COLLOQUIUM MATHEMATICUM

XIV WARSZAWA–WROCŁAW 1966

EXCHANGE OF INDEPENDENT SETS IN ABSTRACT ALGEBRAS (I)

BY

A. HULANICKI, E. MARCZEWSKI AND J. MYCIELSKI (WROCŁAW)

0. Prerequisites. In this paper* we use the terminology and notation of [6] (with slight modifications). In particular, for any abstract algebra, i. e. a set A with a family of fundamental finitary operations, we denote by $A^{(n)}$ the family of all n-ary algebraic operations. The letters f and g always denote algebraic operations in A.

For simplicity sake we say that I is an independent set instead of I is a set of independent elements (in the sense of [5] and [6]). The family of all independent sets has finite character, i. e. I is independent whenever each finite subset of I is independent.

For any non-void set $E \subset A$ we denote by $C(E)$ the subalgebra generated by E, $C(\emptyset)$ denoting the set of algebraic constants (i. e. the values of the constant algebraic operations). The operation C has finite character, i.e.

(F) $C(E) = \bigcup C(F)$, where F runs over the family of all finite subsets of E.

We say that the algebra is *finitely* [*independently*] *generated* if it is generated by a certain finite [independent] subset.

We use the symbol $\equiv$ in the sense "identically equal in A", e. g. $f(x_1, x_2) \equiv g(x_2, x_3)$ is to be understood as $f(x_1, x_2) = g(x_2, x_3)$ for every $x_1, x_2, x_3 \in A$. One-element set $\{a\}$ is written simply as a.

1. Problem and results. The following theorem about exchange of independent sets is true for all algebras ([6], p. 58, theorem 2.4 (ii)):

(o) *Let P, Q and R be subsets of an algebra. If*

(1) $P \cup Q$ *is independent,* (2) $P \cap Q = O$,

(3) R *is independent,* (4) $C(R) = C(Q)$,

* The results of which have been presented without proofs by E. Marczewski in his lecture *Independence in abstract algebras. Result and problems* to the Conference on General Algebra, held in Warsaw, September 7-11, 1964 (see this volume, p. 169-188).

then

(5) $$P \cup R \text{ is independent.}$$

It might seem at first glance that relation (4) could be replaced by a weaker one:

(4*) $$R \subset C(Q).$$

Since, as we shall see later on, this is not generally true, we say that an algebra satisfies *the condition of exchange of independent sets* (EIS) whenever for any subsets P, Q and R of it, the relations (1), (2), (3) and (4*) imply (5). The finite character of the operation C together with the finite character of the family of independent sets imply that in definition of EIS it is enough to consider only finite P, Q and R.

This paper is a contribution to the general problem which algebras satisfy the condition EIS. It turns out that Boolean algebras (see Section 3) and, more generally, Post algebras (Traczyk [11]), vector spaces and, more generally, v^*-algebras (Section 4), and Abelian groups, and, more generally, algebras called here separable variables algebras (Section 5) satisfy EIS.

Nevertheless, there are algebras which do not satisfy EIS. The first example of this kind, namely of a non-Abelian infinite group, in which EIS fails, is due to A. Hulanicki and S. Świerczkowski (1960). It is given at the end of this paper. We give also a simpler example of a group not satisfying EIS. This group is finite and has the minimal possible number of elements which is 729 (Section 6).

A recent paper of Płonka [11] presents different classes of algebras satisfying EIS and a seven-element algebra not satisfying it.

Our theorem concerning v^*-algebras is a corollary of a theorem about the generalized closure operators having finite character and the Steinitz exchange property (Section 4). Thus, that proposition belongs to the theory of abstract linear independence (and, perhaps, is not new).

2. Exchange in algebras. Let us begin by the remark that theorem (o) has been strengthened recently (and at the same time generalized for algebras with infinitary operations) by Schmidt [12] as follows:

(i) *Let $(P_t)_{t\in T}$ be an indexed family of pairwise disjoint independent subsets of an algebra A, $(R_t)_{t\in T}$ another family of disjoint independent subsets of A with $C(P_t) = C(R_t)$ for $t \in T$, and let*

$$P = \bigcup_{t\in T} P_t \quad \text{and} \quad R = \bigcup_{t\in T} R_t.$$

Then the independence of P implies the independence of R.

