Commentationes Mathematicae Universitatis Carolinae

Aleš Pultr; Jiří Sichler

Primitive classes of algebras with two unary idempotent operations, containing all algebraic categories as full subcategories

Commentationes Mathematicae Universitatis Carolinae, Vol. 10 (1969), No. 3, 425--445

Persistent URL: http://dml.cz/dmlcz/105244

Commentationes Mathematicae Universitatis Carolinae
10,3 (1969)

PRIMITIVE CLASSES OF ALGEBRAS WITH TWO UNARY IDEMPOTENT OPERATIONS, CONTAINING ALL ALGEBRAIC CATEGORIES AS FULL SUBCATEGORIES

A. PULTR and J. SICHLER, Praha

Introduction. In the present paper, these primitive classes of algebras are discusssed, into which any category of algebras can be embedded.

To describe the contents of the paper more precisely, let us first introduce some notions: A category $\mathcal{K}$ is said to be algebraic if there exists a full embedding of $\mathcal{K}$ into some category of algebras and all their homomorphisms. A category is said to be binding if every algebraic category can be embedded into it. A concrete category $(\mathcal{K}, \square)$ (under a concrete category we mean a category together with a firmly given forgetful functor, here $\square$) is said to be strongly algebraic if there exists a strong embedding of $(\mathcal{K}, \square)$ into a (concrete) category of algebras. (A strong embedding of $(\mathcal{K}, \square)$ into $(\mathcal{K}', \square')$ is a full embedding $\Phi : \mathcal{K} \longrightarrow \mathcal{K}'$ such that there is a functor F, mapping the category of sets into itself, with $\square' \circ \Phi = F \circ \square$; categories of algebras are treated as concrete categories endowed by the natural forgetful functors.) A concrete category is said to be strongly binding if every strongly algebraic category can be strongly embedded into it.

There was proved in [1] that every algebraic category can be fully embedded into the category $\mathfrak{A}(1, 1)$ of algebras with two unary operations, i.e. that $\mathfrak{A}(1, 1)$ is binding. By [3], $\mathfrak{A}(1, 1)$ is, moreover, strongly binding. There arises naturally the question, which subcategories, particularly which primitive subclasses of $\mathfrak{A}(1, 1)$ are binding or strongly binding. This, in general, seems to be rather complicated, partly due to the large variety of possible systems of identities. We restricted ourselves to the primitive subclasses of the class $I(1, 1)$ of the algebras $(X;\varphi,\psi)$ with $\varphi^2=\varphi$, $\psi^2=\psi$ (we shall call them idempotent algebras; the mentioned basic identities will be frequently omitted), since the systems of identities describing such primitive classes are particularly lucid.

We prove that a primitive subclass of $I(1, 1)$ is binding or strongly binding (these two properties are equivalent in this case) if (see § 1) and only if (see § 2) it contains some primitive class P_k defined by the identities $\varphi^2 = \varphi$, $\psi^2 = \psi$, $(\varphi\psi)^k\varphi = \varphi$, $(\psi\varphi)^k\psi = \psi$ with $k \geq 3$.

Minimal binding primitive subclasses of $I(1,1)$ are exactly the classes P_k with $k = 4$ or $k =$ odd prime. This answers for $I(1,1)$ the problem stated in [4], where minimal binding primitive classes are considered in more details.

By results of § 2, we obtain also another characterization of binding primitive subclasses of $I(1, 1)$

namely (see 2.10) the existence of nontrivial rigid algebras (i.e. algebras without nontrivial endomorphisms). In § 3 we added a complete analysis of cardinalities of rigid algebras appearing in primitive subclasses of $\mathfrak{I}(1,1)$.

§ 1. Strong embedding of $\mathfrak{A}(1,1)$ into P_k .

1.1. Construction I. Let k be a natural number, $k \geq 3$. Let us define unary operations φ, ψ on the set $A = \{(0,0),\dots,(2k-1,0),(0,1),\dots,(2k-1,1),(u,0),(u,1),p,q,r\}$ by

$$\varphi(2i,j) = (2i,j), \qquad \varphi(2i+1,j) = (2(i+1),j),$$

$$\psi(2i,j) = (2i+1,j), \qquad \psi(2i+1,j) = (2i+1,j),$$

$$\varphi(u,j) = (0,j), \quad \psi(u,j) = (3,j), \quad \varphi(p) = (2,0),$$

$$\psi(p) = (2k-1,1), \quad \varphi(q) = (2k-2,1), \quad \psi(q) = (1,0),$$

$$\varphi(r) = (0,0), \qquad \psi(r) = (2k-3,1)$$

($+$ designates the addition $\operatorname{mod} 2k$).
Obviously, $A' = A \dot{-} \{q, r\}$ is a subalgebra of $(A;\varphi,\psi)$.
1.2. Lemma. The embedding of A' into A is the unique homomorphism $A' \longrightarrow A$.

