COLLOQUIUM MATHEMATICUM

XIV WARSZAWA—WROCŁAW 1966

EXCHANGE OF INDEPENDENT SETS IN ABSTRACT ALGEBRAS (II)

BY

J. PŁONKA (WROCŁAW)

We say, following E. Marczewski, that an abstract algebra $\mathfrak{A} = (A; F)$ satisfies the condition of *exchange of independent sets* (EIS) if for any non-empty subsets P, Q, R of A the four relations

(a) $P \cap Q = 0$,

(b) $P \cup Q$ is independent,

(c) R is independent,

(d) R is included in the subalgebra generated by Q,

imply the relation

(e) $P \cup R$ is independent.

If (d) is replaced by the stronger condition, that the subalgebras generated by Q and R coincide, then (e) follows whatever $\mathfrak{A}$ is (Marczewski [2], p. 58, theorem (ii)). EIS is not true in all algebras, not even in groups, as Hulanicki and Świerczkowski have shown. But EIS is true in Abelian groups, Boolean algebras, Post algebras (Traczyk [7]) and v^*-algebras. These results are collected in the paper [1] by Hulanicki, Marczewski and Mycielski.

The purpose of this paper* is to prove or to disprove EIS for some other algebras.

The notation of [2] is adopted in general throughout this paper. Instead of saying "a set of independent elements", the expression "independent set" is used. $C(E)$ denotes the subalgebra generated by E.

Due thanks should be expressed here to Professor E. Marczewski and Docent J. Mycielski for numerous discussions and remarks.

THEOREM 1. *The condition EIS is satisfied in every alegbra in which all algebraic operations depend on at most one variable.*

* The results of this paper were announced in [4] and presented to the Conference on General Algebra, held in Warsaw, September 7-11, 1964.

Proof. Let us consider such an algebra $\mathfrak{A} = (A; F)$, and let P, Q, R be subsets of A satisfying (a)-(d). Let $p, r \in P \cup R$. We have to prove that

$$f(p) = g(r) \text{ implies } f = g. \tag{1}$$

If both elements p, r belong to P or both belong to R, then from the independence of the sets P and R it follows $f = g$. Let now e. g. $p \in P$, $r \in R$. As $R \subset C(Q)$, there exists $q \in Q$ and $h \in A^{(1)}$ such that $r = h(q)$. Hence $f(p) = g(h(q))$. In view of (a), $p \neq q$. The independence of $A \cup B$ implies now $f(x) = g(h(y)) = c$, with some algebraic constant c. From (1) it follows now $g(r) = c$, and from the independence of R we infer $g(x) = c = f(x)$ what completes the proof.

THEOREM 2. *Every algebra with at most six elements satisfies EIS. There exists an algebra $\mathfrak{A}_0$ with seven elements, in which EIS is not satisfied; moreover, every algebra with seven elements in which EIS is not satisfied has the same algebraic operations depending on at most three variables as $\mathfrak{A}_0$.*

Proof. At first we define the algebra $\mathfrak{A}_0 = (a, b, c, d, e, f, s; \circ)$ where $\circ$ is a commutative binary operation defined as follows: $a \circ b = d$, $a \circ c = e$, $b \circ c = f$, and $x \circ y = s$ in all other cases.

Let $P = \{c\}$, $Q = \{a, b\}$ and $R = \{d\}$. It is easy to see that relations (a)-(d) of EIS are satisfied while (e) is not, because $c \circ d = d \circ d = s$ in spite of $x \circ y \not\equiv y \circ y$.

Now it suffices to prove that every at most seven-element algebra either satisfies EIS or consists of precisely seven elements and its ternary algebraic operations are identical with the ternary algebraic operations of $\mathfrak{A}_0$.

We assume that $\mathfrak{A} = (A; F)$ is an at most seven-element algebra with subsets P, Q, R satisfying (a)-(d). As R is generated by Q, then for every $r \in R$ there exists an algebraic operation h and $q_1, \ldots, q_k \in Q$ such that $h(q_1, \ldots, q_k) = r$. Let $\{h_\tau\}_{\tau \in T}$ be the set of all such operations.

