that if $\mathcal{A}_k \simeq \mathcal{A}_m$, $m \neq k$, holds, then $m = k + qd$ for some $q > 0$. Since $l = k + d$, the algebra $\mathcal{A}_k$ cannot have any rank s, such that $k < s < l$. It remains to prove that l is a rank of $\mathcal{A}_k$. Indeed, if $\delta = (a_1, \ldots, a_k)$ is the basic sequence of the free generators of $\mathcal{A}_k$, then the sequence $\varphi(\delta)$ defined by (7) is a basic sequence composed of l elements (cf. Lemma 4). This completes the proof of Theorem 2.

References

[1] G. Birkhoff, *Lattice theory*, Amer. Math. Soc. Colloquium Public., New York, 25 (1948).

[2] A. Goetz and Cz. Ryll-Nardzewski, *On bases of abstract algebras*, Bull. Acad. Pol. Sci., Série des sci. math., astr. et phys. 8 (1960), pp. 157-162.

[3] J. A. Green, *A duality in abstract algebra*, Journ. Lond. Math. Soc. 27 (1952), pp. 64-76.

[4] B. Jónsson and A. Tarski, *Two general theorems concerning free algebras*, Bull. Amer. Math. Soc. 62 (1956), p. 554.

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

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

Reçu par la Rédaction le 5. 7. 1960

Independence and homomorphisms in abstract algebras

by

E. Marczewski (Wrocław)

I have shown in 1958 that many notions called *independence* in different branches of mathematics are particular cases of a certain general notion defined in terms of abstract algebra ([4]).

This general concept of independence has subsequently been treated by several authors. They have discussed some of its properties in finitely generated algebras (Świerczkowski [10]), algebras in which all elements are independent and, more generally, algebras in which every n elements form a basis (i.e. a set of independent generators; Świerczkowski [10], [12], Marczewski and Urbanik [7]), bases of an algebra and the set of their cardinal numbers (Goetz and Ryll-Nardzewski [2], Świerczkowski [13]), and self-dependent elements of an algebra (Goetz and Ryll-Nardzewski [2], Nitka [9]). The study of algebras in which independence has the properties of linear independence (Marczewski [5], Urbanik [14]) constitutes a special domain in this research. A discussion of independence in the algebras of sets and Boolean algebras (Marczewski [6]) is the first step in the study of this general concept in particular classes of algebras usually considered.

The purpose of this paper is to formulate and to prove explicitly several simple but fundamental properties of the notion of independence, no special hypotheses about the algebra in question being postulated. Some concrete algebras quoted below serve merely as counterexamples.

Chapter 1 contains preliminaries without any new results. Chapter 2 contains some lemmas on the extension of mappings to homomorphisms (2.1), the definition of independence, and some equivalence theorems (2.2); one of these (iii) enables us to define the notion of independence by that of homomorphism (1). The following section (2.3) treats of some properties connected with the idea of independence but defined by the notion of the algebraic closure only, i.e. without the use of algebraic operations. It seems interesting that these properties (as well as other

(1) The notion of independence is related to that of free algebra, and the equivalence theorem 2.2 (iii) is a particular case of the known equivalence of two definitions of a free algebra.

conditions of this kind, not expressed here) are essentially weaker than independence (defined in 2.2). Further (2.4) a series of simple theorems are proved by a uniform method, namely by using the definition of independence in terms of homomorphism. The last of those theorems says that the numbers of elements of all bases of an algebra form an arithmetical progression (iv). The paper ends with some remarks on independence and mappings (2.5).

1. Algebras

1.1. Operations. We denote by $A \times B$ the Cartesian product of A and B, by A^n the n-th Cartesian power of A, by B^A the set of all mappings of A into B and by 2^A the class of all subsets of A.

