to any element $a = T[\boldsymbol{A}_1, \boldsymbol{A}_2)$ there exists an additive inverse element $-a = T[\boldsymbol{A}_2, \boldsymbol{A}_1]$. □

4. Let us represent $T[\boldsymbol{A}_1, \boldsymbol{A}_2]$ by $(t(\boldsymbol{A}_1), t(\boldsymbol{A}_2))$. Instead of $(t(\boldsymbol{A}_1), \boldsymbol{0})$ we write $t(\boldsymbol{A}_1)$, instead of $(\boldsymbol{0}, t(\boldsymbol{A}_2)) - t(\boldsymbol{A}_2)$. Clearly, we have $(t(\boldsymbol{A}_1), t(\boldsymbol{A}_2)) = t(\boldsymbol{A}_1) - t(\boldsymbol{A}_2)$ and, thus, the set $\mathfrak{A}^*$ contains elements of the form of polynomials $a_1\boldsymbol{1} + a_2\boldsymbol{2} + \ldots + a_n\boldsymbol{n}$ with integer coefficients a_i, $1 \leqq i \leqq n$.

An algebraic structure $\mathscr{X}$ that is at the same time a commutative ring and a module over K, is called a commutative algebra over K if, moreover,

$$(*)\ \alpha(xy) = (\alpha x)y = x(\alpha y)$$

for any $x, y \in \mathscr{X}$, $\alpha \in K$. Compare [8] p. 386.

5. $\mathfrak{A}^*$ is a commutative algebra over the ring of integers.

Proof: $\mathfrak{A}^*$ is a module over the ring of integers. The axioms of scalar product are clearly satisfied since by 4.4. we proceed with polynomials with integer coefficients. The multiplicative condition $(*)$ from the definition is also fulfilled. Compare 2.1. Together, we have obtained a commutative algebra. □

6. The commutative ring $\mathfrak{A}^*$ cannot be extended to a field since it is not an integral domain. The necessary and sufficient condition for a commutative ring to be an integral domain, is the validity of the cancellation law. Compare [8] the assertion 10, p. 165. The cancellation law for multiplication does not hold in $\mathfrak{A}^*$ (see 3.3.).

7. Let $\mathscr{K}$ be a commutative algebra over the ring of integers. Then the following assertions are equivalent:

(A) $\mathscr{K}$ and $\mathfrak{A}^*$ are isomorphic.

(B) The module of $\mathscr{K}$ is free over a countable set of generators $\{v_i; i > 0\}$ and for these ring elements we have

$$v_i \,.\, v_j = \mathrm{g.c.d.}(i, j) \,.\, v_{\mathrm{l.c.m.}(i,j)}.$$

Proof: I. The algebra $\mathfrak{A}^*$ is formed by polynomials $a_1\boldsymbol{1} + a_2\boldsymbol{2} + \ldots + a_n\boldsymbol{n}$ with the integer coefficient a_i, $1 \leqq i \leqq n$. The elements $\boldsymbol{1}, \boldsymbol{2}, \ldots, \boldsymbol{n}, \ldots$ clearly are generators of the module of $\mathfrak{A}^*$. By 2.1. we have $\boldsymbol{i}\,.\,\boldsymbol{j} = \mathrm{g.c.d.}(i, j)\,\mathbf{l.c.m.}(\boldsymbol{i}, \boldsymbol{j})$. Thus (A) implies (B).