Proof. We see that only $(u,0)$ and $(u,1)$ satisfy $(\psi\varphi)^2(x) = \psi(x)$. Further, we have $(2i,j) = (\varphi\psi)^i(0,j)$, $(2i+1,j) = \psi(\varphi\psi)^i(0,j)$. Thus, for homomorphism $h: A' \longrightarrow A$ we have $h(u,j) = (u,l_j)$, $h(i,j) = (i,l_j)$.
If $l_0 = 1$, we obtain $\varphi(h(p)) = h(\varphi(p)) = (2,1)$, so

that either $h(p)=(2,1)$ or $h(p)=(1,1)$. On the other hand, $\psi(h(p))=h(\psi(p))=(2k-1,\ell_1)$, so that either $h(p)=p$ or $h(p)=(2k-1,\ell_1)$ or $h(p)=$ $=(2k-2,\ell_1)$. This is a contradiction, since $k \geq 3$. Thus,

$$h(u,0)=(u,0)\ ,\ h(i,0)=(i,0)$$
$$(i=0,1,\dots,2k-1)\ .$$

Now, since $\varphi(h(p))=h(\varphi(p))=(2,0)$, $h(p)$ is either p or $(2,0)$ or $(1,0)$. The second and the third case implies that $h(2k-1,1)=h(\psi(p))$ is either $(1,0)$ or $(3,0)$ which is (again by $k \geq 3$) impossible. Thus, $h(p)=p$ and $(2k-1,\ell_1)=h(2k-1,1)=$ $=h(\psi(p))=\psi(p)=(2k-1,1)$. It follows $\ell_1=1$, $h(u,1)=(u,1)$ and $h(i,1)=(i,1)$ $(i=0,\dots,2k-1)$.

1.3. <u>Construction II</u>. Let $(X;\alpha,\beta)$ be an algebra with two unary operations. Preserving the notation from 1.1, we define operations τ^X, $\vartheta^X_{\alpha\beta}$ (if there is no danger of confusion, we write simply τ, ϑ) on $X\times A$ by:

$$\tau(x,a)=(x,\varphi(a))\ \text{ for any } a\in A\ ,$$
$$\vartheta(x,a)=(x,\psi(a))\ \text{ for any } a\in A'\ ,$$
$$\vartheta(x,q)=(\alpha(x),\psi(q))\ ,$$
$$\vartheta(x,r)=(\beta(x),\psi(r))\ .$$

1.4. <u>Lemma</u>. $\pi: X\times A\longrightarrow A$ defined by $\pi(x,a)=a$ is a homomorphism of $(X\times A;\tau,\vartheta)$ into $(A;\varphi,\psi)$. For $x\in X$, $v_x: A\longrightarrow X\times A$ defined by $v_x(a)=(x,a)$ is a homomorphism of $(A';\varphi,\psi)$ into $(X\times A;\tau,\vartheta)$.

Proof is trivial.

1.5. **Lemma**. Let $(X;\alpha,\beta)$, $(X';\alpha',\beta')$ be objects of $\mathcal{O}\!\iota(1,1)$. Let $g:(X\times A;\tau,\vartheta)\longrightarrow(X'\times A;\tau',\vartheta')$ be a homomorphism (we write τ' instead of $\tau^{X'}$, ϑ' instead of $\vartheta^{X'}_{\alpha',\beta'}$). Then $g=f\times id_A$, where $f:(X;\alpha,\beta)\longrightarrow(X';\alpha',\beta')$ is a homomorphism.

Proof. $\pi g v_X$ is a homomorphism. Thus, by 1.2, $g(x,a)=(y,a)$ for any $a\in A'$. Define $f_j: X\rightarrow X'$ by $g(x,(u,j))=(f_j(x),(u,j))$. We obtain $g(x,(2i,j))=$ $=g(\tau\vartheta)^i\tau(x,(u,j))=(\tau\vartheta)^i\tau g(x,(u,j))=(f_j(x),(2i,j))$ and similarly $g(x,(2i+1,j))=g(\vartheta\tau)^{i+1}(x,(u,j))=$ $=f_j(x,(2i+1,j))$. Defining y by $g(x,p)=(y,p)$, we get $(y,(2,0))=\tau'(y,p)=g\tau(x,p)=g(x,(2,0))=(f_0(x),(2,0))$, $(y,(2k-1,1))=\vartheta'(y,p)=g\vartheta(x,p)=(f_1(x),(2k-1,1))$.

Thus, $f_0=f_1=f$ and $g(x,p)=(f(x),p)$.

Now, put $g(x,q)=(y,a)$. We have

(1) $\tau'(y,a)=\tau'g(x,q)=g\tau(x,q)=g(x,(2k-2,1))=$
$=(f(x),(2k-2,1))$,

(2) $\vartheta'(y,a)=\vartheta'g(x,q)=g\vartheta(x,q)=g(\alpha(x),(1,0))=$
$=(f(\alpha(x)),(1,0))$.

By (1), a equals either q or $(z,1)$ for some z, by (2), a equals either q or $(z,0)$ for some z. Thus, $a=q$ and by (1), $y=f(x)$.

Similarly, put $g(x,r)=(y,a)$. We have

(1′) $\tau'(y,a)=\tau'g(x,r)=g\tau(x,r)=g(x,(0,0))=$
$=(f(x),(0,0))$,

(2′) $\vartheta'(y,a)=\vartheta'g(x,r)=g\vartheta(x,r)=g(\beta(x),(2k-3,1))=$

$= (f(\beta(x)), (2k-3, 1))$.

By (1′), a equals either $\varkappa$ or $(x, 0)$, by (2′), a equals either $\varkappa$ or $(x, 1)$. Thus, $a = \varkappa$, $y = f(x)$.

