Algebras which are independently generated by every n elements

by

S. Świerczkowski (Wrocław)

1. Preliminaries and results

By an algebra $\mathscr{A}$ we mean a pair $(A, \boldsymbol{F})$ where A is a set and $\boldsymbol{F}$ is a family of functions of finitely many variables defined on A and A-valued. $\boldsymbol{F}$ is called the *class of fundamental operations*. The *class of algebraic operations* is, by definition, the class of operations $\boldsymbol{A}$ generated by $\boldsymbol{F}$, i. e. the smallest class $\boldsymbol{A}$ such that $\boldsymbol{A}$ contains $\boldsymbol{F}$, all identity operations belong to $\boldsymbol{A}$ and $\boldsymbol{A}$ is closed with respect to composition. The subclass of all algebraic operations of n variables will be denoted by $\boldsymbol{A}^{(n)}$. The above definitions are given in a more detailed form in [3]; we use here the same notation.

Following E. Marczewski [3] we say that $N \subset A$ is a *set of independent elements* if, for each sequence of n different elements $a_1, \ldots, a_n \in N$ and for each pair of operations $f, g \in \boldsymbol{A}^{(n)}$, the equality

$$f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$$

implies that f and g are identical in $\mathscr{A}$.

We shall call the identity operations also *trivial operations*. More exactly: An operation $f(x_1, \ldots, x_k)$ is called *trivial* if, for a certain $l \leqslant k$, we have $f(x_1, \ldots, x_k) = x_l$ for all values of $x_1, \ldots, x_k$. If all algebraic operations are trivial then the algebra will be called trivial. For $A = \{a_1, \ldots, a_n\}$ and $\boldsymbol{F} = \{f\}$ we shall write $(a_1, \ldots, a_n; f)$ instead of $(A, \boldsymbol{F})$. Two algebras, $(A, \boldsymbol{F}_1)$ and $(A, \boldsymbol{F}_2)$, having the same class of all algebraic operations will be treated here as identical.

We say that a set $B \subset A$ *generates* $\mathscr{A}$ if each $x \in A$ is the result of an algebraic operation applied to some elements in B. Let $\overline{\overline{S}}$ denote the cardinal of the set S. We then say that *the algebra is independently generated by every n elements* if each set $B \subset A$ satisfying $\overline{\overline{B}} = n$ is a set of independent elements and B generates $\mathscr{A}$. In this paper we show some properties of those algebras. The results were announced in paper [4].

THEOREM 1. *If all elements of an algebra $\mathcal{A}$ are independent and $\bar{\bar{A}} \neq 2$, then $\mathcal{A}$ is a trivial algebra. There exists a non-trivial two-element algebra $\mathcal{M}$ all elements of which are independent.*

The algebra $\mathcal{M}$ has been found by E. Marczewski. It is evident that all elements of a trivial algebra are independent. Hence, if the trivial algebra has n elements, we obtain an example of an algebra which is independently generated by every n elements. If $n > 3$, then there are no other algebras of this kind since we have

THEOREM 2. *Let $n > 3$. If $\mathcal{A}$ is an algebra such that $\bar{\bar{A}} \geqslant n$ and $\mathcal{A}$ is independently generated by every n elements, then $\mathcal{A}$ is the trivial algebra with n elements.*

The assumption $n > 3$ is essential in this theorem. For $n = 3$ we consider the following:

Let us put $\mathcal{A}_0 = (a, b, c, d; f_0)$ where $f_0 = f_0(x, y, z)$ is the operation which associates with every three distinct elements of the set $\{a, b, c, d\}$ the remaining one and satisfies identically

$$f_0(x, x, y) = f_0(x, y, x) = f_0(y, x, x) = y .$$

THEOREM 3. *The algebra $\mathcal{A}_0$ is independently generated by every three elements.*

THEOREM 4. *$\mathcal{A}_0$ is the unique algebra which is non-trivial, has at least three elements and is independently generated by every three elements.*

There exist non-trivial algebras which are independently generated by every two elements. An example is the algebra $\mathcal{M}$ considered in Theorem 1. Another kind of example gives the following theorem, which was communicated to me by A. M. Macbeath.