Since the union of every increasing transfinite sequence of independent sets is independent (in finitary algebras), we obtain by Kuratowski-Zorn lemma:

(ii) *For any (finitary) algebra satisfying* EIS *we may replace in* (i) *the relation* $C(R_t) = C(P_t)$ *by* $R_t \subset C(P_t)$.

We pass to other facts on EIS which will be used in the final section.

First let us recall that if B is a subalgebra of an algebra A and if a subset I of B is independent in A, then I is independent in B. The converse is not true ([6], p. 56), but it is easy to see that if a finite subset of A is independent in every finitely generated subalgebra including it, then it is independent in A. By this remark, it is not difficult to prove

(iii) *If every finitely generated subalgebra satisfies* EIS, *then the whole algebra satisfies* EIS.

The following propositions concerning independence will be useful in the proof of (iv) and later:

A1. If A is a finite algebra generated by an independent set I, then any independent set in A has cardinal not greater than $|I|$ and every independent set of cardinality $|I|$ generates A.

This is a direct consequence of a known theorem (Świerczkowski [11], p. 749, Theorem 1).

A2. If B is a subalgebra of A and $I, J \subset B$, $|J| \leqslant |I|$, I is independent in A, and J independent in B, then J is independent in A.

Let $a_1, \ldots, a_n$ be distinct elements of J. Since $|I| \geqslant n$, there exist distinct elements $b_1, \ldots, b_n$ of I. If

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

then, by the independence of $\{a_1, \ldots, a_n\}$ in B,

$$f(b_1, \ldots, b_n) = g(b_1, \ldots, b_n),$$

whence f and g are identical in A by the independence of $\{b_1, \ldots, b_n\}$ in A.

(iv) *If each subalgebra generated by a finite independent set is finite and satisfies* EIS, *then the whole algebra satisfies* EIS.

Take any finite sets P, Q and R satisfying (1), (2), (3) and (4*). On account of (4*), $P \cup R$ is contained in the subalgebra $B = C(P \cup Q)$ which is finite and satisfies EIS by the assumption. Hence it follows from (1), (2), (3) and (4*) that $P \cup R$ is independent in B and consequently, by A1, we have $|P \cup R| \leqslant |P \cup Q|$ and, by A2, $P \cup R$ is independent in A, q. e. d.

3. Exchange in Boolean algebras.

THEOREM. *Boolean algebras satisfy the condition of exchange of independent sets* (EIS) [1].

[1] This theorem is contained in an analogous result concerning Post algebras (Traczyk [14]).

Proof. Let $\mathfrak{B} = (B; \cup, \cap, ', 0, 1)$ be a Boolean algebra. For any element $a \in B$ we put

$$a^0 = a' \quad \text{and} \quad a^1 = a,$$

and we call an *atom* of the finite set $a_1, \ldots, a_n \in B$ (where $a_1, \ldots, a_n$ are obviously distinct) every element of the form

$$a_1^{i_1} \cap a_2^{i_2} \cap \ldots \cap a_n^{i_n} \quad \text{where} \quad i_k = 0, 1 \text{ for } k = 1, \ldots, n.$$

It is known that $I \subset B$ is an independent set if and only if every atom of every finite subset of I is different from 0 (see [5]).

In order to prove the theorem we suppose (1), (2), (3) and (4*) and we consider each of the atoms a of any finite non void set $F \subset P \cup R$.

If $F \subset P$ or $F \subset R$, then $a \neq 0$ because of (1) or (3). Thus we may suppose that $a = b \cap c$, where b is an atom of a finite subset S of P and c an atom of a finite subset T of R. In view of (3), we have

$$0 \neq c \in C(Q).$$

It is known that in Boolean algebras every element of $C(E)$ different from 0 is the union of certain atoms of a certain finite subset of E.