Consequently, $g = f \times id_A$. f is a homomorphism, since $(\alpha'(f(x)), (1,0)) = \vartheta' g(x, q) = g\vartheta(x, q) = (f(\alpha(x)), (1, 0))$ (see (2)) and similarly $(\beta'(f(x)), (2k-3, 1)) = (f(\beta(x)), (2k-3, 1))$.

1.6. Lemma. There exists a strong embedding of $\mathcal{O}\!\mathcal{L}(1,1)$ into its primitive subclass P_k of algebras $(X; \tau, \vartheta)$ satisfying $\tau^2 = \tau$, $\vartheta^2 = \vartheta$, $\tau = \tau(\vartheta\tau)^k$, $\vartheta = \vartheta(\tau\vartheta)^k$ where k is a fixed natural number, $k \geq 3$.

Proof. Denote by $\mathcal{S}$ the category of sets and define a functor $F: \mathcal{S} \longrightarrow \mathcal{S}$ by $F(X) = X \times A$, $F(f) = f \times id_A$. Put $\Phi(X; \alpha, \beta) = (X \times A; \tau^X, \vartheta^X_{\alpha\beta})$ (see 1.3). It is easy to see that $\Phi(X; \alpha, \beta)$ is always in P_k .
If $f: (X; \alpha, \beta) \longrightarrow (X'; \alpha', \beta')$ is a homomorphism, $f \times id_A$ is obviously a homomorphism of $\Phi(X; \alpha, \beta)$ into $\Phi(X'; \alpha', \beta')$. Thus, extending the prescription Φ for morphisms by $\square\Phi(f) = F\square f$, we obtain a functor $\Phi: \mathcal{O}\!\mathcal{L}(1,1) \longrightarrow P_k$. Φ is evidently one-to-one and maps $\mathcal{O}\!\mathcal{L}(1,1)$ onto a full subcategory of P_k (see 1.5). We have, of course, $\square \circ \Phi = F \circ \square$.

§ 2. Embeddings into general primitive subclasses of I(1,1).

In the following lemmas, $(X; \alpha, \beta)$ is always an algebra with two unary idempotent operations.

2.1. Lemma. Let $|X| > 1$, $\alpha(x) = \beta(y)$ for some $x, y \in X$. Then, $(X; \alpha, \beta)$ has a proper endomorphism.

Proof. For $z = \alpha(x)$ we obtain $z = \alpha(z) = \beta(z)$. Thus, $const_z$ is a homomorphism.

2.2. Lemma. Let $|X| > 2$, $\alpha\beta(x_0) = x_0$. Then, $(X; \alpha, \beta)$ has a proper endomorphism h.

Proof. We may assume (see 2.1) that for no z $\alpha(z) = z = \beta(z)$ holds. Put $y_0 = \beta(x_0)$. We have $\alpha(y_0) = x_0$, $\alpha(x_0) = x_0$, $\beta(y_0) = y_0$, $\beta(x_0) = y_0$. Put $h(x) = y_0$ whenever $\beta(x) = x$, $h(x) = x_0$ otherwise.

2.3. Lemma. Let w be a non-empty word in α, β. Let $w(x) = x$ for every $x \in X$. Then, $(X; \alpha, \beta)$ has a proper endomorphism.

Proof. Let, e.g., $w = v \circ \beta$. Thus, β is one-to-one, so that, by $\beta^2(x) = \beta(x)$, $\beta(x) = x$ for every $x \in X$. Take $x_0 \in X$, we have $\alpha(x_0) = \beta\alpha(x_0)$ and we may use 2.1.

2.4. Lemma. Let v, w be words. If either $\alpha v(x) = \beta w(x)$ for every x and $|X| > 1$, or if $v\alpha(x) = w\beta(x)$ for every x and $|X| > 2$, then $(X; \alpha, \beta)$ has a proper andomorphism.

Proof. By 2.1 this is trivial for $\alpha v = \beta w$. Now, put $v = (\alpha\beta)^k$ (after a possible renotation of α and β) and we obtain $\alpha\beta(v\alpha(x)) = (\alpha\beta)^k\alpha\beta\alpha(x) = (v\alpha)\beta\alpha(x) = (w\beta)\alpha(x) = (v\alpha)(x)$.

The second statement follows by 2.2.

2.5. Definition. A cycle of the length $2m$ $(m \geq 1)$ in $(X; \alpha, \beta)$ is a sequence $a_0, b_0, a_1, b_1, \dots$ $\dots, a_{m-1}, b_{m-1}$ of elements of X such that

1. $\beta(a_i) = b_i$ $(i \leqq m-1)$, $\alpha(b_i) = a_{i+1}$ $(i \leqq m-2)$, $\alpha(b_{m-1}) = a_0$,

2. the elements $a_0, b_0, \dots, a_{m-1}, b_{m-1}$ are distinct.

A cycle of the length 0 is an element x with $x = \alpha(x) = \beta(x)$, an infinite cycle is a sequence $a_0, b_0, a_1, b_1, \dots$ such that $\beta(a_i) = b_i$, $\alpha(b_i) = a_{i+1}$ and all the elements a_i, b_i are distinct.