THEOREM 5. *Let K be a field, let A be the set of all elements of K and let $\boldsymbol{F}$ be the class of all operations $f(x_1, x_2) = \lambda x_1 + (1-\lambda)x_2$; $\lambda \in K$. Then the algebra $\mathcal{A} = (A, \boldsymbol{F})$ is independently generated by every two elements.*

It follows from this theorem that there is, for every number p^k (p prime, k natural), an algebra with p^k elements which is independently generated by every two elements. Also the converse of this result is true:

THEOREM 6. *If $\mathcal{A}$ is a finite algebra which is independently generated by every two elements, then $\bar{\bar{A}}$ is a power of a prime.*

In view of Theorems 5 and 6 (cf. also [5]) one might suspect that each algebra which is independently generated by every two elements is defined, as in Theorem 5, by a corresponding field. This, however, is not true and the simplest counter-example is the algebra $\mathcal{M}$ of Theorem 1.

For every set A there is a class of operations $\boldsymbol{F}$ such that $\mathcal{A} = (A, \boldsymbol{F})$ is an algebra which is independently generated by every element. To prove this we introduce in A a group addition so that A is an Abelian group. We associate with every $a \in A$ the operation $f_a(x) = a + x$ and we denote by $\boldsymbol{F}$ the class of all those operations. Then $\mathcal{A}$ is generated by every element. Moreover, every element is independent since f_a are the only operations of one variable.

2. Algebras with all elements independent

In this section we shall prove Theorem 1. Denote by n the cardinal of A. The theorem is trivial for $n = 1$. We assume therefore that $n \geqslant 3$ and we have to show that every algebraic operation $f(x_1, \ldots, x_k)$ is a trivial one. We consider the possibilities: $k < n$ and $k \geqslant n$ (the latter obviously only for finite n).

For $k < n$ it is convenient, for a further application, to derive the result from the weaker assumption $\bar{\bar{A}} \geqslant n$. So we first prove the following:

(α) *If $\bar{\bar{A}} \geqslant n$ and every n elements of $\mathcal{A}$ are independent, then $\boldsymbol{A}^{(k)}$ contains, for each $k < n$, only trivial operations.*

Proof of (α). Let $k < n$ and let $f \in \boldsymbol{A}^{(k)}$. Consider k different elements $a_1, \ldots, a_k \in A$. The elements $a_1, \ldots, a_k, a_{k+1} = f(a_1, \ldots, a_k)$ are obviously not independent. Thus they cannot be different, by $k+1 \leqslant n$, and we have

$$f(a_1, \ldots, a_k) = a_l \quad \text{for some} \quad l < k .$$

From the independence of the a_i it follows that we have identically $f(x_1, \ldots, x_k) = x_l$, so that f is a trivial operation. Hence (α) is proved.

Now let $k \geqslant n$, $f \in \boldsymbol{A}^{(k)}$ and let $a_1, \ldots, a_k \in A$. Suppose that the element $a_{k+1} = f(a_1, \ldots, a_k)$ is different from all a_i, $i \leqslant k$. Then, if r is the number of distinct elements $a_{i_1}, \ldots, a_{i_r}$ occuring in the sequence $\langle a_1, \ldots, a_k \rangle$, we infer that all $a_{i_1}, \ldots, a_{i_r}, a_{k+1}$ are different and thus independent. This is impossible since a_{k+1} is the result of an algebraic operation on $a_{i_1}, \ldots, a_{i_r}$. So

$$(*) \qquad f(a_1, \ldots, a_k) = a_u$$

for some $u \leqslant k$. Let $S = \{1, \ldots, k\}$ and let $\Delta(a_1, \ldots, a_k)$ be the subset of all $u \in S$ satisfying ($*$). We shall show that f is a trivial operation if we prove that there is a number u such that ($*$) holds for that u and for arbitrary $a_1, \ldots, a_k \in A$. Equivalently, we have to show that the intersection of all sets $\Delta(a_1, \ldots, a_k)$ is non-empty.

Suppose we have a one-to-one mapping of A onto itself. Let a' denote the image of a. It follows from the independence of all elements of $\mathcal{A}$ (cf. [3], sec. 2 (ii)) that ($*$) holds with the same numbers u for $a_1, \ldots, a_k$ and $a'_1, \ldots, a'_k$. Thus $\Delta(a_1, \ldots, a_k)$ depends only on the decomposition δ of the set of indices S in the disjoint sets $D_1, \ldots, D_m$ containing indices of equal a_i (so that $a_i = a_j$ if and only if i, j belong to the same D_l, whence $m \leqslant n = \overline{\overline{A}}$). Evidently $\Delta(a_1, \ldots, a_k)$ is one of those sets D_l and since it depends only on the decomposition δ, it will be denoted by $\varphi\delta$. We observe that every decomposition of S into not more than n subsets is realized by some sequence $\langle a_1, \ldots, a_k\rangle$.