Consequently, there is an atom d of a finite subset T of Q such that $d \subset c$. In view of (2), the sets S and T are disjoint, whence, $b \cap d$ is an atom of $S \cup T^*$. Hence, by (1),

$$0 \neq b \cap d \supset b \cap c = a.$$

Thus we obtain (5) and the theorem is proved.

4. Exchange of C-independent sets. Exchange in v^*-algebras. A generalized closure operator C in a set A (i. e. an extensive, monotone and idempotent mapping of the family $\mathfrak{P}(A)$ of all subsets of A into $\mathfrak{P}(A)$; cf. e. g. Birkhoff [1], p. 49) is said to have *finite character*, if it satisfies condition (F) (see Prerequisites).

C has the *exchange property* (called also *Stenitz property*), whenever

(E) if $q \notin C(E)$ and $q \in C(E \cup p)$, then $p \in C(E \cup q)$.

A set $I \subset A$ is called *C-independent*, whenever $p \notin C(I \setminus p)$ for every $p \in I$ (see e. g. Bleicher-Marczewski [2] and the papers quoted there).

Now we replace the independence by the C-independence in the condition EIS, saying that C satisfies the condition of *exchange of C-independent sets* (ECIS), whenever the conditions

(1^c) $P \cup Q$ is a C-independent set, (2) $P \cap Q = 0$,

(3^c) R is a C-independent set, (4*) $T \subset C(Q)$

imply

(5^c) $P \cup R$ is a C-independent set.

THEOREM. *If a generalized closure operator C has finite character* (F) *and Stenitz exchange property* (E), *then C satisfies the condition of exchange of C-independent sets* (ECIS).

Proof. Assume (1^c), (2), (3^c), (4*) and suppose, that (5^c) is not true. Thus there exists an element $a \in P \cup R$ such that $a \in C(P \cup R \setminus a)$,

In virtue of (F) there exists a minimal finite set F such that $F \subset P \cup R \setminus a$ and $a \in C(F)$. We have $F = P_0 \cup R_0$, where $P_0 = F \cap P$ and $R_0 = F \cap R$.

$$(\alpha) \quad a \in P \qquad \text{and} \qquad (\beta) \quad a \in R \setminus P.$$

If (α), then in view of (4*)

$$a \in C(P \cup R \setminus a) \subset C\big((P \setminus a) \cup R\big) \subset C\big((P \setminus a) \cup Q\big),$$

which is impossible by virtue of (1^c) and (2).

If (β), then, for each $b \in P_0$, by the definition of F, we have

$$a \in C(F) \quad \text{and} \quad a \notin C(F \setminus b),$$

whence, because of (E), (β), (4*) and (2),

$$b \in C(F \setminus b \cup a) \subset C\big((P_0 \setminus b) \cup R\big) \subset C\big((P \setminus b) \cup R\big) \subset C\big((P \setminus b) \cup Q\big) = C(P \cup Q \setminus b)$$

which is impossible, in virtue of (1^c). Hence, $P_0 = \emptyset$, and consequently, by the definition of F and R_0,

$$a \in C(F) = C(R_0) \subset C(R \setminus a),$$

which contradicts (3^c).

Thus condition (5) must be satisfied and the theorem is proved.

For every algebra A the operation C (where $C(E)$ denotes the subalgebra generated by E) is a generalized closure operator of finite character. A is called a *v^*-algebra* if 1° independence and C-independence coincide for it and 2° C has the exchange property (E). Thus, Theorem implies

COROLLARY. *Every v^*-algebra satisfies the condition of exchange of independent sets* (EIS).

Let us recall that v^*-algebras are a generalization of vector spaces (see Narkiewicz [8] and Urbanik [12]).

Examples due to J. Płonka show that each of the conditions (F) and (E) in Theorem are essential.

5. Exchange in separable variables algebras and in Abelian groups. We say that in an algebra A the *variables can be separated* or *that A is a separable variable algebra* if for each pair of different operations $f, g \in A^{(n)}$

(where $n = 1, 2, \ldots$) and each m with $1 \leqslant m < n$ there are $f^* \in A^{(m)}$ and $g^* \in A^{(n-m)}$ such that the equations

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \quad \text{and} \quad f^*(x_1, \ldots, x_m) = g^*(x_{m+1}, \ldots, x_n)$$

are equivalent.