2.6. Lemma. Let $(X; \alpha, \beta)$ contain a cycle of the length 4 and let all the other cycles be of a finite non-zero length divisible by 4. Then, $(X; \alpha, \beta)$ has a non-identical endomorphism. Consequently, if $(\alpha\beta)^{m+2}(x) = (\alpha\beta)^m(x)$ for every $x \in X$ and if $|X| > 2$, $(X; \alpha, \beta)$ has a non-identical endomorphism.

Proof. Denote by $0, 1, 2, 3$ the elements of the cycle of the length 4, let $\beta(0) = 1$, $\alpha(1) = 2$, $\beta(2) = 3$, $\alpha(3) = 0$. Put $h(j) = j$. Let C be any other cycle. Choose $a_c \in C$ with $\alpha(a_c) = a_c$ and define $h(\alpha\beta)^{2i}(a_c) = 0$, $h\beta(\alpha\beta)^{2i}(a_c) = 1$, $h(\alpha\beta)^{2i+1}(a_c) = 2$, $h\beta(\alpha\beta)^{2i+1}(a_c) = 3$.

Now, let x be contained in no cycle. Since there are no infinite cycles, $h((\alpha\beta)^k(x))$ is defined for some k and equal to 0. According to the possible lengths of the cycles such a k is always (for a given x) even or always odd.

If k is even, put

$h(x)=0$ for $x=\alpha(x)$, $h(x)=1$ for $x=\beta(x)$,

if $x\in X \dot{-} (\alpha(X)\cup\beta(X))$ and $(\alpha\beta)^{\ell}\alpha(x)=0$, then $h(x)=0$ for ℓ even, $h(x)=1$ for ℓ odd.

If k is odd, put

$h(x)=2$ for $x=\alpha(x)$, $h(x)=3$ for $x=\beta(x)$,

if $x\in X \dot{-} (\alpha(X)\cup\beta(X))$ and $(\alpha\beta)^{\ell}\alpha(x)=0$, then $h(x)=3$ for ℓ even, $h(x)=2$ for ℓ odd.

It is easy to see that h is a homomorphism. If $|X|=4$, $(X;\alpha,\beta)$ has an endomorphism f defined by $f(i)=i+2$ (addition $mod\ 4$).

The second statement is obtained as follows: If α, β satisfy the mentioned equation, $(X;\alpha,\beta)$ either has a cycle of the length 0 (see 2.1), or has a cycle of the length 2 (see 2.2), or all its cycles are of the length 4 and we can use the first statement.

2.7. <u>Lemma.</u> Let v, w be words in α, β, let $w(x)=v(y)$ for every x, $y\in X$. If $|X|>2$, then $(X;\alpha,\beta)$ has a proper endomorphism.

<u>Proof</u>. In particular, $w\alpha(x)=v\beta(x)$ for every x. Statement follows by 2.4.

2.8. <u>Lemma</u>. Let $k_1,\dots,k_n$ be natural numbers, d their greatest common divisor. Then there is an m_0 such that for every $m\geqq m_0$, the equation

$$x_1k_1+\dots+x_nk_n=m\cdot d$$

has a solution with natural

<u>Proof</u>. See, e.g.[2], p.25.

2.9. <u>Theorem.</u> Let $\mathcal{K}$ be a primitive subclass of $I(1,1)$. Let there be an algebra $(X;\alpha,\beta)$ in $\mathcal{K}$ without proper endomorphisms with $|X| > 4$. Then there is a $k \geq 3$ such that $P_k \subseteq \mathcal{K}$.

<u>Proof.</u> Let $\mathcal{K}$ be determined by equations

$$(1)\qquad (\alpha\beta)^{k_i+n_i}(x) = (\alpha\beta)^{k_i}(x) \qquad (i \in I_1),$$

$$(2)\qquad (\beta\alpha)^{k_i+n_i}(x) = (\beta\alpha)^{k_i}(x) \qquad (i \in I_2),$$

$$(3)\qquad \alpha(\beta\alpha)^{k_i+n_i}(x) = \alpha(\beta\alpha)^{k_i}(x) \qquad (i \in I_3),$$

$$(4)\qquad \beta(\alpha\beta)^{k_i+n_i}(x) = \beta(\alpha\beta)^{k_i}(x) \qquad (i \in I_4).$$

(By 2.4 and 2.7, any of the equations determining $\mathcal{K}$ is of some of these forms.)

Put $l_i = k_i$ for $i \in I_1$, $l_i = k_i + 1$ for $i \in I_2 \cup I_3 \cup I_4$. We obtain

$$(\alpha\beta)^{l_i+n_i}(x) = (\alpha\beta)^{l_i}(x) \qquad (i \in I_1 \cup \ldots \cup I_4),$$

and, consequently, for arbitrary natural numbers x_i:

$$(\alpha\beta)^{l_i+n_i x_i}(x) = (\alpha\beta)^{l_i}(x).$$

If I is finite, $I \subseteq I_1 \cup \ldots \cup I_4$, $l = \sum_I l_i$, we have

$$(5)\qquad (\alpha\beta)^{l+\sum_I x_i n_i}(x) = (\alpha\beta)^{l}(x).$$

By 2.8, there exist natural numbers m, x_i, x_i' $(i \in I)$ such that $\sum_I x_i n_i = m$, $\sum_I x_i' n_i = m + d$, where · is the greatest common divisor of n_i $(i \in I)$. By (5),

$$(\alpha\beta)^{l+m+d}(x) = (\alpha\beta)^{l+m}(x).$$

Since I was arbitrary finite, we see that there exist a natural number k dividing all the k_i $(i \in I_1 \cup \dots \cup I_4)$ and a natural number n such that
$$(\alpha\beta)^{n+k}(x) = (\alpha\beta)^{n}(x) .$$
By 2.2 and 2.6, $k \geqq 3$. Now, we see that $P_k \subseteq \mathcal{K}$, since all the equalities (1) - (4) are consequences of $\alpha(\beta\alpha)^{k} = \alpha$ and $\beta(\alpha\beta)^{k} = \beta$. (For (1) and (2), this holds only under the assumption of $k_i > 0$ for $i \in I_1 \cup I_2$. This, however, follows by 2.3.)