DEFINITION. For any decompositions δ, δ' we write $\delta < \delta'$ if, for each set D_i of δ, there is a set D'_j of δ' which contains D_i.

Let us prove that $\delta < \delta'$ implies $\varphi\delta \subset \varphi\delta'$. Indeed, if $\delta < \delta'$ and $\langle a_1, \ldots, a_k\rangle$ is a sequence that determines the decomposition δ, then there is a mapping of A into itself such that the sequence $\langle a'_1, \ldots, a'_k\rangle$, which is the image of $\langle a_1, \ldots, a_k\rangle$, determines the decomposition δ'. From the independence of the elements of $\mathcal{A}$ it follows ([3], sec. 2, (ii)) that if $(*)$ holds for some u and $a_1, \ldots, a_k$, then it holds for the same u for $a'_1, \ldots, a'_k$. Thus $\varphi\delta \subset \varphi\delta'$.

We have to prove that the intersection of all $\varphi\delta$ is non-empty. This follows from the lemma

(β) *If we have a fixed number $n \geqslant 3$, S is a finite set, and to every decomposition δ of S in not more than n disjoint subsets corresponds a set $\varphi\delta$ of that decomposition so that $\delta < \delta'$ implies $\varphi\delta \subset \varphi\delta'$, then the intersection of all $\varphi\delta$ is non-empty.*

Proof of (β). The assumption $n \geqslant 3$ means that the correspondence $\delta \to \varphi\delta$ is defined for all decompositions in not more than three subsets.

It is sufficient to verify that, for any δ', δ'' the set $\varphi\delta' \cap \varphi\delta''$ is also a $\varphi\delta$. We prove first that $\varphi\delta'$ and $\varphi\delta''$ are not disjoint. Consider the decompositions δ_1, δ_2

$$S = \varphi\delta' \cup B\,, \qquad S = \varphi\delta'' \cup C\,,$$

where B and C are uniquely determined. We have $\delta' < \delta_1$, $\delta'' < \delta_2$ and this implies $\varphi\delta_1 = \varphi\delta'$, $\varphi\delta_2 = \varphi\delta''$. Suppose that $\varphi\delta'$ and $\varphi\delta''$ are disjoint. Then the decomposition δ^*

$$S = \varphi\delta' \cup \varphi\delta'' \cup D$$

satisfies $\delta^* < \delta_1$, $\delta^* < \delta_2$. $\varphi\delta^*$ is contained in both $\varphi\delta_1$ and $\varphi\delta_2$, which contradicts $\varphi\delta_1 \cap \varphi\delta_2 = \varphi\delta' \cap \varphi\delta'' = \emptyset$ ($\emptyset$ is the empty set).

Now consider the decomposition δ defined by

$$S = (\varphi\delta' \cap \varphi\delta'') \cup (\varphi\delta' - \varphi\delta'') \cup B\,.$$

From $\delta < \delta_1$ follows $\varphi\delta \subset \varphi\delta_1 = \varphi\delta'$ and thus $\varphi\delta \neq B$. Since two sets $\varphi\delta, \varphi\delta''$ are never disjoint, we have $\varphi\delta = \varphi\delta' \cap \varphi\delta''$. This completes the proof of (β) and of the first part of Theorem 1.

Let $\mathcal{M} = (a, b; f)$ where $f = f(x, y, z)$ is the operation defined on $\{a, b\}$ so that identically

$$f(x, x, y) = f(x, y, x) = f(y, x, x) = x\,.$$

Hence f is non-trivial and thus the algebra $\mathcal{M}$ is non-trivial. All elements of $\mathcal{M}$ are independent, since, for any algebraic operations g, h of two variables, the equality $g(a, b) = h(a, b)$ implies $g(b, a) = h(b, a)$ because of symmetry and $g(x, x) = x = h(x, x)$ holds since there is no non-trivial operation of one variable in $\mathcal{M}$.

3. Algebras which have more than three independent generators

We shall now prove Theorem 2. The result follows by Theorem 1 if we verify that there are only n elements in A. If n is infinite, then, by (α), every operation is trivial and hence A contains only the n generators. If n is finite, then it is enough to prove that $A^{(n)}$ contains only trivial operations.