II. Let $\mathscr{K}$ be a free module over the ring of integers with a set of free generators $\{v_i; i > 0\}$. We show that the mapping θ described by the assignment $v_i \to \boldsymbol{i}$ induces an isomorphism of $\mathscr{K}$ onto $\mathfrak{A}^*$. Indeed, as $\{v_i; i > 0\}$ is a set of generators, the mapping θ can be extended to a linear mapping of modules of algebras $\mathscr{K}$ and $\mathfrak{A}^*$, that is at the same time a ring homomorphism. Further, we have $\theta(v_i \,.\, v_j) = \theta(\mathrm{g.c.d.}(i, j) \,.\, v_{\mathrm{l.c.m.}(i,j)}) = \mathrm{g.c.d.}(i, j) \,.\, \theta(v_{\mathrm{l.c.m.}(i,j)}) = = \mathrm{g.c.d.}(i,j)\, \mathbf{l.c.m.}(\boldsymbol{i},\boldsymbol{j}) = \boldsymbol{i} \,.\, \boldsymbol{j}$. Similarly a mapping ϑ given by the prescription $\boldsymbol{i} \to v_i$ can be extended to a homomorphism of $\mathfrak{A}^*$ onto $\mathscr{K}$ that satisfies the relation

$$\vartheta(\boldsymbol{i} \,.\, \boldsymbol{j}) = \vartheta(\mathrm{g.c.d.}(i,j)\, \mathbf{l.c.m.}(\boldsymbol{i}, \boldsymbol{j})) = \mathrm{g.c.d.}(i,j)\, v_{\mathrm{l.c.m.}(i,j)} = v_i \,.\, v_j.$$

By a composition of the mappings $\theta \,.\, \vartheta$ we obtain the identity on $\mathfrak{A}^*$ and by a composition of the mappings $\vartheta \,.\, \theta$ the identity on $\mathscr{K}$. Hence (B) implies (A). □

5. Concluding remarks

We have presented the example of the pseudovariety different from Eilenberg's examples. Moreover, we have achieved a full characterization of the algebra of types from $\mathfrak{A}^*$ by means of commutative algebras.

REFERENCES

[1] BIRKHOFF, G.: Extended arithmetic. Duke Math. J. 3 (1937), 312—316.

[2] BIRKHOFF, G.: Generalized arithmetic. Duke Math. J. 9 (1942), 283—302.

[3] EILENBERG, S.: Automata, Languages, and Machines. Volume B, Academic Press, New York 1976.

[4] JAKUBÍKOVÁ—STUDENOVSKÁ, D.: On completions of partial monounary algebras. Czech. Math. J. 38 (113) 1988, 256—268.

[5] JÓNSSON, B.: Topics in Universal Algebra. Lecture Notes in Mathematics 250, Springer Verlag, Berlin 1972.

[6] JÓNSSON, B.: The arithmetic of ordered sets. In: Ordered sets (ed. I. Rival), 3—41, D. Reidel Publ. Comp., Dordrecht 1982.

[7] LOVÁSZ, L.: Operations with structures. Acta Math. Acad. Sci. Hung. 18 (3—4), 1967, 321—328.

[8] MAC LANE, S.—BIRKHOFF, G.: Algebra. Macmillan Comp., New York 1968.

[9] MARICA, J. C.—BRYANT, S. J.: Unary algebras. Pacif. Math. J. 10 (1960), 1347—1359.

[10] MC KENZIE, R. N.—MC NULTY, G. F.—TAYLOR, W. F.: Algebras, Lattices, Varieties. Volume I, Wadsworth&Brooks, Monterey, California 1987.

[11] NOVOTNÝ, J.: Cardinal arithmetic of a certain class of monounary algebras. Čas. pro pěst. mat. 111 (1986), 384—393.

[12] NOVOTNÝ, J.: Morphisms of a certain class of monounary algebras. Math. Slovaca 38, 1988, 243—247.

[13] SKORNJAKOV, L. A.: Unars. Collog. Math. Soc. János Bolyai 29, Univ. algebra, Esztergom 1977, 735—743.

Received September 5, 1988

Katedra matematiky a deskriptivní geometrie FAST VUT
Barvičova 85,
662 37 Brno

О ХАРАКТЕРИЗАЦИИ ОДНОГО КЛАССА МОНОУНАРНЫХ АЛГЕБР

Jiří Novotný

Резюме

В статье показано, какие подклассы класса циклических моноунарных алгебр удовлетворяют законам сокращения для произведения. Далее решается вопрос алгебраической характеризации изучаемого класса моноунарных алгебр.