Any A-valued function of many variables running over A will be called an *operation* on A. The class of all n-ary operations on A, i.e. the set A^{A^n} will be denoted by $\boldsymbol{O}^{(n)}(A)$, or briefly $\boldsymbol{O}^{(n)}$. We put $\boldsymbol{O} = \boldsymbol{O}(A) = \boldsymbol{O}^{(1)}(A) \cup \boldsymbol{O}^{(2)}(A) \cup \ldots$

If $\varphi, \psi \in \boldsymbol{O}^{(n)}(A)$ and the set A is fixed, then the identity

$$\varphi(x_1, \ldots, x_n) \equiv \psi(x_1, \ldots, x_n)$$

means that

$$\varphi(x_1, \ldots, x_n) = \psi(x_1, \ldots, x_n) \quad \text{for every} \quad (x_1, \ldots, x_n) \in A^n.$$

We denote by $\boldsymbol{E}^{(n)}(A)$ or $\boldsymbol{E}^{(n)}$ the set consisting of n *trivial* operations (or "identity-operations"), i.e. operations defined on A by the formulas

$$e_j^{(n)}(x_1, \ldots, x_n) \equiv x_j \quad (j = 1, 2, \ldots, n;\ n = 1, 2, \ldots).$$

We put $\boldsymbol{E} = \boldsymbol{E}(A) = \boldsymbol{E}^{(1)}(A) \cup \boldsymbol{E}^{(2)}(A) \cup \ldots$

In general, for any class $\boldsymbol{F} \subset \boldsymbol{O}$ we denote by $\boldsymbol{F}^{(n)}$ the class of all n-ary operations belonging to $\boldsymbol{F}$, so that

$$\boldsymbol{F}^{(n)} = \boldsymbol{F} \cap \boldsymbol{O}^{(n)}, \quad \boldsymbol{F} = \boldsymbol{F}^{(1)} \cup \boldsymbol{F}^{(2)} \cup \ldots$$

For any $\varphi \in \boldsymbol{O}^{(n)}$ and $S \subset A$ we denote by $\varphi|S$ the *restriction* of φ to S^n, or, in other terms, we put $\varphi|S = \varphi \cap (S^n \times A)$. For any class $\boldsymbol{F} \subset \boldsymbol{O}$ we put

$$\boldsymbol{F}|S = \{\varphi|S\colon\ \varphi \in \boldsymbol{F}\}.$$

For any class $\boldsymbol{F} \subset \boldsymbol{O}(A)$, we say that a set $B \subset A$ is *closed* with respect to $\boldsymbol{F}$, whenever $\boldsymbol{F}|B \subset \boldsymbol{O}(B)$.

If $\varphi \in \boldsymbol{O}^{(m)}(A)$ and $\varphi_1, \ldots, \varphi_m \in \boldsymbol{O}^{(n)}(A)$ then the operation on A defined by the formula

$$\psi(x_1, \ldots, x_n) \equiv \varphi\big(\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_m(x_1, \ldots, x_n)\big)$$

will be denoted by

$$\psi = \hat{\varphi}(\varphi_1, \ldots, \varphi_m).$$

If $\boldsymbol{F} \subset \boldsymbol{O}(A)$ we put further $\hat{\boldsymbol{F}} = \{\hat{\varphi}\colon\ \varphi \in \boldsymbol{F}\}$. Following the common usage, we omit the sign $\hat{}$ when no confusion can arise.

1.2. Algebras and algebraic operations. A non-void set A with a class $\boldsymbol{F}$ of operations on A, or, more precisely, the system $\mathfrak{A} = (A; \boldsymbol{F})$, where $\boldsymbol{F} \subset \boldsymbol{O}(A)$, will be called an *algebra* [2]. The class $\boldsymbol{F}$ will be called the class of *fundamental* operations of $\mathfrak{A}$.

If $A = \{a, b, \ldots\}$ and $\boldsymbol{F} = \{f, g, \ldots\}$ we sometimes write $(a, b, \ldots; f, g, \ldots)$ instead of $(A; \boldsymbol{F})$.

In this paper the following examples of algebras will be used several times:

$$\mathfrak{J}_k = (0, 1, \ldots, k-1;\ +(\mathrm{mod}\, k)) \quad (k = 1, 2, \ldots)$$

and the Boolean algebra $\mathfrak{B}_k$ of all subsets of the k-element set $X_k = \{1, 2, \ldots, k\}$, i.e. the algebra

$$\mathfrak{B}_k = (2^{X_k};\ \cup, ') \quad (k = 1, 2, \ldots)$$

where $'$ denotes complementation.