Let us suppose that there is in $A^{(n)}$ a non-trivial operation $f(x_1, \ldots, x_n)$. By (α), the operation on $n-1$ variables $f(x_1, x_2, x_2, x_4, \ldots, x_n)$ is trivial, whence it is identically equal to one of the variables $x_1, x_2, x_4, \ldots, x_n$. Certainly one of the two variables x_1, x_4 (we have $n \geqslant 4$) is not identically equal to $f(x_1, x_2, x_2, x_4, \ldots, x_n)$ and we may assume that it is the variable x_1, performing in the opposite case a suitable rearrangement of indices. Therefore, identically

$$f(x_1, x_2, x_2, x_4, \ldots, x_n) = x_2 \text{ or } x_4 \text{ or } \ldots \text{ or } x_n\,.$$

Let $a_1, \ldots, a_n \in A$ be distinct elements and let $a_{n+1} = f(a_1, \ldots, a_n)$. Since f is non-trivial and $a_1, \ldots, a_n$ are independent, we have $a_{n+1} \neq a_1, \ldots, a_n$. The elements $a_2, \ldots, a_{n+1}$, being different, generate the algebra. Hence, for a certain algebraic operation h, $a_1 = h(a_2, \ldots, a_{n+1})$, i. e.

$$a_1 = h\big(a_2, a_3, a_4, \ldots, f(a_1, a_2, a_3, \ldots, a_n)\big)\,.$$

Since all elements appearing in the above equality are independent, the equality holds identically, e. g. holds also if we put a_2 in place of a_3. Now $f(a_1, a_2, a_2, a_4, \ldots, a_n)$ is one of the elements $a_2, a_4, \ldots, a_n$ and so a_1 is the result of an algebraic operation on $a_2, a_4, \ldots, a_n$ in spite of the independence of $a_1, \ldots, a_n$. We have obtained a contradiction and we have proved the theorem.

4. The algebra $\mathcal{A}_0$

Fundamental properties. Let us prove Theorem 3. Since evidently $\mathcal{A}_0$ is generated by every three elements, we have to show that every three elements are independent. Let us denote by e_1, e_2, e_3 the three trivial operations in $A_0^{(3)}$ so that identically

$$e_1(x, y, z) = x\,, \qquad e_2(x, y, z) = y\,, \qquad e_3(x, y, z) = z\,.$$

It is easy to check that the class of operations $\Phi = \{f_0, e_1, e_2, e_3\}$ has the following property:

If $h_1, h_2, h_3 \in \Phi$, then the operation h defined by the formula

$$h(x, y, z) = f_0\big(h_1(x, y, z), h_2(x, y, z), h_3(x, y, z)\big)$$

also belongs to Φ.

This shows, by the definition of $A_0^{(3)}$ (cf. [3], sec. 1, (a)) that $A_0^{(3)} = \Phi$. Knowing $A_0^{(3)}$ we easily check that every three elements are independent.

Uniqueness of $\mathcal{A}_0$. We now proceed to prove Theorem 4. We assume that the algebra $\mathcal{A} = (A, \boldsymbol{A})$ is non-trivial, independently generated by every three elements and $\overline{\overline{A}} \geqslant 3$ (where $\boldsymbol{A}$ denotes the class of all algebraic operations). We first show that

(γ) *If $f \in \boldsymbol{A}^{(3)}$ is non-trivial, then identically*

$$f(x, x, y) = f(x, y, x) = f(y, x, x) = y .$$

Proof of (γ). Let a, b, c be independent generators of $\mathcal{A}$. If f is non-trivial, we have $f(a, b, c) \neq a, b, c$ and thus $a, b, f(a, b, c)$ generate $\mathcal{A}$. It follows that, for a certain algebraic operation $h(x, y, z)$,

$$c = h\big(a, b, f(a, b, c)\big) .$$

Since a, b, c are independent, this equation holds identically, e. g. also if a stands at the place of b. So $c = h\big(a, a, f(a, a, c)\big)$. Now $f(x, x, y)$ is, by (α), a trivial operation, whence $f(x, x, y) = x$ or y. But $f(a, a, c) = a$ gives $c = h(a, a, a)$, which is a contradiction. Thus we have $f(x, x, y) = y$. The other equalities in (γ) hold by symmetry.

Now let us show that $\mathcal{A}$ has exactly four elements. We have assumed $\overline{\overline{A}} \geqslant 3$. Since $\mathcal{A}$ is non-trivial and every three elements are independent, we have, by Theorem 1, $\overline{\overline{A}} > 3$. Let us suppose that there are at least five elements $a, b, c, d, e \in A$. Since a, b, c are generators, there are operations f, g such that

$$d = f(a, b, c), \quad e = g(a, b, c) .$$

Also c, d, e are generators; thus, for some operation h, $a = h(c, d, e)$ and we have

$$a = h\big(c, f(a, b, c), g(a, b, c)\big) .$$

Since this equality must hold identically, we have, writing a at the place of b, by (γ), $a = h(c, c, c)$. This is a contradiction and so $\overline{\overline{A}} = 4$.