2.10. Theorem. Let $\mathcal{K}$ be a primitive subclass of $I(1,1)$. Then the following statements are equivalent:

(1) There is a $k \geqq 3$ with $P_k \subseteq \mathcal{K}$.

(2) There is a rigid algebra of a cardinality at least 5 in $\mathcal{K}$.

(3) For every cardinal m there is a rigid algebra of a cardinality greater or equal than m in $\mathcal{K}$.

(4) There is an algebra in $\mathcal{K}$ such that its semigroup of endomorphisms is a non-trivial group which is not isomorphic to the cyclic group of the order 2.

(5) For every monoid S there is an algebra in $\mathcal{K}$ such that its semigroup of endomorphisms is isomorphic to S.

(6) $\mathcal{K}$ is binding.

(7) $\mathcal{K}$ is strongly binding.

Proof. By 1.6, (1) $\Longrightarrow$ (7). Evidently (7) $\Longrightarrow$ (6) $\Longrightarrow$ (5) $\Longrightarrow$ (4), (6) $\Longrightarrow$ (3) $\Longrightarrow$ (2). By 2.9, (2) $\Longrightarrow$ (1). It remains to prove that non (1) $\Longrightarrow$ non(4).

If (1) does not hold, an algebra $(X; \alpha, \beta)$ with a non-trivial group of endomorphisms must have by 2.9 a cardinality $2, 3$ or 4. Since $(X; \alpha, \beta)$ has no proper endomorphisms, we have neither α = identity nor β = identity and hence $\alpha(x_0) = x_1 \neq x_0$ for some x_0. $\beta(x_1) = x_1$ by 2.1, $\beta(x_1) \neq x_0$ by 2.2 (for $|X| = 2$, this algebra would be rigid). Put $\beta(x_1) = x_2$. $\alpha(x_2)$ is neither x_2 (by 2.1), nor x_1 (by 2.2), nor x_0 (since $\alpha^2(x_2) = \alpha(x_2)$). Put $\alpha(x_2) = x_3$. Similarly, $\beta(x_3)$ is inequal x_1, x_2, x_3 and hence $\beta(x_3) = x_0$. Thus, $(X; \alpha, \beta)$ is determined and we see that its endomorphism semigroup is the cyclic group of the order 2.

2.11. Theorem. Minimal binding primitive subclasses of $I(1,1)$ are exactly the P_k where either k is an odd prime or $k = 4$.

Proof. Immediately by 2.9 and 2.10 and by the fact that $\alpha(\beta\alpha)^k = \alpha$ implies $\alpha(\beta\alpha)^{nk} = \alpha$.

§ 3. Cardinalities of rigid algebras in primitive subclasses of $I(1,1)$.

In the whole paragraph, the trivial rigid algebras of cardinalities 1 and 2 are ignored.

3.1. Lemma. Let $k \geq 5$. For every $m \geq 2k+1$ there is a rigid algebra $(X; \alpha, \beta)$ in $I(1,1)$ satisfying

$$(\alpha\beta)^k\alpha = \alpha, \quad (\beta\alpha)^k\beta = \beta$$

with $|X| = m$.

If $k = 4$, then there are such algebras for $9 \leq m \leq 15$ and for $m \geq 18$, if $k = 3$, then there are such algebras for $7 \leqq n \leqq 8$ and for $n \geqq 15$.

Proof Let $M \subseteqq k \times k$ (natural number n is treated as the set of all natural numbers less than n), $a \notin 2k \cup M$. Put

$A_k(n, M) = ((2k) \times n \cup M \times (n-1) \cup \{a\} \times (n-1); \alpha, \beta)$,

where $\alpha(2i, r) = (2i+1, r)$, $\beta(2i, r) = (2i, r)$,

$\alpha(2i+1, r) = (2i+1, r)$, $\beta(2i+1, r) = (2i+2, r)$,

$\alpha(a, r) = (1, r+1)$, $\beta(a, r) = (0, r)$, $\alpha(i, j, r) =$

$= (2i+1, r)$, $\beta(i, j, r) = (2j, r+1)$

($+$ designates the addition $mod\, 2k$ unless otherwise stated).

The following two statements are evident:

I. If $\alpha(x) = (i, r)$ and $\beta(x) = (j, r)$ then $i - j = 1$ or $j - i = 1$.

II. If $f(i_0, r) = (j_0, s)$ for a homomorphism f, then $f(i, r) =$ $= (i + j_0 - i_0, s)$ and, consequently, $f(C_r) = C_s$, where $C_r = 2k \times \{r\}$.