THEOREM. *A separable variable algebra satisfies the condition of exchange of independent sets* (EIS).

Proof. Suppose (1), (2), (3) and (4*) (see definition of EIS).

Let $\{p_1, \ldots, p_k\} \subset P$, $\{r_1, \ldots, r_n\} \subset R$, and

$$(*) \qquad f(p_1, \ldots, p_k, r_1, \ldots, r_n) = g(p_1, \ldots, p_k, r_1, \ldots, r_n).$$

In order to show (5) we have to prove that $f = g$.

Since, by hypothesis, the variables can be sepatated, there are f^* and g^* such that the equations

$$f(x_1, \ldots, x_k, y_1, \ldots, y_n) = g(x_1, \ldots, x_k, y_1, \ldots, y_n)$$

and

$$f^*(x_1, \ldots, x_k) = g^*(y_1, \ldots, y_n)$$

are equivalent.

Hence, (*) implies $f^*(p_1, \ldots, p_k) = g^*(r_1, \ldots, r_n)$.

By (4*), there exists g_* and $q_1, \ldots, q_m \in Q$ such that

$$(*_*) \qquad g^*(r_1, \ldots, r_n) = g_*(q_1, \ldots, q_m),$$

whence

$$f^*(p_1, \ldots, p_k) = g_*(q_1, \ldots, q_m).$$

In view of (1) and (2), $\{p_1, \ldots, p_k\}$ and $\{q_1, \ldots, q_m\}$ are disjoint subsets of an independent set $P \cup Q$, whence (on account of proposition (iv) of [7]), f^* and g_* are constant. Their common value is of course an algebraic constant c. Hence, by $(*_*)$,

$$g^*(r_1, \ldots, r_n) = c,$$

and, by (3),

$$g^*(y_1, \ldots, y_n) \equiv c.$$

Finally, we have

$$f^*(x_1, \ldots, x_k) \equiv g^*(y_1, \ldots, y_n),$$

whence, by definition of f^* and g^*, we get $f = g$, q. e. d.

Every group G with the operations $x \cdot y$ and x^{-1} will be regarded as the algebra $(G, \cdot, {}^{-1})$.

Since, obviously, in Abelian groups the variables can be separated we get

COROLLARY. *Abelian groups satisfy the condition of exchange of independent sets* (EIS).

Let us remark that two conditions obtained by replacing in EIS independence by linear independence in the sense of [3], p. 37, or by linear independence in the sense of [4], p. 123, are also satisfied in every Abelian group.

6. Exchange in non-Abelian groups. In this section we consider condition EIS for some non-Abelian groups. We note that a group is independently generated if and only if it is a reduced free group in a variety (i. e. an equational class) of groups (see [9] and [10]). According to our general-algebraic notation, the subgroup generated by a subset E of a group is denoted by $C(E)$.

THEOREM 1. *Every finite group independently generated by one or two elements satisfies the condition* EIS.

(At the end of this section we add an example showing that the assumption of finiteness is essential.)

Proof. Let F be a finite group independently generated by 2 elements (for cyclic groups the result is obvious). Since F is finite, there is an $n > 0$ such that $x^n \equiv 1$ holds in F. Let n be the least of such exponents. By A1 any independent set in F has at most 2 elements. Thus we may assume that $P = \{a\}$ and $Q = \{b\}$ and the orders of a and b are equal to n. Now if $R \subset C(Q)$ and R is independent, then $R = \{a^k\}$ and $(n, k) = 1$. Thus $C(R) = C(Q)$ and by (o) (see p. 203) the result follows.

THEOREM 2. *Every group of order* $\leqslant 729$ *satisfies the condition* EIS *except one whose order is* 729 *and which has* 3 *independent generators.*

The proof will follow in several lemmas.