From what we have shown it follows that we may assume that both algebras, $\mathcal{A}_0$ and $\mathcal{A}$, have the same set of elements $A_0 = A = \{a, b, c, d\}$. To complete the proof of our theorem it remains to prove that the operations are in both algebras the same, i. e. that $\boldsymbol{A}_0 = \boldsymbol{A}$.

Since a, b, c generate $\mathcal{A}$, we have, for a certain $f \in \boldsymbol{A}^{(3)}$, $d = f(a, b, c)$. Thus f is non-trivial and hence it associates with every three elements of A the remaining one. Since the equalities in (γ) hold, we infer that f coincides with the fundamental operation f_0 of $\mathcal{A}_0$. Consequently $\boldsymbol{A}_0$ is the class of operations generated by f and we have $\boldsymbol{A}_0 \subset \boldsymbol{A}$.

Given an operation $h \in \boldsymbol{A}^{(k)}$, we say that h depends on the variable x_i, where $1 \leqslant i \leqslant k$, if there is a sequence $\langle a_1, \ldots, a_i, \ldots, a_k \rangle$ of elements of A and an $a_i' \in A$ such that

$$h(a_1, \ldots, a_i, \ldots, a_k) \neq h(a_1, \ldots, a_i', \ldots, a_k) .$$

We have to show that $\boldsymbol{A} \subset \boldsymbol{A}_0$. We observe that if $h \in \boldsymbol{A}$, then h must depend on some variables, for if h takes a constant value, say $h = a$, then also $h(b, \ldots, b) = a$, contradicting the independence of a and b. We can even assume that h depends on every variable, for if $h(x_1, \ldots, x_k)$ does not depend on some of the variables, then, after a suitable rearrangement of indices if necessary, we have

$$h(x_1, \ldots, x_k) = g(x_1, \ldots, x_m), \qquad m < k ;$$

g depends on every variable and if $g \in \boldsymbol{A}_0$, then $h \in \boldsymbol{A}_0$.

The idea of our proof is now the following. To show that if $h \in \boldsymbol{A}^{(k)}$ depends on every variable, then $h \in \boldsymbol{A}_0^{(k)}$, it is enough to verify that there is at most one operation in $\boldsymbol{A}^{(k)}$ which depends on every variable, and, if there is one, then there is at least one which belongs to $\boldsymbol{A}_0^{(k)}$. This follows, by $\boldsymbol{A}_0 \subset \boldsymbol{A}$, from

(ε) *For any k, if there exists an operation $h \in \boldsymbol{A}^{(k)}$ which depends on every variable, then there is exactly one such operation and k is an odd integer.*

(η) *For every odd integer k, there exists an operation $h \in \boldsymbol{A}_0^{(k)}$ which depends on every variable.*

Since the proof of (η) is much simpler than the proof of (ε), we shall give it first.

Proof of (η). The assertion is trivial for $k = 1$. Suppose that, for some odd $k \geqslant 1$, there is an operation $h(x_1, \ldots, x_k)$ belonging to $\boldsymbol{A}_0^{(k)}$ and depending on every variable. Then the operation g defined by

$$g(x_1, \ldots, x_{k+2}) = f\big(h(x_1, \ldots, x_k), x_{k+1}, x_{k+2}\big)$$

belongs to $\boldsymbol{A}_0^{(k+2)}$. From $g(x_1, \ldots, x_k, x, x) = h(x_1, \ldots, x_k)$ we infer that g depends on each of the variables $x_1, \ldots, x_k$. Since, for a constant $u \in A$, the function $f(u, x, y)$ depends on each of the variables x, y, it follows that g depends also on x_{k+1} and x_{k+2}.

Proof of (ε). Since, by (α), every operation of not more than two variables is trivial, (ε) holds for $k = 1$ and $k = 2$. Let us show that (ε) holds for $k = 3$, i. e., that $f(x, y, z)$ is the only operation in $\boldsymbol{A}^{(3)}$ which depends on all variables. Suppose that $g(x,y,z)\in A^{(3)}$ depends on every variable. Hence g is a non-trivial operation and we must have $g(a,b,c)=d$, by the independence of a,b,c. So $g(a,b,c)=f(a,b,c)$ and, using again the independence of a,b,c, $g(x,y,z)=f(x,y,z)$.