Suppose that (e) is not satisfied, i. e. that there exist $a_1', \ldots, a_s' \in P \cup R$ ($a_i' \neq a_j'$ for $i \neq j$) and two algebraic operations $\varphi \neq \psi$ such that

$$\varphi(a_1', \ldots, a_s') = \psi(a_1', \ldots, a_s'). \tag{2}$$

We can write this in the form

$$f(a_1, \ldots, a_m) = g(a_{1+m}, \ldots, a_{n+m}), \tag{3}$$

where $a_i \in P \cup R$, $a_i \neq a_j$ for $i < j \leqslant m$ and for $m+1 \leqslant j < i$; $f \neq g$, f depends on all m variables, g depends on all n variables. (We do not assume here $a_i \neq a_j$ for $i \leqslant m$, $j \geqslant 1+m$.)

We shall denote the elements of the sets P, Q, R by p, q, r with indices, respectively.

Let us now consider all possibilities.

1° *Each of the operations f, g, h depends on at most one variable.* (Evidently the operations h_τ cannot be constant, as R is independent.)

Consider now the algebra $\mathfrak{B} = (A; f, g, \{h_\tau\}_{\tau\in T})$. Then this algebra does not satisfy the condition EIS, which contradicts Theorem 1.

2° *For some $r_0 \in R$, $\tau_0 \in T$, $n > 1$ and $q_1, \ldots, q_n \in Q$ we have $r_0 = h_{\tau_0}(q_1, \ldots$ $\ldots, q_n)$, and h_{τ_0} depends on all n variables.*

It follows that in $P \cup Q$ there exist at least $1+n$ elements, as P is non-empty. Operation h_{τ_0} depends on n elements and consequently (in view of the formula (iii) in [2], p. 725, or the formula (1) in [6], p. 191) A contains at least $2n+2$ elements. If $n > 2$, then $2n+2 > 7$, so it must be $n = 2$. For simplicity we shall write $h_\tau(x, y) = x\cdot y$.

Let $p \in P$. Then the following six elements are certainly distinct: $p, q_1, q_2, pq_1, pq_2, q_1q_2$, and none of them is an algebraic constant, as $P \cup Q$ is independent.

If $x\cdot y$ is non-commutative, then the elements q_1p, q_2p, q_2q_1, are distinct and different from the listed above and so $|A| \geqslant 9$. An obvious contradiction.

Hence $x\cdot y$ is commutative. If there are no algebraic constants, then by Theorem I in [6] there exist in $\mathfrak{A}$ n-ary algebraic operations dependent on all variables for $n = 3, 4, \ldots$

An argument of Marczewski ([3], p. 725) gives the following proposition (which is a slight modification of his proposition (ii) on p. 725 of [3]):

(o) If an algebra $(E; \boldsymbol{F})$ has the following properties: 1° there exist algebraic k-ary operations dependent on all variables for $k = 2, 3, 4, \ldots, n$ $(n > 2)$, 2° there are no algebraic constants, 3° there exists an independent set $I = \{a_1, \ldots, a_n\}$, 4° $|A| = 2^n - 1$, then the algebraic n-ary operations in $(E, \boldsymbol{F})$ are roughly speaking the same as in $(2^I \setminus \{\emptyset\}, \cup)$ or, more precisely, there exists a one-one mapping $\varphi: E \to 2^I \setminus \{\emptyset\}$ transforming the family $\boldsymbol{A}^{(n)}(E; \boldsymbol{F})$ onto the family $\boldsymbol{A}^{(n)}(2^I \setminus \{\emptyset\}; \cup)$.

We apply this proposition to the algebra $\mathfrak{A}$. Since there exists in A at least 3-element independent set, we have (by inequality (*) of [3], p. 724, or Theorem 3 of [6], p. 192) $|A| \geqslant 2^3 - 1 = 7$ and since, by hypothesis, $|A| \leqslant 7$, we have finally $|A| = 7$. Hence the hypotheses of proposition (o) are satisfied.

In order to prove (e) for at most three-element set $P \cup R$ it suffices to consider ternary operations only and hence it is easy to verify, with the aid of (o), that in the considered case EIS is satisfied.

Hence there are constants in $\mathfrak{A}$ and so

$$A = \{p, q_1, q_2, pq_1, pq_2, q_1q_2, c\},$$

where c is a constant.

Let us observe that $(xy)z$ can depend on at most two variables, as (p, q_1, q_2) is independent.