Proposition (iv) implies the following

LEMMA 1. *If all independently generated groups of order* < 729 *satisfy* EIS, *then so does every group of order* < 729 *and any group of order* 729 *which is not independently generated.*

Now for any group G we put

$$G' = C\{[x, y]: x, y \in G\},$$

$$G^2 = C\{[x, y]: x \in G', y \in G\},$$

where $[x, y] = x^{-1}y^{-1}xy$.

The following known propositions will be applied

B1([2]). If F is a group independently generated by k elements, then F/F' is a direct product of k cyclic group of equal orders, say n, and if n is finite, then the relation $x^n \equiv 1$ holds in F.

([2]) See B. H. Neumann [9], theorem 19.5. Recall that the term "reduced free" used in [9] coincides with our "independently generated".

B2 ([3]). If F is independently generated by k elements $a_1, \ldots, a_k$ and $|F'/F^2| \neq 1$, then F'/F^2 is a direct product of $k(k-1)/2$ cyclic groups of equal orders generated by the cosets $[a_i, a_j]F^2$ where $1 \leqslant i < j \leqslant k$.

Proof. Let $c_{ij} = [a_i, a_j]$. We note that, since

$$[xy, z] \in [x, z][y, z]F^2, \quad [x, yz] \in [x, y][x, z]F^2,$$

$$[x^{-1}, y] \in [x, y]^{-1}F^2, \quad [x, y^{-1}] \in [x, y]^{-1}F^2,$$

$$[x, y] = [y, x]^{-1},$$

we have

$$F' = (C\{c_{ij}: i, j = 1, 2, \ldots, k, i < j\})F^2.$$

Thus the cosets $c_{ij}F^2$ generate F'/F^2.

Clearly, F'/F^2 is Abelian. Suppose that for some integers n_i we have

$$(\circ) \qquad \prod_{1 \leqslant i < j \leqslant k} c_{ij}^{n_{ij}} \in F^2.$$

For any pair of indices $i < j$ we consider the endomorphism f of F induced by the mapping $a_i \to a_i$, $a_j \to a_j$, $a_s \to 1$ for any $s \neq i, j$. Then $c_{i'j'}f = c_{i'j'}f = 1$ for any pair $(i', j') \neq (i, j)$. Thus the image of the left-hand side of $(\circ)$ is $c_{ij}^{n_{ij}}$, the right-hand side remaining in F^2. Consequently,

$$c_{ij}^{n_{ij}} \in F^2,$$

which proves that F'/F^2 is the direct product of the cyclic groups generated by the cosets $c_{ij}F^2$.

For showing that these cyclic groups have equal orders it is enough to apply permutations of the set $a_1, \ldots, a_k$ interchanging the c_{ij} which clearly extend to automorphisms of F under which F' and F^2 are invariant and thus they interchange the cosets $c_{ij}F^2$. This concludes the proof of B2.

By Theorem 1 and Lemma 1, it is enough to prove Theorem 2 for groups of order $\leqslant 729$ which are independently generated by $k \geqslant 3$ generators. For every such group F there is a minimal n such that $x^n \equiv 1$ holds in F. If $n = 2$, then the group is Abelian and as such satisfies EIS (see Section 5). Since, by B1,

$$(*) \qquad |F/F'| = n^k,$$

all we have to consider are the cases when

$$(**) \qquad n^k \leqslant 729, \quad k \geqslant 3, \quad n \geqslant 3.$$

([3]) This proposition while unpublished up to now is well known to the specialists. Nevertheless for reader's convenience we present a proof here. Mrs Hanna Neumann has kindly informed us that this proposition was proved in 1963 by Peter M. Neumann.