Thus it remains to prove (ε) for $k>3$. Suppose that $h\in A^{(k)}$, $k>3$ and h depends on every variable. Since we have only four elements in A, the operation h is given by a system of operations of not more than four variables which are obtained from h by identifying some of the variables $x_1,\ldots,x_k$ so that not more than four different ones are left. Let us call those operations *derived* from h. If we show that each operation derived from h depends only on the given identification of the variables and not on h, then it is evident that h is unique. This proof will be given in two steps. First, in (ε_0), we show that each operation h_δ derived from h is determined by the system of operations of two variables derived from h_δ. Then, in (ε_1), we prove that the system of operations of two variables derived from h can be determined without knowing h.

We consider the family of all decompositions of the set of indices $S=\{1,\ldots,k\}$ in not more than four subsets. For each decomposition δ

$$S=X\cup Y\cup Z\cup U$$

(where some of the sets $X,\ldots,U$ may be empty) we identify those variables in $h(x_1,\ldots,x_k)$ which have indices belonging to the same set of the decomposition. We denote by x,y,z,u those variables x_i whose indices belong to the sets $X,\ldots,U$ respectively. Thus we obtain an operation $h_\delta(x,y,z,u)$, which is derived from h.

(ε_0) *The operation $h_\delta(x,y,z,u)$ is determined by the system of operations of two variables which are derived from h_δ.*

Proof of (ε_0). Our assertion is trivial if δ is a decomposition of S in two sets. If δ is a decomposition in three sets, then $h_\delta=h_\delta(x,y,z)$. If h_δ is not trivial, then $h_\delta=f$ since f is the only non-trivial algebraic operation of three variables. Consequently $h_\delta(x,x,y)=h_\delta(x,y,x)=h_\delta(y,x,x)=y$. If h_δ is trivial, then only two of these equalities holds and the remaining four are false. Moreover, we know h_δ if we know which of the equalities holds. Thus all the possible cases are distinguished by the behaviour of the operations of two variables derived from h_δ; we can determine h_δ by examining those operations.

Now suppose that δ is a decomposition of S in four sets. We have to consider an operation $h_\delta(x,y,z,u)$. Let us determine first $h_\delta(a,b,c,d)$. Suppose that $h_\delta(a,b,c,d)=d$. Then $h_\delta(a,b,c,f(a,b,c))=f(a,b,c)$ and, by the independence of a,b,c, we have $h_\delta(x,y,z,f(x,y,z))=f(x,y,z)$. Identifying any two of the variables x,y,z we easily obtain

$$h_\delta(x,x,y,y)=h_\delta(x,y,x,y)=h_\delta(y,x,x,y)=y\,.$$

Let us call an identification of some of the variables x,y,z,u *even* if it results in one of those which appear in brackets in the above equalities. Thus we infer that for any even identification of variables, $h_\delta(x,y,z,u)=u$. By symmetry, if we assume that $h_\delta(a,b,c,d)=c$, we shall find that, for every even identification of variables, $h_\delta(x,y,z,u)=z$ holds and it is similar for a and b instead of c,d. So we see that by examining the operations of two variables derived from h_δ (in fact only those which are derived by an even identification of variables) we can determine $h_\delta(a,b,c,d)$.

It remains to verify that also in the case when two of the arguments x,y,z,u are equal, h_δ can be determined. It is not difficult to see that we then have to find the value of an operation $h_{\bar\delta}$ of not more than three variables which is derived from h_δ. Since we know the operation of two variables derived from $h_{\bar\delta}$ (they are also derived from h_δ) we determine $h_{\bar\delta}$ so in the same way as we determined h_δ when it was assumed to be an operation of not more than three variables. Thus (ε_0) is proved.

Let Ω_h be the family of subsets of S which contains, for every decomposition $\delta\colon S=X\cup Y$, one of the two sets X, Y, namely

$$X \text{ if } h_\delta(x,y)=x,\qquad Y \text{ if } h_\delta(x,y)=y\,.$$

(Let us recall that in $\mathcal{A}$ every algebraic operation of two variables is trivial.)

Obviously

(o) $S\in\Omega_h$.

(i) *If $G\cup H=S$ and $G\cap H=\emptyset$, then exactly one of the sets G and H belongs to Ω_h.*

It is evident that Ω_h determines the system of operations of two variables derived from h. Thus, by (ε_0), h is completely determined by Ω_h. To show that h is unique it is enough to show that Ω_h is unique, i. e. that Ω_h is fully determined by the mere condition that h is operation of k variables which depends on every variable. This will be shown in (ε_1), but to prove (ε_1) we need some more properties of Ω_h. Assume that $G,H\in\Omega_h$, Let us prove

(ii) *If $G\cap H\neq\emptyset$ and $S=G\cup H$, then $G\cap H\in\Omega_h$.*

(iii) *If $G\cap H=\emptyset$, then $G\cup H\notin\Omega_h$.*

(iv) *If $G\subset H$, then $H-G\notin\Omega_h$.*

In the proofs of (ii), (iii) and (iv) we shall consider an operation $h_\delta(x,y,z)$ given by a decomposition $\delta\colon S=X\cup Y\cup Z$. The sets X,Y,Z will be defined in each case separately.

