COLLOQUIUM MATHEMATICUM

VOL. XV 1966 FASC. 1

REMARKS ON ABSTRACT ALGEBRAS HAVING BASES WITH DIFFERENT NUMBER OF ELEMENTS

BY

W. NARKIEWICZ (WROCŁAW)

1. Let $\mathfrak{A} = (A, F)$ be an abstract algebra. By $A^{(n)}$ we shall denote the set of all algebraic operations of n variables in this algebra, and by $A^{(n,k)}$ the subset of $A^{(n)}$ consisting of all operations depending on at most k variables. By $\mathfrak{A}^{(n)}$ we shall denote the algebra $(A^{(n)}, F)$. (For the definitions of other notions used in this note see [3].)

By $S(\mathfrak{A})$ we shall denote the set of all natural numbers $n \geqslant 2$ for which the set $A^{(n)} \setminus A^{(n,n-1)}$ is not empty. The set $S(\mathfrak{A})$ was investigated by Urbanik [8] for idempotent algebras (i. e. for algebras without non-trivial algebraic operations of one variable). He gave a full description of possible sets $S(\mathfrak{A})$ in this case. Moreover, Płonka [6] proved that if there exists in $\mathfrak{A}$ a symmetric binary operation depending on both variables, and the algebra has no algebraic constants, then $S(\mathfrak{A}) = (2, 3, \ldots)$.

Marczewski [4], P 527, put forward the following conjecture:

(C_1) If the algebra $\mathfrak{A}$ has two bases of different cardinalities, then $S(\mathfrak{A}) = (2, 3, \ldots)$.

This conjecture is equivalent with the following one:

(C_2) If there exist rational integers $n > m \geqslant 1$ such that the algebras $\mathfrak{A}^{(m)}$ and $\mathfrak{A}^{(n)}$ are isomorphic, then $S(\mathfrak{A}) = (2, 3, \ldots)$.

Indeed, if (C_2) is true and an algebra $\mathfrak{A}$ has two bases of different cardinalities, then by theorem 1 of [1] it follows that for some $n > m \geqslant 1$ the algebras $\mathfrak{A}^{(m)}$ and $\mathfrak{A}^{(n)}$ are isomorphic, hence $S(\mathfrak{A}) = (2, 3, \ldots)$ by (C_2).

Assume now that (C_1) is true. If for some $n > m \geqslant 1$ the algebras $\mathfrak{A}^{(n)}$ and $\mathfrak{A}^{(m)}$ are isomorphic, then the algebra $\mathfrak{A}^{(n)}$ has two bases of different cardinalities and from (C_1) follows $S(\mathfrak{A}^{(n)}) = (2, 3, \ldots)$. Now it remains to observe that $S(\mathfrak{A}^{(n)}) \subset S(\mathfrak{A})$, and so $S(\mathfrak{A}) = (2, 3, \ldots)$.

(Note that in general the sets $S(\mathfrak{A})$ and $S(\mathfrak{A}^{(n)})$ can be different, e. g. when $\mathfrak{A}$ is idempotent and $n = 1$.)

The conjecture can also be stated without use of algebraic concepts:

(C_3) Let X be an arbitrary infinite set. Consider a one-to-one mapping between X^m and X^n ($m \neq n$). Suppose it is defined by

$$
\begin{aligned}
y_i &= f_i(x_1, \ldots, x_n) \quad (i = 1, 2, \ldots, m), \\
x_j &= g_j(y_1, \ldots, y_m) \quad (j = 1, 2, \ldots, n).
\end{aligned} \tag{1}
$$

Let $k \geqslant 2$ be a given rational integer. Then among the superpositions of $f_1, \ldots, f_m, g_1, \ldots, g_n$ and the trivial operations there is a function depending on exactly k variables.

(The equivalence of (C_2) and (C_3) follows from theorem 2 in [1]. Compare also [2] and [7].)

The purpose of this note is to give some partial results concerning this conjecture. We prove (C_2) in the cases $m = 1$ and $m = 2$, and show that $2 \in S(\mathfrak{A})$ without restriction on m. We shall work actually under less stringent conditions than the hypothesis in (C_2) as we assume merely that $\mathfrak{A}^{(n)}$ has a generating system (not necessarily a basis) of m elements.