If $(xy)z = c$, then $xx = c$, because $\mathfrak{A}$ cannot have non-trivial operations of one variable which are not constants, as otherwise we would have three more elements, say $\varphi(q_1)$, $\varphi(q_2)$, $\varphi(p)$, and $xx = x$ would imply $c = (xx)x = xx = x$, a contradiction.

It is clear that in $\mathfrak{A}$ there are no operations depending on at most 3 variables, which are not generated by $x \cdot y$. As $(A; x \cdot y)$ is isomorphic with $\mathfrak{A}_0$ our theorem follows in the case $(xy)z = c$.

Now, consider the remaining possibilities:

If $(xy)z = x$ and $xx = x$, then $x = (xx)z = xz$, $p = pq_1$.
If $(xy)z = x$ and $xx = c$, then $x = (xy)(xy) = c$.
If $(xy)z = y$ and $xx = x$, then $x = (xx)z = xz$, $p = pq_1$.
If $(xy)z = y$ and $xx = c$, then $y = (xy)(xy) = c$.
If $(xy)z = z$ and $xx = x$, then $z = (xx)z = xz$, $p = pq_1$.
If $(xy)z = z$ and $xx = c$, then $c = (xy)(xy) = xy$, $c = pq_1$.
If $(xy)z = xy$ and $xx = x$, then $x = xx = (xx)z = xz$, $p = pq_1$.
If $(xy)z = xy$ and $xx = c$, then $c = (xy)(xy) = xy$, $c = pq_1$.
If $(xy)z = xz$, then $yz = (yx)z = (xy)z = xz$, $pq_1 = pq_2$.
If $(xy)z = yz$, then $yz = (xy)z = (yx)z = xz$, $pq_1 = pq_2$.

In all these cases we got a contradiction, and so the theorem is proved under the assumption of 2°.

3° *For some* $r \in R$, $q \in Q$ *and* $h \in A^{(1)}$, $r = h(q)$ *and, moreover,* $h^{(k)} \neq e_1^{(1)}$ *for* $k = 1, 2, \ldots$, (where $h^{(k)}(x)$ denotes the k-th iterate of h, and $(e_1^{(1)}x) = x$).

In this case we prove that all elements $h^n(r)$ $(n = 1, 2, \ldots)$ are distinct, what will lead to an obvious contradiction with $|A| \leqslant 7$. Indeed, suppose that

$$h^m(r) = h^p(r).$$

where $1 < m < p$ and m is as small as possible.

Since the set $\{r\}$ is independent, it must be $h^m(x) = h^p(x)$, whence, $h^{m-1}(r) = h^{m-1}(h(q)) = h^m(q) = h^p(q) = h^{p-1}(h(q)) = h^{p-1}(r)$, what does not lead to a contradiction with the minimal property of m only in the case $m = 1$, but then $h(x) = h^p(x)$ and so $r = h(q) = h^p(q) = h^{p-1}(h(q)) = h^{p-1}(r)$ contrary to our assumption.

4° *All functions* h_t *depend on at most one variable, and for each* t *there exists* $k(t)$ *such that* $h_t^{k(t)} = e_1^{(1)}$.

Then at least one of the functions f, g (viz. (3)) *must depend on more than one variable.*

Suppose f depends on more than one variable. The elements $a_1, \ldots, a_{m+n}$ cannot all belong to P or all to R, as it would imply the dependence of one of those sets. If it were $\{a_1, \ldots, a_m\} \subset P$, $\{a_{m+1}, \ldots, a_n\} \subset R$ or *vice versa*, then the condition (d) would imply $f = g$. Hence we can write (3) in the form

$$(4) \qquad f(p_1, \ldots, p_{m_1}, r_1, \ldots, r_{m_2}) = g(p_{m_1+1}, p_{m_1+n_1}, r_{m_2+1}, \ldots, r_{m_2+n_2}),$$

where $m_1+m_2 = m$, $n_1+n_2 = n$ and $m > 1$, $m_1 \geqslant 1$, $m_2 \geqslant 1$.