The following relations will be in permanent use:

$$(\overset{*}{**}) \qquad 729 \geqslant |F| = |F/F'|\cdot|F'| \quad \text{and} \quad |F'| = |F'/F^2|\cdot|F^2|.$$

LEMMA 2. *For any solution* (k, n) *of inequalities* $(\overset{*}{*})$ *other than* (3.3) *and* (3.4) *the group* F *is Abelian.*

Proof. All the solutions of $(\overset{*}{*})$ are in the following table:

k	n
3	3, 4, 5, 6, 7, 8, 9
4	3, 4, 5
5	3
6	3

Consider the case $k = 3$, $n \geqslant 6$, first. If $F' \neq 1$, then, putting $|F'| = s$, by $(*)$ and $(\overset{**}{*})$ we have $n^3 \cdot s \leqslant 729$ and $s \mid n^m$ for an $m \geqslant 1$ (since F is an n-group, $|F|$ must divide a power of n). Hence, $s = 3$ or $s = 2$. This means that F' is a cyclic group of order 2 or 3. Let a, b, c be independent generators of F. If for a pair of these generators, say for a and b, we have $[a, b] = 1$, then $[x, y] \equiv 1$ i. e. F is Abelian, contrary to the assumption $F' \neq 1$. Now, since $s < 4$, at least two of the commutators $[a, b]$, $[b, c]$, $[c, a] \in F'$ must be equal. Suppose $[a, b] = [b, c]$. Then $[x, y] \equiv [y, z]$. Put $z = 1$ and again we get $[x, y] \equiv 1$ contrary to the assumption $F' \neq 1$.

Now for any of the remaining cases n is a power of a prime, which, since F is finite, implies that F is nilpotent. Therefore in order to prove that for any pair (k, n) other than (3.3) and (3.4) the group F is Abelian, it is sufficient to show that $F' = F^2$, i. e. $|F'/F^2| = 1$. We have.

$$(6) \qquad 729 \geqslant |F| = |F/F'|\cdot|F'/F^2|\cdot|F^2|.$$

Hence, if $k > 3$ and $F'/F^2 \neq 1$, then, by B2, F'/F^2 is the direct product of at least $\binom{4}{2} = 6$ copies of a cyclic group. That is $|F'/F^2| \geqslant 2^6$. On the other hand, by B1, $|F/F'| = n^k \geqslant 3^4$ whence, by $(\overset{**}{*})$, $729 \geqslant 3^4 \cdot 2^6$, which is false. In the case of $k = 3$, the only value of n which is left to be considered is $n = 5$. Then, since F is a 5-group, F'/F^2 is a 5-group, whence, by B2, if non-trivial, it is the direct product of 3 copies of a cyclic group of order 5, so, by $(\overset{**}{*})$ nad B1, $729 \geqslant 5^3 \cdot 5^3$, which again is false, q. e. d.

By Lemma 2 we know that EIS holds in all groups of order $\leqslant 729$ except possibly the groups independently generated by 3 elements satisfying either $x^3 \equiv 1$ or $x^4 \equiv 1$.

Now we are going to show that for each of these identities there is precisely one non-Abelian group of that kind. One of them has 512 elements and satisfies condition EIS while the other has 729 elements and does not satisfy EIS.

LEMMA 3. *If F has 3 independent generators, $|F| < 729$ and F satisfies the relation*

(a) $$x^4 \equiv 1,$$

then it satisfies also

(b) $$[[x, y], z] \equiv 1,$$

(c) $$[x, y]^2 \equiv 1$$

and $|F| \leqslant 512$.

Proof. If F is Abelian, then (b) and (c) are obvious, and $|F| = 4^3 < 512$. Suppose it is non-Abelian. Then, as a finite 2-group, it is nilpotent and so $F'/F^2 \neq 1$. By B2 since also F'/F^2 is a 2-group,

$(^{**}_{**})$ $$|F'/F^2| = (2^m)^3 \quad \text{for an integer } m \geqslant 1.$$

By B1, $F/F' = 4^3$. Therefore, in virtue of $(^{**}_{*})$, we must have $m = 1$ and $|F^2| = 1$. This proves that (b) is satisfied. By B2, F'/F^2 is the direct sum of three cyclic groups, which in virtue of $(^{**}_{**})$ with $m = 1$, shows that F'/F^2 is the direct sum of three cyclic groups of order 2. This combined with the fact that $F^2 = 1$, shows that any element of F' is of order 2, i. e. that (c) holds. Clearly, by $(^{**}_{*})$, $|F| = 4^3 \cdot 2^3 = 512$.