It should be noted that there exist algebras having bases of m and n elements ($m \neq n$) such that $\boldsymbol{A}^{(1)}$ consists of the trivial operation $e(x) = x$ only. Indeed, let X be an arbitrary infinite set and consider a one-to-one mapping between X^m and X^n which acts trivially on the diagonals, i. e. transforms $(x, x, \ldots, x, x) \in X^m$ in $(x, x, \ldots, x, x) \in X^n$. Suppose that mapping is defined by (1) and take $\boldsymbol{F} = (f_1, \ldots, f_m, g_1, \ldots, g_n)$. Let $\mathfrak{A} = (X, \boldsymbol{F})$. Then the algebra $(\boldsymbol{A}^{(n)}, \boldsymbol{F})$ has bases of m and n elements, and obviously all algebraic operations of one variable are trivial.

2. Suppose $n \geqslant 2$, and $\mathfrak{A}^{(n)}$ has a generating system consisting of $m < n$ elements. Then there exist $f_1, \ldots, f_m \in \boldsymbol{A}^{(n)}$ and $g_1, \ldots, g_n \in \boldsymbol{A}^{(m)}$ such that

$$
x_j = g_j\big(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)\big) \tag{2}
$$

holds for $j = 1, 2, \ldots, n$. (See e. g. [1], th. 2, [2], [7].)

THEOREM I. *Assume that $n \geqslant 2$ and $\mathfrak{A}^{(n)}$ has m generators with $m < n$. Let $f_1, \ldots, f_m$ be algebraic operations satisfying* (2) *with suitable $g_1, \ldots, g_n \in \boldsymbol{A}^{(m)}$. Then there are at least $2^n - 2^m$ substitutions*

$$
I = \begin{pmatrix} 1, & 2, & \ldots, & n \\ a_1, & a_2, & \ldots, & a_n \end{pmatrix} \quad (1 \leqslant a_k \leqslant 2,\ k = 1, 2, \ldots, n)
$$

such that not all operations $f_i(I) = f_i(x_{a_1}, \ldots, x_{a_n})$ $(i = 1, 2, \ldots, m)$ depend on at most one variable.

COROLLARY 1. *If an algebra has no algebraic operations depending on exactly two variables, then every basis in this algebra has the same cardinal number.*

(Note that if an algebra has no algebraic operations depending on exactly two variables, and has only a finite number of algebraic operations depending on exactly one variable, then this corollary follows at once from a theorem of B. Jónsson and A. Tarski (see [2]).)

COROLLARY 2. *If $\mathfrak{A}$ is an idempotent algebra such that the algebra $\mathfrak{A}^{(n)}$ has a generating system consisting of $m < n$ elements, then $S(\mathfrak{A}) = (2, 3, \ldots)$.*

THEOREM II. *The conjecture* (C_2) *holds for $m = 1$ and $m = 2$.*

COROLLARY 3. *Under the assumptions of theorem* I *with $m = 3$ one has $3 \in S(\mathfrak{A})$.*

3. Proofs.

LEMMA 1. *If the algebra $\mathfrak{A}^{(n)}$ has a generating system consisting of m elements, then the algebra $\mathfrak{A}^{(2n-m)}$ has also a generating system consisting of m elements.*

(In the case when this generating system is a basis this lemma is a direct consequence from the fact that the powers of all bases in an algebra form an arithmetical progression. See [1], [3], [7]).

Proof. Let $[h_1, \ldots, h_r]$ denote the subalgebra of $\mathfrak{A}^{(2n-m)}$ generated by $h_1, \ldots, h_r$. As $[f_1, \ldots, f_m] = [x_1, \ldots, x_n]$, we have

$$\mathfrak{A}^{(2n-m)} = [x_1, \ldots, x_{2n-m}] = [f_1, \ldots, f_m, x_{n+1}, \ldots, x_{2n-m}]$$
$$= [f_1(f_1, \ldots, f_m, x_{n+1}, \ldots, x_{2n-m}), \ldots, f_m(f_1, \ldots, f_m, x_{n+1}, \ldots, x_{2n-m})].$$

Proof of theorem I. Let S be the set of all substitutions I such that $f_i(I)$ depends on at most one variable for $i = 1, 2, \ldots, m$. For $I \in S$ there is $f_i(I) = \hat{f}_i(x_{j_i(I)})$, where $\hat{f}_i(x) = f_i(x, x, \ldots, x)$ and $j_i(I) = 1$ or 2. Let T be the set of all m-tuples $(t_1, \ldots, t_m)$ with $1 \leqslant t_i \leqslant 2$.