At least one of the r_i occurring here belongs to $R \setminus Q$, say $r_{i_0} \in R \setminus Q$. Then we have $r_{i_0} = h_{t_0}(q_1)$ with some $q_1 \in Q$. We must have at least one more element, say q_2 in Q, as otherwise $h_{t_0}^{(k_{t_0})} = e_1^{(1)}$ would imply $q_1 = h_{t_0}^{(k_{t_0}-1)}(r_{i_0})$, and so $Q \subset C(R)$, but then, by Theorem 1, EIS would be satisfied, contrary to our assumption.

Let $p \in P$. Then the following elements of A are certainly distinct: $p, q_1, q_2, h_{t_0}(p), h_{t_0}(q_1), h_{t_0}(q_2)$. If $h_{t_0}(q_2) \in R \setminus Q$, then we conclude as before that Q contains a further element, say q_3, and that $h_{t_0}(q_3)$ would be different from the elements listed above, and so $|A| \geqslant 8$. A contradiction. Thus $h_{t_0}(q_2) \notin R \setminus Q$. If R was generated by Q by means of 2 operations, h_{t_1}, h_{t_2} say, then A would contain at least 9 elements. Let $h(x)$ be thus the only operation by means of which Q generates R. Obviously $|P| = 1$, $|Q| = 2$.

Evidently $h(h(x)) = x$ as otherwise A would contain 9 elements. Moreover, q_2 does not belong to R as otherwise R would generate Q and in view of a theorem of Marczewski ([2], p. 58, th. (iii)) the condition EIS would be fulfilled. It follows that R contains the element $h(q_1)$ only, and so the operation f occurring in (3) must depend on exactly two variables. But now the elements $f(p, q_1), f(p, q_2), f(q_1, q_2)$ would be distinct and A would contain at least 9 elements, a contradiction.

The theorem is thus proved in all cases.

An n-dimensional *diagonal algebra* (see [4] and [5]) is an algebra $\mathfrak{D} = (X; d)$ with a unique fundamental operation $d(x_1, \ldots, x_n)$ satisfying the following postulates:

1° $d(x, \ldots, x) = x$,

2° $d\big(d(x_1^1, \ldots, x_n^1), d(x_1^2, \ldots, x_n^2), \ldots, d(x_1^n, \ldots, x_n^n)\big) = d(x_1^1, x_2^2, \ldots, x_n^n)$.

If the operation $d(x_1, \ldots, x_n)$ depends on each variable, then the n-dimensional diagonal algebra will be called *proper*.

We say that an element a of the n-dimensional diagonal algebra is *collinear in the p-th direction* with an element b of this algebra, which relation we shall denote by

$$a \equiv_p b,$$

if $a = d(a, \ldots, a, b, a, \ldots, a)$, where the element b in parantheses on the right-hand side is on the p-th place.

The diagonal algebras have the following properties (see [3]):

(x) A subset J of an n-dimensional proper diagonal algebra is dependent if and only if there exist in it two different elements a and b which are collinear in some direction.

(xx) Every algebraic operation $f \in A^{(m)}$ of the n-dimensional diagonal algebra is of the form

$$f(x_1, \ldots, x_m) = d(x_{i_1}, \ldots, x_{i_n}),$$

$1 \leqslant i_p \leqslant m$ for $p = 1, \ldots, n$.

(xxx) If $a = d(a_1, \ldots, a_n)$, then $a \equiv_p a_p$ for $p = 1, \ldots, n$.

(xxxx) Each relation $\equiv_p$ is an equivalence.

THEOREM 3. *In every proper n-dimensional diagonal algebra the condition EIS is satisfied.*

Proof. Let P, Q, R be non-empty subsets of such an algebra, satisfying (a)-(d) but not (e). In view of (x) we can find in $P \cup R$ two different elements collinear in some direction. Clearly, we may assume that one of them belongs to P and the other to R, and so let $p \in P$, $r \in R$ and

$$p \equiv_t r. \tag{5}$$

From (d) and (xx) it follows $r = k(q_1, \ldots, q_n)$, hence by (xxx) we have

$$r \equiv_t q_t. \tag{6}$$

From (5) and (6) it follows by (xxxx) that $p \equiv_t q_t$, but that contradicts the independence of $P \cup Q$.

A *semilattice* is a commutative semi-group with an idempotent multiplication. In a semilattice we define the relation "$\leqslant$" putting $a \leqslant b$ if $ab = a$.