In a fixed algebra $\mathfrak{A} = (A; \boldsymbol{F})$, for $n = 1, 2, \ldots$, we denote by $\boldsymbol{A}^{(n)}(\mathfrak{A})$ (or $\boldsymbol{A}^{(n)}(A; \boldsymbol{F})$, or $\boldsymbol{A}^{(n)}(A)$, or briefly $\boldsymbol{A}^{(n)}$) the class of all *algebraic* n-ary operations [3] in $\mathfrak{A}$, i.e. the smallest class of operations satisfying the conditions:

1° $\boldsymbol{E}^{(n)} \subset \boldsymbol{A}^{(n)} \subset \boldsymbol{O}^{(n)}$,

2° if $f \in \boldsymbol{F}^{(m)}$, $f_1, \ldots, f_m \in \boldsymbol{A}^{(n)}$, then $f(f_1, \ldots, f_m) \in \boldsymbol{A}^{(n)}$.

We put further $\boldsymbol{A} = \boldsymbol{A}^{(1)} \cup \boldsymbol{A}^{(2)} \cup \ldots$

E.g. the class $\boldsymbol{A}^{(n)}(\mathfrak{J}_k)$ consists of all functions of the form $m_1 x_1 + \ldots + m_n x_n$ where the coefficients m_j assume the values $0, 1, \ldots, k-1$, and the class $\boldsymbol{A}^{(n)}(\mathfrak{B}_k)$ consists of all so-called Boolean polynomials of n variables.

Since for every $f \in \boldsymbol{F}^{(n)}$ we have $f = f(e_1^{(n)}, \ldots, e_n^{(n)})$, we obtain from 1° and 2°:

(i) $\boldsymbol{F}^{(n)} \subset \boldsymbol{A}^{(n)}$ *for* $n = 1, 2, \ldots$

An auxiliary rôle in some proofs is played by the classes $\boldsymbol{A}_k^{(n)}$ $(n = 1, 2, \ldots;\ k = 0, 1, \ldots)$, defined recursively as follows:

$$\boldsymbol{A}_0^{(n)} = \boldsymbol{E}^{(n)}, \quad \boldsymbol{A}_{k+1}^{(n)} = \boldsymbol{A}_k^{(n)} \cup \bigcup_{m=1}^{\infty} \{f(f_1, \ldots, f_m)\colon\ f_j \in \boldsymbol{A}_k^{(n)},\ f \in \boldsymbol{F}^{(m)}\}.$$

---

[2] Cf. e.g. Birkhoff [1], p. vii.

[3] Cf. e.g. McKinsey and Tarski [8], p. 160.

We obviously have

$$A_0^{(n)} \subset A_1^{(n)} \subset \dots$$

It is easily seen that $A_0^{(n)} \cup A_1^{(n)} \cup \dots$ is a subclass of $A^{(n)}$ and satisfies 1° and 2°. Hence, by the definition of $A^{(n)}$, we obtain

(ii) $A^{(n)} = A_0^{(n)} \cup A_1^{(n)} \cup \dots$ *for* $n = 1, 2, \dots$

In order to prove the theorem

(iii) *If* $f \in A^{(m)}$, *and* $f_1, \dots, f_m \in A^{(n)}$, *then* $f(f_1, \dots, f_m) \in A^{(n)}$,

it suffices, in view of (ii), to prove the same implication under the hypothesis $f \in A_k^{(m)}$ ($k = 0, 1, 2, \dots$). This is easy to verify by induction with respect to k.

(iv) *If* $f \in A^{(n)}$ ($n = 1, 2, \dots$) *and*

$$g(x_1, \dots, x_n, x_{n+1}) \equiv f(x_1, \dots, x_n)$$

then $g \in A^{(n+1)}$.

In fact, $g = f(e_1^{(n+1)}, \dots, e_n^{(n+1)})$, whence, by (iii), $g \in A^{(n+1)}$.

(v) *If* $f \in A^{(n+1)}$ ($n = 1, 2, \dots$) *and*

$$g(x_1, \dots, x_n) \equiv f(x_1, \dots, x_n, x_n)$$

then $g \in A^{(n)}$.