Consider now the mapping $\beta\colon S \to T$ defined by

$$\beta(I) = \big(j_1(I), \ldots, j_m(I)\big).$$

Observe that from $\beta(I_1) = \beta(I_2)$ follows $I_1 = I_2$. Indeed, if

$$I_1 = \begin{pmatrix} 1, & 2, & \ldots, & n \\ i_1, & i_2, & \ldots, & i_n \end{pmatrix} \quad \text{and} \quad I_2 = \begin{pmatrix} 1, & 2, & \ldots, & n \\ j_1, & j_2, & \ldots, & j_n \end{pmatrix},$$

then

$$x_{i_k} = g_k\big(f_1(I_1), \ldots, f_m(I_1)\big) = g_k\big(f_1(I_2), \ldots, f_m(I_2)\big) = x_{j_k},$$

hence $i_k = j_k$ for $k = 1, 2, \ldots, m$ and so $I_1 = I_2$. It follows that the set S contains at most as many elements as the set T. Consequently, there are at most 2^m substitutions in S and the theorem follows.

Proof of corollary 1. As $2^n - 2^m$ is positive, it follows the existence of I such that some operation $f_i(I)$ depends on exactly two variables.

Proof of corollary 2. By a theorem of K. Urbanik (see [8]) and using the just proved theorem, it follows that in this case the set $S(\mathfrak{A})$ is of one of the following forms:

(i) $S(\mathfrak{A}) = (2, 3, \ldots)$. In this case there is nothing to prove.

(ii) $S(\mathfrak{A}) = (2, 3, \ldots, R)$ with some R, and $\mathfrak{A}$ being a diagonal algebra (see [5] for definition and properties). But in a diagonal algebra all minimal generating systems have the same cardinality, which contradicts our assumption.

(iii) $S(\mathfrak{A}) = (2, 3, \ldots, R) \cup (R'+1, R'+2, \ldots)$ and $\mathfrak{A}$ being of the form $\mathfrak{A} = (A, \{d\} \cup F)$, where $(A, \{d\})$ is a diagonal algebra of dimension R and F is a set of operations such that the set of all algebraic operations of R variables of $(A, \{d\})$ coincides with $A^{(R)}$. From the properties of diagonal algebras it follows easily that all bases in $\mathfrak{A}^{(R)}$ have the cardinality R and no set of less than R elements can generate $\mathfrak{A}^{(R)}$, contrary to our assumption. The corollary is thus proved.

LEMMA 2. *If the algebra $\mathfrak{A}^{(n)}$ $(n \neq 0, 1)$ has a system of generators consisting of one element, then $(2, 3, \ldots, n) \subset S(\mathfrak{A})$.*

Proof. Here $m = 1$, and so we have

$$x_i = g_i\big(f_1(x_1, \ldots, x_n)\big) \qquad (i = 1, 2, \ldots, n)$$

with suitable $f_1 \in A^{(n)}$, $g_1, \ldots, g_n \in A^{(1)}$.

Let $F_k(x_1, \ldots, x_k) = f_1(x_1, \ldots, x_k, x_k, \ldots, x_k)$ for $k = 1, 2, \ldots, n$. The operation F_k depends on k variables, because for $i = 1, 2, \ldots, k$

$$x_i = g_i\big(F_k(x_1, \ldots, x_k)\big).$$

and so the lemma is proved.

To prove the theorem in the case $m = 1$ it is now sufficient to observe that if $\mathfrak{A}^{(n)}$ has a system of generators consisting of one element, then by repeated application of lemma 1 one can obtain the existence of arbitrary large N such that $\mathfrak{A}^{(N)}$ has a system of generators consisting of one element, and the result follows by lemma 2.

LEMMA 3. *If the operations $g_1, g_2, \ldots, g_n$ satisfying* (2) *with $m < n$ depend on at most one variable, then $S(\mathfrak{A}) = (2, 3, \ldots)$.*

Proof. Suppose $g_i(x_1, \ldots, x_m)$ depends on the variable x_{k_i} only. As $n > m$, there exist $i \neq j$ such that $k_i = k_j$. Then

$$x_i = \hat{g}_i\big(f_{k_i}(x_1, \ldots, x_n)\big),$$
$$x_j = \hat{g}_j\big(f_{k_i}(x_1, \ldots, x_n)\big), \quad \text{where} \quad \hat{g}_a(x) = g_a(x, x, \ldots, x).$$

If now $F(x, y) = f_{k_i}(x, \ldots, x, y, x, \ldots, x)$, where the variable y is substituted on the j-th place, then the operation $F(x, y)$ generates the algebra $\mathfrak{A}^{(2)}$ and the lemma follows by the just proved part of our theorem.