LEMMA 4. *A group F with 3 independent generators which satisfies the relations* (a), (b) *and* (c) *of Lemma 3 has property* EIS.

Proof. F is finite (it has $\leqslant 4^3 \cdot 2^3 = 512$ elements). Therefore, by A1, the maximal cardinal of a set of independent elements is 3. If $|Q| = 1$, then EIS is proved as in Lemma 2. Suppose $|Q| \equiv 2$ and $|P| = 1$ and let $\{a, b\} = Q$, $\{c\} = P$. By A1, a, b, c are independent generators of F. Let $R \subset C\{a, b\}$ be a set of independent elements. If $|R| = 2 = |Q|$, then, by A1, $C(Q) = C(R)$, whence, by (o), $R \cup P$ is independent. Let then $R = \{d\} \subset C\{a, b\}$. Relations (a), (b), (c) imply that

$$d = a^\alpha b^\beta [a, b]^\varepsilon, \quad \text{where} \quad 0 \leqslant \alpha, \beta \leqslant 3, \ 0 \leqslant \varepsilon \leqslant 1,$$

and, since d is independent, the order of it must be 4. As a consequence of (b) we have in F

$$[x^n, y] \equiv [x, y^n] \equiv [x, y]^n \text{ for any } n.$$

Therefore, using (c), we see that, for any $x \in F$, x^2 commutes with all elements of F. Hence, since d has order 4, either α or β must be odd, because if both α and β were even, then

$$d^2 = a^\alpha b^\beta a^\alpha b^\beta [a, b]^2 = a^{2\alpha} b^{2\beta} = 1,$$

since a^α and b^β commute. Let then α be odd and let $\alpha\mu \equiv 1 (\mathrm{mod}\, 4)$. Then the endomorphism of F induced by the mapping $a \to a^\mu$, $b \to 1$, $c \to c$ maps d onto a and c onto c, which proves that the set $P \cup R = \{d, c\}$ is independent, which was to be proved.

LEMMA 5. *If F has three independent generators, is non Abelian, satisfies*

(a) $$x^3 \equiv 1$$

and $|F| \leqslant 729$, then F is the reduced free group of three generators of the variety of groups given by relations (a) *and*

(b) $$[[x, y], z] \equiv 1.$$

Moreover, $|F| = 729$.

Proof. Let P be the direct product of two cyclic groups of order 3, i. e. the group of pairs (s, t), where s, t are integers and $s, t = 0, 1, 2$, with the coordinatewise addition mod3. Let f be the automorphism of P defined by

$$(s, t)f = (s, s+t).$$

Clearly, $(s, t)f^3 = (s, t)$. Let G be the splitting extension of P by the automorphism f that is the group of pairs (f^m, p) where $p \in P$ and $m = 0, 1, 2$, the multiplication being defined by

$$(f^m, p)(f^n, q) = (f^{m+n}, pf^n + q).$$

It is the matter of simple computation to verify that F is non-Abelian and satisfies (a) and (b) and is generated by two elements $(f^0, (1, 0))$ and $(f, (0, 0))$. Therefore, the free group F_3 with three free generators in the variety of groups given by (a) and (b) is non-Abelian.

It follows immediately from (a) and (b) that any element of F_3 is representable in the form

$$a^{\alpha_1} b^{\alpha_2} c^{\alpha_3} [a, b]^{\alpha_4} [b, c]^{\alpha_5} [c, a]^{\alpha_6},$$

where a, b, c are free generators of F_3 and $0 \leqslant \alpha_i < 3$, $i = 1, \ldots, 6$. So $|F_3| \leqslant 3^6 = 729$.

Let F satisfy the conditions of Lemma 5 as F_3 does. Since F is finite and satisfies (a), it is nilpotent. Therefore, if non-Abelian, $|F'/F^2| \neq 1$. Hence, by B1 and B2 in virtue of $\binom{**}{*}$, we have

$$729 \geqslant |F| = 3^3 \cdot 3^3 \cdot |F^2| = 729\,|F^2|,$$

whence $|F^2| = 1$, i. e. (b) holds and $|F| = 729$. Hence, $F = F_3$.