Szász [5] proved that a subset $A = \{a_1, \ldots, a_r\}$ of a semilattice is dependent iff for some i one has $a_i \geqslant a_1 \ldots a_{i-1} a_{i+1} \ldots a_r$. We prove now

THEOREM 4. *In every semilattice condition EIS is satisfied.*

Proof. Let P, Q, R be subsets of a semilattice and let us assume that the conditions (a)-(d) are satisfied, while the condition (e) is not. There exists then a set $J = \{j_0, \ldots, j_s\} \subset P \cup R$ such that

$$j_0 \geqslant j_1 \ldots j_s. \tag{7}$$

It can be neither $J \cap P = \emptyset$ nor $J \cap R = \emptyset$, because one of the sets P, R would be dependent. If $p_0 \in P$, then (7) may be written in the form

$$p_0 \geqslant p_1 \ldots p_m r_1 \ldots r_n \quad (m+n = s, p_i \in P,\ r_i \in R). \tag{8}$$

But (d) implies

$$r_i = q_1^{(i)} \ldots q_{k_i}^{(i)} \quad (i = 1, \ldots, n;\ q_j^{(i)} \in Q). \tag{9}$$

From (8) and (9) we get

$$p_0 \geqslant p_1 \ldots p_m (q_1^{(1)} \ldots q_{k_1}^{(1)}) \ldots (q_1^{(n)} \ldots q_{k_n}^{(n)}). \tag{10}$$

But this contradicts the independence of the set $P \cup Q$. Hence, $j_0 \notin P$ and so $j_0 \in R$. Thus (7) may be written in the form

$$r_0 \geqslant p_1 \ldots p_m r_1 \ldots r_n \quad (m+n = s,\ p_i \in P,\ r_i \in R). \tag{11}$$

As $r_i = q_1^{(i)} \ldots q_{k_i}^{(i)}$ $(q_j^{(i)} \in Q,\ i = 0, 1, \ldots, n)$, we have

$$q_1^{(0)} \ldots q_{k_0}^{(0)} \geqslant p_1 \ldots p_m (q_1^{(1)} \ldots q_{k_1}^{(1)}) \ldots (q_1^{(n)} \ldots q_{k_n}^{(n)}). \tag{12}$$

Each of the elements $q_j^{(0)}$ $(j = 1, \ldots, k_0)$ must appear explicite in one of the parantheses on the right-hand side of (12) because otherwise from

$$q_j^{(0)} \geqslant q_1^{(0)} \ldots q_{k_0}^{(0)} \quad \text{for some } j$$

we would have

$$q_j^{(0)} \geqslant p_1 \ldots p_m (q_1^{(1)} \ldots q_{k_n}^{(n)})$$

in contradiction with the independence of the set $P \cup Q$.

But now we can write

$$q_1^{(0)} \ldots q_{k_0}^{(0)} \geqslant (q_1^{(1)} \ldots q_{k_1}^{(1)}) \ldots (q_1^{(n)} \ldots q_{k_n}^{(n)}),$$

i. e. $r_0 \geqslant r_1 \ldots r_n$.

The last formula contradicts the independence of the set R which completes the proof.

Remark (*added in proof*). In view of some recent results of K. Urbanik (contained in the paper *On some numerical constants associated with abstract algebras*, Fundamenta Mathematicae, in print), Theorem 2 can be strengthened by omitting the words "depending on at most three variables".

REFERENCES

[1] A. Hulanicki, E. Marczewski and J. Mycielski, *Exchange of independent sets in abstract algebras (I)*, Colloquium Mathematicum 14 (1964), p. 203-215.

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

[3] — *Number of independent elements in abstract algebras with unary and binary operations*, Bulletin de l'Académie Polonaise des Sciences, Série des sc. math., astr. et phys., 12 (1964), p. 723-727.

[4] J. Płonka, *Diagonal algebras and algebraic independence*, ibidem, p. 729-733.

[5] — *Diagonal algebras*, Fundamenta 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] G. Szász, *Marczewski's independence in lattices and semi-lattices*, ibidem 10 (1963), p. 15-20.

[8] T. Traczyk, *Some theorems on independence in Post algebras*, Bulletin de l'Académie Polonaise des Sciences, Série des sc. math., astr. et phys., 11 (1963), p. 3-8.

Reçu par la Rédaction le 1. 3. 1965