In fact, $g = f(e_1^{(n)}, \dots, e_n^{(n)}, e_n^{(n)})$, whence, by (iii), $g \in A^{(n)}$.

(vi) *If an operation* $f \in A^{(n+1)}$ *does not depend on the* $(n+1)$*-th variable, and*

$$g(x_1, \dots, x_n) \equiv f(x_1, \dots, x_n, x_{n+1})$$

then $g \in A^{(n)}$.

In fact, we have

$$g(x_1, \dots, x_n) \equiv f(x_1, \dots, x_n, x_n)$$

and we apply (v).

From (vi) we directly infer that

(vii) *If an operation* $f \in A^{(n)}$ *is constant*:

$$f(x_1, \dots, x_n) \equiv c,$$

then the unary operation $g(x) \equiv c$ *belongs to* $A^{(1)}$.

(viii) *If* $f \in A^{(n)}$, $(k_1, \dots, k_n)$ *is a sequence of positive integers with* $1 \leqslant k_i \leqslant m$, *and*

$$g(x_1, \dots, x_m) \equiv f(x_{k_1}, \dots, x_{k_n})$$

then $g \in A^{(m)}$.

In fact, $g = f(e_{k_1}^{(m)}, \dots, e_{k_n}^{(m)})$, whence, by (iii), $g \in A^{(m)}$.

If $A^{(n)}$ denotes, as it has done so far, the class of all n-ary algebraic operations on an algebra $(A; F)$, then every operation $f \in F$ may be considered as an operation on $A^{(n)}$ (see 1.1), so that $(A^{(n)}; F)$ (or, more precisely, $(A^{(n)}; \hat{F})$) forms a new algebra: the *algebra of* n*-ary algebraic operations* on $\mathfrak{A}$.

In all further considerations the class of algebraic operations plays a fundamental part. All the notions concerning algebras considered here can be defined by means of algebraic operations without using fundamental operations (cf. 1.3 (iv) and 2.1). Consequently, two algebras $\mathfrak{A} = (A, F)$ and $\mathfrak{A}^* = (A, F^*)$ are considered as identical whenever $A(\mathfrak{A}) = A(\mathfrak{A}^*)$.

The letters f and g (with or without indices, asterisks, etc.) will always denote algebraic operations in the algebras in question.

1.3. Subalgebras, algebraic closure and generators. Let us consider an algebra $\mathfrak{A} = (A; F)$. A non-void set $B \subset A$ is called a *subalgebra* of $\mathfrak{A}$ (or of A) if it is closed with respect to F, or (which is equivalent in view of 1.2 (ii)) to A. Each subalgebra B of A may be treated as a new algebra: $\mathfrak{B} = (B; F|B)$. In order to prove that

(i) *If* B *is a subalgebra of* $(A; F)$, *then*

$$A^{(n)}(B; F|B) = A^{(n)}(A; F)|B$$

it suffices to verify by induction that

$$A_k^{(n)}(B; F|B) = A_k^{(n)}(A; F)|B \quad \text{for} \quad k = 0, 1, \dots$$

(which presents no difficulty) and to apply 1.2 (ii).

It is easy to see that the notion of subalgebra has an absolute character: any subset S of B is a subalgebra of B if and only if it is a subalgebra of A.

We denote by $C(A)$ or briefly by C the set of all *algebraic constants* of $\mathfrak{A}$ [4], i.e. the set of all values of constant algebraic operations in $\mathfrak{A}$, or else (which is equivalent in view of 1.2 (vii)) of all values of constant unary algebraic operations in $\mathfrak{A}$. Obviously the set $C(A)$ is a subalgebra of A contained in every subalgebra of A. Nevertheless the notion of algebraic constant has no absolute character: an algebraic constant of a subalgebra may not be an algebraic constant in the whole algebra.