LEMMA 6. *The reduced free groups F_3 of three free generators a, b, c of the variety given by identities* (a) *and* (b) *of Lemma* 5 *does not satisfy* EIS.

In fact, F_3 is non-Abelian, so the element $[a, b] \in C\{a, b\}$ is independent, since the order of it is 3. But the set $\{[a, b], c\}$ is not independent because $[[a, b], c] = 1$ and $[x, y] \equiv 1$ does not hold in F_3.

This concludes the proof of Theorem 2.

Now let us show that the assumption of *finiteness in Theorem* 1 *is essential* (by Theorem 2 the other assumption is also essential).

First we define an auxiliary group G. It is the group of pairs of integers with group operations defined by

$$(m, n)(k, l) = (m+k, (-1)^k n+l),$$
$$(m, n)^{-1} = (-m, (-1)^{m+1} n).$$

It is easy to see that this is the group with two generators $a = (1, 0)$ and $b = (0, 1)$ and one defining relation

$$(^+) \qquad ba = ab^{-1}.$$

Of course $b^n = (0, n)$ and hence

$$(^+_+) \qquad b \text{ is of infinite order.}$$

It is also easy to check that the identity

$$(^{++}_+) \qquad [x^2, y^2] \equiv 1$$

holds in G.

EXAMPLE. *The reduced free group F of two free generators in the variety defined by $(^{++}_+)$ does not satisfy* EIS.

In fact let α and β be the free generators of F. We put $P = \alpha$, $Q = \beta$, $R = \beta^2$. It is clear that conditions (1), (2) and (4) are satisfied. Since G satisfies $(^{++}_+)$, then the mapping $\alpha \to a$, $\beta \to b$ defines a homomorphism of F onto G, whence, by $(^+_+)$, β^2 is of infinite order and so (3) is also true. To show that (5) fails we consider the function $f(u, v) = [u^2, v]$. Of course $f(\alpha, \beta^2) = 1$ and it is enough to show that $f(x, y) \equiv 1$ fails in F. But, since G is in the variety of F, this would follow from $f(b, a) \neq 1$. Indeed, by $(^+)$ and $(^{++}_+)$ we have

$$f(b, a) = b^{-2}a^{-1}b^2a = b^{-2}a^{-1}ab^{-2} = b^{-4} \neq 1.$$

REFERENCES

[1] G. Birkhoff, *Lattice theory*, New York 1948.

[2] M. N. Bleicher and E. Marczewski, *Remarks on dependence relations and closure operators*, Colloquium Mathematicum 9 (1962), p. 209-212.

[3] M. Hall, Jr., *The theory of groups*, New York 1959.

[4] А. Г. Курош, *Теория групп*, Москва 1953.

[5] E. Marczewski, *Independence in algebras of sets and Boolean algebras*, Fundamenta Mathematicae 48 (1960), p. 135-145.

[6] — *Independence and homomorphism in abstract algebras*, Fundamenta Mathematicae 50 (1961), p. 45-61.

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

[8] W. Narkiewicz, *Independence in a certain class of abstract algebras*, Fundamenta Mathematicae 50 (1962), p. 333-340.

[9] B. H. Neumann, *Identical relations in groups I*, Mathematische Annalen 114 (1947), p. 506-525.

[10] Hanna Neumann, *On varieties of groups and their associated near-rings*, Mathematische Zeitschrift 65 (1956), p. 36-69.

[11] J. Płonka, *Exchange of independent sets in abstract algebras (II)*, this volume, p. 217-223.

[12] J. Schmidt, *Concerning some theorems of Marczewski on algebras independence*, Colloquium Mathematicum 13 (1964-5), p. 11-15.

[13] S. Świerczkowski, *On independent elements in finitely generated algebras*, Bulletin de l'Académie Polonaise des Sciences, Série des sc. math., astr. et phys., 6 (1958), p. 749-752.

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

[15] K. Urbanik, *A representation theorem for v*-algebras*, Fundamenta Mathematicae 52 (1963), p. 291-316.

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

Reçu par la Rédaction le 10. 1. 1965