LEMMA 4. *Suppose the operation* $f(x_1, \ldots, x_k) \in A^{(k)}$ *depends on* $s \neq 0,1$ *variables* $x_{i_1}, \ldots, x_{i_s}$. *Suppose the operations* $f_1, \ldots, f_t \in A^{(k)}$ *do not depend on* r *variables* $x_{i_1}, \ldots, x_{i_r}$. *Suppose, moreover, that there exist* $h_j(y_0, y_1, \ldots, y_t) \in A^{(t+1)}$ $(j = 1, 2, \ldots, r)$ *such that*

$$x_{i_j} = h_j\big(f(x_1, \ldots, x_k), f_1(x_1, \ldots, x_k), \ldots, f_t(x_1, \ldots, x_k)\big) \tag{3}$$

holds for $j = 1, 2, \ldots, r$.

Let $F_i(u_1, \ldots, u_{z_i})$ *be algebraic operations depending on all variables* $u_1, \ldots, u_{z_i}$ $(i = 1, 2, \ldots, r)$ *and suppose that the mapping of* A^{z_i} *in* A *induced by* F_i *is a mapping onto* A.

If now

$$G(u_1^{(1)}, \ldots, u_{z_1}^{(1)}, u_1^{(2)}, \ldots, u_{z_2}^{(2)}, \ldots, u_1^{(r)}, \ldots, u_{z_r}^{(r)}, x_{i_{r+1}}, \ldots, x_{i_s}) = f(x_1, \ldots, x_k)$$
$$\text{with } x_{i_j} = F_j(u_1^{(j)}, \ldots, u_{z_j}^{(j)}) \quad (j = 1, 2, \ldots, r),$$

then the operation G *depends on all variables* $u_1^{(1)}, \ldots, x_{i_s}$, *i. e. it is an operation depending on exactly* $z_1 + z_2 + \ldots + z_r + s - r$ *variables.*

Proof. Let $r+1 \leqslant p \leqslant s$. As f depends on the variable x_{i_p}, there exist $a_1, \ldots, a_k, b \in A$ such that

$$f(a_1, \ldots, a_k) \neq f(a_1, \ldots, a_{i_p-1}, b, a_{i_p+1}, \ldots, a_k).$$

There exist $c_1^{(1)}, \ldots, c_{z_r}^{(r)} \in A$ such that for $j = 1, 2, \ldots, r$ we have $F_j(c_1^{(j)}, \ldots, c_{z_j}^{(j)}) = a_{i_j}$. Then

$$\begin{aligned} G(c_1^{(1)}, \ldots, c_{z_r}^{(r)}, a_{i_{r+1}}, \ldots, a_{i_s}) &= f(a_1, \ldots, a_k) \\ &\neq f(a_1, \ldots, a_{i_p-1}, b, a_{i_p+1}, \ldots, a_k) \\ &= G(c_1^{(1)}, \ldots, c_{z_r}^{(r)}, a_{i_{r+1}}, \ldots, a_{i_p-1}, b, a_{i_p+1}, \ldots, a_{i_s}) \end{aligned}$$

consequently, G depends on the variable x_{j_p}.

Now put in (3)

$$x_{i_j} = F_j(u_1^{(j)}, \ldots, u_{z_j}^{(j)}) \quad \text{for} \quad j = 1, 2, \ldots, r.$$

It results

$$\begin{aligned} &F_j(u_1^{(j)}, \ldots, u_{z_j}^{(j)}) \\ &= h_j\big(G(u_1^{(1)}, \ldots, u_{z_r}^{(r)}, x_{i_{r+1}}, \ldots, x_{i_s}), f_1(x_1, \ldots, x_k), \ldots, f_t(x_1, \ldots, x_k)\big), \end{aligned}$$

because the operations $f_1, \ldots, f_t$ do not depend on x_{i_j} and so do not change after the just made substitution.

It follows that G depends on every variable $u_1^{(1)}, \ldots, u_{z_r}^{(r)}$, because otherwise the operations F_j would not depend on all variables. The lemma is thus proved.