We shall prove that $A_k(n, M)$ with $n \geqq 2$ is rigid, whenever $(0,3) \in M$ and $k \geqq 4$ or $\{(0,0), (0,2)\} \subseteqq$ $\subseteqq M$ and $k = 3$.

Let $f: A_k(n, m) \longrightarrow A_k(n, M)$ be a homomorphism. If $f(a, r) = (2i_0, s)$, we obtain $f(0, r) = (2i_0, s)$, $f(1, r+1) =$ $= (2i_0 + 1, s)$ and hence $\alpha f(0,3,r) = f\alpha(0,3,r) = f(1,r) =$ $= (2i_0 + 1, s)$ (by II), while $\beta f(0,3,r) = f\beta(0,3,r) = f(6, r+1) =$ $= (2i_0 + 6, s)$ in a contradiction with I; if $k = 3$, we obtain a contradiction considering $\alpha f(0,2,r)$ and $\beta f(0,2,r)$. If $f(a, r) = (2i_0 + 1, s)$, we have $f(0, r) = (2i_0 + 2, s)$, $f(1, r+1) = (2i_0 + 1, s)$ and we obtain again a contradiction considering the images of $(0,3,k)$ ($(0,0,k)$ for $k=3$) under f and βf. If $f(a,k)=(i,j,s)$, we obtain easily by II $f(C_k)=C_{s+1}$ and $f(C_{k+1})=C_s$ and, consequently, $f(p,q,k)=(a,s)$ for any $(p,q)\in$ $\in M$. This yields an immediate contradiction in the case of $|M|\geq 2$. If $|M|=1$, we have $k\geq 4$ and $M=\{(0,3)\}$. Then, $(0,s)=\beta(a,s)=f\beta(0,3,k)=$ $=f(6,k+1)$. On the other hand, $f(a,k)=(0,3,s)$ and hence $f(1,k+1)=(1,s)$ and (by II) $f(6,k+1)=(6,s)$ - a contradiction.

Thus, $f(a,k)=(a,s(k))$. Put $w=\beta(\alpha\beta)^{k-1}$. We have $\beta f(a,k+1)=f(0,k+1)=f(w(1,k+1)=wf\alpha(a,k)=$ $=w\alpha(a,s(k))=w(1,s(k)+1)=(0,s(k)+1)$ and $\beta f(a,k+1)=$ $=(0,s(k+1))$. Thus $s(k+1)=s(k)+1$. Now, we see easily that $s(k)=k$ for any k, so that $f(a,k)=(a,k)$ for any k. Consequently, using β and II, we obtain $f(i,k)=$ $=(i,k)$ for any i,k and finally, using both α and β, we obtain $f(i,j,k)=(i,j,k)$ for any i,j,k.

Thus we obtained for $k\geq 4$ algebras of cardinalities beginning with $4k+2$, for $k=3$ rigid algebras of cardinalities beginning with 15 with the exception of 23. Such an algebra with cardinality 23 may be constructed as follows: Put $A=A_3(2,3\times 3)\cup\{b\}$ and define $\alpha(b)=(3,0)$, $\beta(b)=(0,0)$. The proof of rigidity of A is analogous to the previous one, we must only prove first that $f(a,0)\neq b$. If $f(a,0)=b$, we have $f(0,0)=\beta f(a,0)=(0,0)$ and hence $f(i,0)=$ $=(i,0)$, $f(1,1)=\alpha f(a,0)=(3,0)$ and $f(i,1)=$

$=(i+2,0)$. Thus, $\alpha f(0,1,0)=f(1,0)=(1,0)$, $\beta f(0,1,0)=$ $=f(2,1)=(4,0)$ in a contradiction with I.

Now, let $M \subseteq k \times k$ be such that

1) $(i,j)\in M \Longrightarrow i \neq j,\ i-j \not\equiv 1 \ (\mathrm{mod}\ k)$,

2) $(0,1)\in M,\ (k-1,0)\notin M$,

3) $(i,i+1)\in M,\ 0\leq j<i, \Longrightarrow (j,j+1)\in M$.

Put $A_k(M)=(2k\cup M;\alpha,\beta)$, where $\alpha(2i)=2i+1=$ $=\alpha(2i+1)$, $\beta(2i+1)=2i+2$, $\beta(2i)=2i$, $\alpha(i,j)=2j+1$, $\beta(i,j)=2i$.

We have $(\alpha\beta)^2(x)=\alpha(x)$ iff $x=(i,i+1)$. Thus, $f(0,1)=(i_0,i_0+1)$ for some $i_0<k-1$. Consequently, $f(i)=2i_0+1$. Thus, $\alpha f(i,i+1)=$ $=f(2i+3)=2(i+i_0+1)+1$, $\beta f(i,i+1)=f(2i)=2(i+i_0)$. The unique element with these images under α and β would be $(i+i_0,i+i_0+1)$ (here, the addition is $\mathrm{mod}\ k$), if it were in M. Let j be the first natural number with $(j,j+1)\notin M$ (see 2)). If $i_0\neq 0$, $x=$ $=(j-i_0,j-i_0+1)$ is in M. We have $\alpha f(x)=2(j+1)+1$, $\beta f(x)=2j$. But there is no element with these images under α and β in $A_k(M)$. Thus, $f(0,1)=(0,1)$, and $f(i)=i$ and $f(i,j)=(i,j)$.