Proof of (ii). Assume $G\cap H\neq\emptyset$, $S=G\cup H$. Define $X=G-H$, $Y=G\cap H$, $Z=H-G$. Consider the operation $h_\delta(x,y,z)$. We have $X\cup Y$, $Z\cup Y\in\Omega_h$ and thus $h_\delta(x,x,y)=x$ and $h_\delta(x,y,y)=y$. Hence

h_δ is different from f and thus it is a trivial operation. Consequently $h_\delta(x,y,z)=y$. It follows that $h_\delta(x,y,x)=y$ and thus (ii).

Proof of (iii). Suppose that $G\cap H=\emptyset$. Let $X=G$, $Y=H$, $Z=S-(G\cup H)$. From $X,Y\in\Omega_h$ it follows $h_\delta(x,y,y)=x$, $h_\delta(x,y,x)=y$ and thus h_δ cannot be a trivial operation. Hence $h_\delta(x,y,z)=f(x,y,z)$ and we have $h_\delta(x,x,z)=z$. Thus $Z\in\Omega_h$ and consequently $G\cup H\notin\Omega_h$.

Proof of (iv). Let $G\subset H$. Define $X=G$, $Y=S-H$, $Z=H-G$. It follows from $X, X\cup Z\in\Omega_h$ that $h_\delta(x,y,y)=x=h_\delta(x,y,x)$. We see that h_δ is different from f. Thus it is a trivial operation satisfying $h_\delta(x,y,z)=x$. For $x=y$ we obtain $Z\notin\Omega_h$. This proves (iv).

We shall derive from (ε_0), (ii) and (iii) that

(v) *Every one-element subset of S belongs to Ω_h.*

Proof of (v). Without loss of generality it will be enough to prove that $\{1\}\in\Omega_h$. Since $h(x_1,\dots,x_\delta)$ depends on x_1, there are sequences $\langle a_1,\dots,a_k\rangle$, $\langle b_1,\dots,b_k\rangle$, $a_i,b_i\in A$ such that $a_i=b_i$ for $i\geqslant 2$ and

$$h(a_1,\dots,a_k)\neq h(b_1,\dots,b_k)\,.$$

Since obviously $a_1\neq b_1$, we can assume that $a_1=a$, $b_1=b$. Both sequences, $\langle a_1,\dots,a_k\rangle$, and $\langle b_1,\dots,b_k\rangle$, are composed of the elements a,b,c,d, and thus there are uniquely determined decompositions δ and $\bar\delta$ of S.

$$S=X\cup Y\cup Z\cup U\,,\qquad S=\bar X\cup\bar Y\cup\bar Z\cup\bar U$$

such that

$$h(a_1,\dots,a_k)=h_\delta(a,b,c,d)\,;\qquad h(b_1,\dots,b_k)=h_{\bar\delta}(a,b,c,d)\,.$$

It is not difficult to check that $\bar X=X-\{1\}$, $\bar Y=Y\cup\{1\}$, $\bar Z=Z$, $\bar U=U$. We see also that the operations h_δ and $h_{\bar\delta}$ are different.

Let C_1,C_2,C_3,C_4 stand for the symbols X,Y,Z,U but not necessarily in the same order. We find, by $h_\delta\neq h_{\bar\delta}$ and by (ε_0) that there are two *different* operations of two variables, one derived from $h_\delta(x,y,z,u)$, the other from $h_{\bar\delta}(x,y,z,u)$ and both obtained by *the same* identification of some of the variables x,y,z,u. This means that there is a set $C\subset S$ which can be denoted by $C_1\cup C_2\cup C_3$ or by $C_1\cup C_2$ or by C_1 such that $C\in\Omega_h$ but the corresponding set $\bar C\subset S$ denoted by $\bar C_1\cup\bar C_2\cup\bar C_3$ or $\bar C_1\cup\bar C_2$ or $\bar C_1$ does not belong to Ω_h.