Proof of theorem II. Thus $m = 2$. In view of lemma 1 it is sufficient to prove that $(2, 3, \ldots, n) \subset S(\mathfrak{A})$. Suppose that $2 \leqslant r \leqslant n$, and $r \notin S(\mathfrak{A})$, i. e. $A^{(r)} = A^{(r,r-1)}$. In view of theorem I we may assume that $r \neq 2$. From the same theorem we infer that there exists such a substitution

$$I = \begin{pmatrix} 1, \ldots, n \\ a_1, \ldots, a_n \end{pmatrix}$$

($1 \leqslant a_i \leqslant r$, and all numbers $1, 2, \ldots, r$ occur among $a_1, \ldots, a_n$) that one of operations $f_1(I)$, $f_2(I)$ depends on at least two variables. We may freely assume that $f_1(I)$ depends on at least as many variables as $f_2(I)$ does. We have

$$f_1(I) = \varphi_1(x_{i_1}, \ldots, x_{i_{r-1}}) \quad \text{and} \quad f_2(I) = \varphi_2(x_{j_1}, \ldots, x_{j_{r-1}})$$

with $1 \leqslant i_k, j_k \leqslant r$. Suppose that φ_1 depends on $x_{i_1}, \ldots, x_{i_s}$ and φ_2 depends on $x_{j_1}, \ldots, x_{j_t}$, where $t \leqslant s \leqslant r-1$.

In the sequence $i_1, \ldots, i_s, j_1, \ldots, j_t$ must occur all numbers from the set $(1, 2, \ldots, r)$, because $x_{a_i} = g_i(\varphi_1, \varphi_2)$ for $i = 1, 2, \ldots, n$. Consequently, φ_1 has to depend on at least $r-s$ variables on which φ_2 does not depend. Moreover, we may assume that at least one of the operations g_i depends on two variables, because otherwise we could apply lemma 3 to get the desired result. Let F be this operation. Now we can apply lemma 4 with $f = \varphi_1$, $f_1 = \varphi_2$, $h_i = g_i$, $F_1 = \ldots = F_{r-s} = F$. It follows the existence of an algebraic operation depending on exactly $2(r-s)+s-r+s = r$ variables, in contradiction to our assumption. Thus $A^{(r)} \neq A^{(r,r-1)}$, hence $r \in S(\mathfrak{A})$, and so the inclusion $(2, 3, \ldots, n) \subset S(\mathfrak{A})$ is proved. As observed before the theorem follows.

Proof of corollary 3. Suppose $m = 3$. If $3 \notin S(\mathfrak{A})$, then the operations $g_1, \ldots, g_n$ depend on at most two variables. Without restrictions we may assume that $n \geqslant 10$ by lemma 1. Suppose $g_i(x_1, x_2, x_3) = h_i(x_{k_i}, x_{l_i})$ for $i = 1, 2, \ldots, n$. There must be at least three indices i_1, i_2, i_3 such that $k_{i_1} = k_{i_2} = k_{i_3}$ and $l_{i_1} = l_{i_2} = l_{i_3}$. Then

$$x_{i_j} = h_{i_j}\big(f_{k_{i_1}}(x_1, \ldots, x_n), f_{l_{i_1}}(x_1, \ldots, x_n)\big) \qquad j = 1, 2, 3.$$

If we put here $x_i = x_{i_1}$ for all $i \neq i_2, i_3$, then we see that the operations F_1 and F_2 which result from $f_{k_{i_l}}$ resp. $f_{l_{i_l}}$ by this substitution form a set of generators for the algebra $\mathfrak{A}^{(3)}$, and from theorem II it results $S(\mathfrak{A}) = (2, 3, \ldots)$ contrary to our assumption that $3 \notin S(\mathfrak{A})$. Thus $3 \in S(\mathfrak{A})$, and the corollary is proved.

REFERENCES

[1] A. Goetz and C. Ryll-Nardzewski, *On bases of abstract algebras*, Bulletin de l'Académie Polonaise des Sciences, Sér. sci. math., astr. et phys., 8 (1960), p. 157-161.

[2] B. Jónsson and A. Tarski, *On two properties of free algebras*, Mathematica Scandinavica 9 (1961), p. 95-101.

[3] E. Marczewski, *Independence and homomorphisms in abstract algebras*, Fundamenta Mathematicae 50 (1961), p. 45-61.

[4] — *Independence in abstract algebras. Results and problems,* Colloquium Mathematicum 14 (1966), p. 169-188.

[5] J. Płonka, *Diagonal algebras*, Fundementa Mathematicae, in print.

[6] — *On the number of independent elements in finite abstract algebras having a binary operation,* Colloquium Mathematicum 14 (1966), p. 189-201.

[7] S. Świerczkowski, *On isomorphic free algebras*, Fundamenta Mathematicae 50 (1961), p. 35-44.

[8] K. Urbanik, *On algebraic operations in idempotent algebras*, Colloquium Mathematicum 13 (1965), p. 129-157.

INSTITUTE OF MATHEMATICS OF THE POLISH ACADEMY OF SCIENCES
INSTITUTE OF MATHEMATICS, WROCŁAW UNIVERSITY

Reçu par la Rédaction le 15. 3. 1965