If S is a non-void subset of A, then the smallest subalgebra containing S will be denoted $\overline{S}$ [5] and called the *algebraic closure* of S. We say that $\overline{S}$ is the subalgebra *generated* by S or else, that S is a set of *generators* of $\overline{S}$. The symbol $\overline{0}$ will denote the set $C(A)$. In view of 1.2 (iv) and 1.2 (iii)

(ii) *For any non-void set* $S \subset A$

$$\overline{S} = \bigcup_{n=1}^{\infty} \{f(a_1, \dots, a_n)\colon\ a_1, \dots, a_n \in S,\ f \in A^{(n)}\}.$$

---

[4] Sometimes it is convenient to denote C by the symbol $A^{(0)}$ (cf. e.g. [5] and [9]), i.e. to treat algebraic constants as „algebraic operations of 0 arguments".

[5] The correspondence $S \to \overline{S}$ is a so-called closure operation (cf. e.g. Birkhoff [1], p. 49).

For non-void sets, the operation of algebraic closure has an absolute character, i.e. if B is a subalgebra of A, and $0 \neq S \subset B$, then the closure of S in the algebra A and the closure of S in the algebra B are identical. (However, the symbol $\overline{0}$ may have another sense in these two algebras.)

The representation: $d = f(a_1, \ldots, a_n)$ of an element d of $\overline{S}$ by the elements $a_1, \ldots, a_n$ of S is called *irreducible* if $a_1, \ldots, a_n$ are different and f depends on every variable. It follows from (ii), 1.2 (v) and 1.2 (vi) that

(iii) *Every elements $d \in \overline{S} \setminus C(A)$ has at least one irreducible representation by the elements of S.*

We will prove that

(iv) *If an algebra has an infinite minimal set of generators G, then any of its minimal sets of generators G^* has the same cardinal number.*

In fact, if $a \in G^*$ then there is a finite subset $T_a \subset G$ such that $a \in \overline{T}_a$. Thus the set

$$\bigcup_{a \in G^*} T_a$$

is a set of generators contained in G and, consequently, identical with G. Consequently $|G^*| \geqslant |G|$ and thus G^* is infinite. Hence, by the same argument, $|G| \geqslant |G^*|$.

The hypothesis that G is infinite is essential: see 2.4.

2. Homomorphisms and independence

2.1. Homomorphisms and isomorphisms. We establish in this chapter an algebra $\mathfrak{A} = (A; \boldsymbol{F})$ and suppose that A contains at least 2 elements.

If B_1 and B_2 are two subalgebras of A, then a mapping h of B_1 into B_2 is called a *homomorphism of B_1 into B_2*, provided that for any $f \in \boldsymbol{F}$

$$(+) \qquad h\big(f(x_1, \ldots, x_n)\big) = f\big(h(x_1), \ldots, h(x_n)\big) \quad \text{for} \quad x_1, \ldots, x_n \in B_1 .$$

It follows from the definition of algebraic operations that if h is a homomorphism of B_1, then (+) is true for any algebraic operation f. Consequently, for any non-void $S \subset B_1$ we have $h(\overline{S}) = \overline{h(S)}$. Hence $h(B_1)$ is a subalgebra of A.

It may happen that two algebraic operations different in A are equal in a subalgebra of A. Nevertheless,

(i) *If A is a homomorphic image of a subalgebra B of A: $h(B) = A$, then two algebraic operations f and g equal in B are equal in A.*

In fact, if $x_1, \ldots, x_n \in A$, then there are $u_1, \ldots, u_n \in B$ such that $h(u_j) = x_j$ for $j = 1, 2, \ldots$ Hence

$$f(x_1, \ldots, x_n) = h\big(f(u_1, \ldots, u_n)\big) = h\big(g(u_1, \ldots, u_n)\big) = g(x_1, \ldots, x_n) .$$

Now let us consider some problems of the extension of mappings to homomorphisms.

(ii) *Let p be a mapping of a set $S \subset A$ into A. The following conditions are equivalent*:

(h) *there exists an extension of p to a homomorphism h of $\overline{S}$ into A,*

(a) *if $a_1, \ldots, a_{m+n} \in S$, $f \in A^{(m)}$, $g \in A^{(n)}$ $(m, n = 1, 2, \ldots)$ and*

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

then

$$f\big(p(a_1), \ldots, p(a_m)\big) = g\big(p(a_{m+1}), \ldots, p(a_{m+n})\big) .$$

Roughly speaking, condition (a) says that p preserves all algebraic equalities.