By 1),2),3), M can have any cardinality between 1 and k^2-2k-1. Thus, we obtained for $k=3$ algebras with cardinalities 7 and 8, for $k=4$ algebras of cardinalities between 9 and 15, for $k\geq 5$ algebras of cardinalities between $2k+1$ and k^2-1 (and k^2-1 is now greater than $4k+1$).

3.2. Lemma. Let $k \geq 3$. For every $n \geq 2k+1$ there is a rigid algebra $(X; \alpha, \beta)$ in $I(1,1)$ satisfying

$$(\alpha\beta)^k\alpha = \alpha, \quad (\beta\alpha)^{k+1}\beta = \beta\alpha\beta$$

with $|X| = n$.

Proof. According to 3.1 it suffices to find for $k = 3$ rigid algebras of cardinalities between 9 and 14, for $k = 4$ rigid algebras of cardinalities 16 and 17.

Put $X(j) = 6 \cup j \times 2 \cup \{a\}$, where $a \notin 6 \cup (j \times 2)$, $j = 1, 2, 3$. Define operations α, β on $X(j)$ by

$$\alpha(2i) = \alpha(2i+1) = 2i+1, \; \beta(2i) = 2i, \; \beta(2i+1) = 2i+2,$$

$$\alpha(i,0) = 2i+1, \; \beta(i,0) = \beta(i,1) = (i,1), \; \alpha(i,1) = 2i-1, \; \alpha(a) = 3, \; \beta(a) = (0,1).$$

We have $\alpha(x) = (\alpha\beta)^2(x)$ iff $x = (i,0)$. Thus, $f(i,0) = (j,0)$ and, consequently, $f(i,1) = (j,1)$. We have further $\alpha\beta\alpha(a) = \alpha\beta(a)$, so that $f(a) \in 6 \cup \{a\}$. If $f(a) \in 6$, then $f(0,1) \in 6$ - a contradiction. Thus, $f(a) = a$ and we see now easily that f = identity. Thus we obtained rigid algebras of cardinalities 9,11,13. Rigid algebras of cardinalities 12 and 14 are obtained joining a new element b to $X(j)$. $(j = 2, 3)$ and defining $\alpha(b) = 5$, $\beta(b) = (1,1)$.

Now, add to $A_3(\{(0,1), (1,2)\})$ (see proof of 3.1) new distinct elements a, b and put $\alpha(a) = 1$, $\beta(a) = \beta(b) = b$, $\alpha(b) = 5$. The elements $(i, i+1)$ only satisfy $\beta(x) = (\beta\alpha)^2(x)$. If $f(0,1) = (1,2)$ for a homomorphism f, we obtain easily a contradiction considering $f(1,2)$. Thus, $f(0,1) = (0,1)$, $f(1,2) = (1,2)$ and

$f(i) = i$. We have $\alpha f(a) = f\alpha(a) = 1$ and hence $f(a)$ is either 0 or 1 or a; since $\alpha(a) = (\alpha\beta)^2(a)$, we have $f(a) = a$ and, consequently, $f(b) = f(\beta a) = b$. We obtained a rigid algebra of cardinality 10.

In order to obtain for $k = 4$ algebras with cardinalities 16 and 17, add to $A_4(M_i)$ $(i = 0, 1)$, where $M_0 = \{(0,1), (1,2), (0,2), (1,3), (2,0), (3,1)\}$, $M_1 = M_0 \cup \{(2,3)\}$, new elements a, b and define $\alpha(a) = 1$, $\beta(a) = \beta(b) = b$, $\alpha(b) = 7$.

The proof that these two algebras are rigid is quite analogous to the proof that $A_4(M_i)$ is rigid; we must only prove first that $f(0,1) \neq a$.

If $f(0,1) = a$, we have $f(0) = f\beta(0,1) = \beta(a) = b$, $f(1) = f\alpha(0) = \alpha(b) = 7$, so that $f(0) = 6$ - a contradiction. We obtain again $f(i, i+1) = (i, i+1)$, $f(i) = i$, $f(i, i+2) = (i, i+2)$. Consequently, $\alpha f(a) = 1$ and, therefore, considering that $(\alpha\beta)^2(a) = \alpha(a)$, $f(a) = a$ and finally $f(b) = b$.

3.3. <u>Lemma.</u> Let $k = 6h$. Then there are rigid algebras with cardinalities 11 and 12 satisfying $(\alpha\beta)^k\alpha = \alpha$ and $(\beta\alpha)^k\beta = \beta$.

<u>Proof</u>. Put $C = 4 \times \{0\}$, $D = 6 \times \{1\}$, a, b be two elements not contained in $C \cup D$. Define operations on $C \cup D \cup \{a\}$ ($C \cup D \cup \{a, b\}$ respectively) by $\alpha(2i, j) = (2i+1, j)$, $\beta(2i, j) = (2i, j)$, $\alpha(2i+1, j) = (2i+1, j)$, $\beta(2i+1, j) = (2i+2, j)$, $\alpha(a) = (1, 0)$, $\alpha(b) = (1, 1)$, $\beta(a) = (0, 1)$, $\beta(b) = (0, 0)$

(for $j = 0$ a ddition $mod\ 4$,for $j = 1$ $mod\ 6$).