It is obvious that C and $\bar C$ differ only in the element 1 of S and we have either $\{1\}=C-\bar C$ and $\bar C\subset C$ or $\{1\}=\bar C-C$ and $C\subset\bar C$. We define $G=C$, $H=S-\bar C$ so that $G\in\Omega_h$ and, by (i), $H\in\Omega_h$.

If $\{1\}=C-\bar C$, then $S=G\cup H$ and $G\cap H=\{1\}$. We derive from (ii) that $\{1\}\in\Omega_h$. If $\{1\}=\bar C-C$, we have $G\cap H=\emptyset$ and therefore, by (iii), $G\cup H\notin\Omega_h$ and, by (i), $\{1\}\in\Omega_h$.

We are now in a position to prove that Ω_h does not depend on h. By applying induction on the number of elements in X and using (o), (i), (iii), (iv) and (v) we find that

(ε_1) *A set $X\subset S$ belongs to Ω_h if and only if the number of elements in X is odd. In particular, since $S\in\Omega_h$, k is odd.*

As we noticed above, (ε_1) implies that there is at most one operation $h\in A^{(k)}$ which depends on every variable. Since k must then be odd, our proof of (ε) and of the theorem is now complete.

5. Algebras independently generated by every two elements

We shall prove here Theorems 5 and 6. Consider first the algebra $\mathfrak{A}$ defined in Theorem 5. It is easy to see that the class of all algebraic operations A consists of operations of the form

$$f(x_1,\dots,x_k)=\lambda_1x_1+\dots+\lambda_kx_k$$

where $\sum_i\lambda_i=1$. Let a,b be distinct elements in A. Then there exists, for every $c\in A$, exactly one operation $f\in A^{(2)}$ for which $c=f(a,b)$ (since the equations $\lambda_1a+\lambda_2b=c$, $\lambda_1+\lambda_2=1$ determine λ_1 and λ_2). Suppose that $g(a,b)=h(a,b)$ holds for some $g,h\in A^{(2)}$. It follows that $g=h$ and thus a,b are independent. Obviously these two elements generate the algebra and thus we have proved Theorem 5.

To prove Theorem 6 suppose that $\mathfrak{A}$ is an algebra which is independently generated by every two elements. A group T of one-to-one mappings of a set onto itself is called *doubly transitive* when it contains one or more mappings changing given two elements a,b into any two elements c,d. If the conditions $c=t(a)$, $d=t(b)$ determine uniquely the mapping $t\in T$, then T is said to be *minimal*. We prove first that

(λ) *The group T of all automorphisms of $\mathfrak{A}$ is a doubly transitive and minimal group of one-to-one mappings of A onto itself.*

Proof of (λ). If a,b are distinct elements of A and c,d also, then, by the independence of a,b, we infer that the mapping $a\to c$, $b\to d$ has an extension to a homomorphism t of the subalgebra generated by a,b on the subalgebra generated by c,d and obviously this extension is unique (cf. [3], sec. 2, (ii)). Since a,b generate $\mathfrak{A}$, t is an endomorphism and since c,d generate $\mathfrak{A}$, t is onto. Finally, from the independence of c,d it follows that t is an automorphism. Hence T is doubly transitive and since t is determined uniquely by the conditions $t(a)=c$, $t(b)=d$, T is minimal.

Our theorem now follows by (λ) since it is well known that if there exists, for a finite set, a doubly transitive and minimal group of one-to-one mappings of this set onto itself, then the number of elements of this set is a power of a prime (cf. [1], sec. 105; also [2]).

References

[1] W. Burnside, *Theory of groups of finite order*, Cambridge 1897.

[2] — *On doubly transitive groups of degree n and order n(n−1)*, The Messenger of Mathematics XXV (1896), p. 147-153.

[3] E. Marczewski, *A general scheme of the notions of independence in mathematics*, Bull. Acad. Pol. Sci. Série math., astr. et phys. 6 (1958), p. 731-736.

[4] S. Świerczkowski, *Algebras independently generated by every n elements*, Bull. Acad. Pol. Sci. Série math., astr. et phys. 7 (1959), p. 501-502.

[5] K. Urbanik, *A representation theorem for Marczewski's algebras*, Fund. Math. 48 (1960), p. 147-167.

INSTYTUT MATEMATYCZNY POLSKIEJ AKADEMII NAUK
MATHEMATICAL INSTITUTE OF THE POLISH ACADEMY OF SCIENCES

Reçu par la Rédaction le 30. 12. 1959

POLSKA AKADEMIA NAUK

FUNDAMENTA MATHEMATICAE

XLIX. 2

WARSZAWA 1961
PAŃSTWOWE WYDAWNICTWO NAUKOWE