It is easy to see that for a homomorphism f there is neither $f(C) \subseteq D$ nor $f(D) \subseteq C$. If $f(a) \neq a$, we obtain, however, some of these two cases. Thus $f(a) = a$ and now it is easy to see that f = identity.

3.4. Lemma. Let $(X; \alpha, \beta)$ be a rigid algebra such that the equation $(\alpha\beta)^{n+k}\alpha(x) = (\alpha\beta)^n\alpha(x)$ is satisfied for every $x \in X$, let $|X| \geq 3$. Then there is a cycle of the length $2d$ in X, where d is a divisor of k, $d > 1$. By 2.1 and 2.2, of course, there is no cycle of the length 0 or 2 in X .

Proof is trivial.

3.5. Notation. Let $\mathcal{K}$ be a binding primitive subclass of $I(1,1)$ determined by the equations (1) - (4) from the proof of Theorem 2.9. Denote by $d(\mathcal{K})$ the greatest common divisor of the numbers r_i . Let

$$d(\mathcal{K}) = 2^{a_2}3^{a_3}5^{a_5}\ldots$$

be its prime decomposition. If $a_2 \leq 1$, define $m(\mathcal{K})$ as the least odd prime p with $a_p \neq 0$, if $a_2 \geq 2$ and $a_3 = 0$ put $m(\mathcal{K}) = 4$, if $a_3 > 0$, put $m(\mathcal{K}) = 3$.

3.6. Theorem. Let $\mathcal{K}$ be a binding primitive subclass of $I(1,1)$. Then the cardinalities of (non-trivial) rigid algebras in $\mathcal{K}$ are exactly all the cardinal numbers greater or equal to $2m(\mathcal{K}) + 1$ with the following exceptions:

If $\mathcal{K} = P_d$, $d = 2^{a_2}3^{a_3}\ldots\ldots$ and

1. if $a_2 \leq 1$, $a_3 \neq 0 \neq a_5$, there are no rigid algebras with cardinalities 9 and 10,

2. if $a_2 = a_5 = 0,\ a_3 \neq 0$, there are no rigid algebras with cardinalities 9,10,...,14,

3. if $a_2 = 1,\ a_3 \neq 0 = a_5$, there are no rigid algebras with cardinalities 9 and 10,

4. if $a_2 = 2,\ a_3 = a_5 = a_7 = 0$, there are no rigid algebras with cardinalities 16 and 17,

5. if $a_2 > 2,\ a_3 = a_5 = a_7 = 0$, there is no rigid algebra with cardinality 16.

Proof. Since the embedding of $\mathcal{O}\!\mathcal{L}(1,1)$ into P_k described in 1.6 preserves all infinite cardinalities and since $\mathcal{O}\!\mathcal{L}(1,1)$ has a rigid algebra of every infinite cardinality (see [1] and [5]), it suffices to discuss the finite case.

The positive part of the statement follows easily by 3.1, 3.2 and 3.3.

Now, let $(X; \alpha, \beta)$ be a non-trivial rigid algebra in $\mathcal{K}$. By (the proof of 2.9 and) 3.4 and 2.6, X contains a cycle of a length at least $2m(\mathcal{K})$. The cycle alone is not rigid.

Now, let us discuss the exceptions:

1. By 3.4 and 2.6, a rigid algebra with cardinality 9 or 10 contains a cycle of the length 6. The remaining four (or three) points evidently cannot form a cycle. On the other hand, we cannot add three or four points to a cycle of the length 6 without allowing a nonidentical endomorphism.

2. The cardinalities 9, 10 and 11 are excluded by a consideration similar to that in 1 - there could be only

one cycle of the length 6 there. For the case of cardinality 12 it remains only algebra consisting of two cycles, which is not rigid. A rigid algebra of the cardinality 13 or 14 should contain two cycles of the length 6. It is easy to see that we cannot obtain a rigid algebra adding two points to such cycles, however.

3. A rigid algebra with the cardinality 9 or 10 must contain a cycle of the length 6, since it cannot (by 2.6) contain only cycles of the length 4. Contradiction is obtained by similar way as above.

4. By 2.6 (and 3.4), a rigid algebra with cardinality 16 or 17 contains one or two cycles of the length 8 (and no other cycles). We see easily that there is no such rigid algebra.

5. The situation is quite analogous to that of 4, with the exception that there is a possibility of a cycle of the length 16. This yields the rigid algebra with the cardinality 17.

References

[1] Z. HEDRLÍN, A. PULTR: On full embeddings of categories of algebras, Illinois J.of Math., 10(1966),392-406.

[2] OSTMANN: Additive Zahlentheorie I, Springer 1956.

[3] A. PULTR: Eine Bemerkung über volle Einbettungen von Kategorien von Algebren, Math.Annalen,178(1968), 78 - 82.

[4] J. SICHLER: Concerning minimal primitive classes of algebras containing any category of

algebras as a full subcategory, Comment. Math.Univ.Carolinae 9(1968),627-635.

[5] P. VOPĚNKA, A. PULTR, Z. HEDRLÍN: A rigid relation exists on any set, Comment.Math.Univ.Carolinae 6(1965),149-155.

Matematicko-fyzikální fakulta KU
Sokolovská 83, Praha 8-Karlín
Československo

(Oblatum 15.9.1969)