The implication (h)$\Rightarrow$(a) follows easily from (+) In order to prove that (a)$\Rightarrow$(h) let us define the mapping h of $\overline{S}$ by putting

$$hf(x_1, \ldots, x_n) = f\big(p(x_1), \ldots, p(x_n)\big) .$$

It follows from (a) that this definition is consistent. In the case of $f(x) = x$ the above formula gives the identity of h and p on S, whence, applying once more the same formula, we see that h is a homomorphism of S into A. Theorem (ii) is thus proved.

(iii) *For any mapping p of $S \subset A$ into A condition* (a) *is equivalent to each of the following*:

(a′) *if $a_1, \ldots, a_n \in S$, $f, g \in A^{(n)}$ $(n = 1, 2, \ldots)$ and*

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

then

$$(**) \qquad f\big(p(a_1), \ldots, p(a_n)\big) = g\big(p(a_1), \ldots, p(a_n)\big) ;$$

(a″) *if $a_1, \ldots, a_n$ are different elements of S, $f, g \in A^{(n)}$ $(n = 1, 2, \ldots)$ and* (*), *then* (**).

The implications (a)$\Rightarrow$(a′)$\Rightarrow$(a″) are trivial.

In order to prove that (a″)$\Rightarrow$(a′) let us suppose that p satisfies (a″). Thus the implication (*)$\Rightarrow$(**) is true for any system $a_1, \ldots, a_n$ of different terms. Let us suppose, by induction, that this implication is true for any system for which there are at most k pairs $i < j$ such that $a_i = a_j$. If there are $k+1$ such pairs in a system $a_1, \ldots, a_n$, we may admit, without loss of generality, that $a_{n-1} = a_n$. Let us suppose further that

$$f(a_1, \ldots, a_{n-1}, a_n) = g(a_1, \ldots, a_{n-1}, a_n) .$$

and put

$$f_0(x_1, \ldots, x_{n-1}) \equiv f(x_1, \ldots, x_{n-1}, x_{n-1}) , \qquad g_0(x_1, \ldots, x_{n-1}) \equiv g(x_1, \ldots, x_{n-1}, x_{n-1}) .$$

Hence f_0 and g_0 are algebraic by 1.2 (v) and

$$f_0(a_1, \ldots, a_{n-1}) = g_0(a_1, \ldots, a_{n-1}).$$

There exist in the system $a_1, \ldots, a_n$ at most k pairs $i < j$ with $a_i = a_j$. Consequently, in view of the identity $p(a_{n-1}) = p(a_n)$,

$$f\big(p(a_1), \ldots, p(a_{n-1}), p(a_n)\big) = f_0\big(p(a_1), \ldots, p(a_{n-1})\big)$$
$$= g_0\big(p(a_1), \ldots, p(a_{n-1})\big) = g\big(p(a_1), \ldots, p(a_{n-1}), p(a_n)\big).$$

In order to prove that (a')⇒(a) let us suppose that p satisfies (a') and that

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

The operations

$$f_1(x_1, \ldots, x_{m+n}) \equiv f(x_1, \ldots, x_m), \quad g_1(x_1, \ldots, x_{m+n}) \equiv g(x_{m+1} \ldots, x_{m+n})$$

are algebraic in view of 1.2 (iv). Successively we obtain

$$f_1(a_1, \ldots, a_{m+n}) = g_1(a_1, \ldots, a_{m+n}),$$
$$f_1\big(p(a_1), \ldots, p(a_{m+n})\big) = g_1\big(p(a_1), \ldots, p(a_{m+n})\big),$$
$$f\big(p(a_1), \ldots, p(a_m)\big) = g\big(p(a_{m+1}), \ldots, p(a_{m+n})\big), \quad \text{q.e.d.}$$

Theorem (ii) and (iii) give the following corollary:

(iv) *For a mapping p of a subalgebra B into A, each of the conditions* (a), (a') *and* (a'') *is necessary and sufficient in order that p be a homomorphism.*

A one-one homomorphism h of a subalgebra B_1 onto a subalgebra B_2 is called an *isomorphism* (of B_1 onto B_2). Its converse mapping is an isomorphism of B_2 onto B_1. If h is an isomorphism of B_1 onto B_2, $f_1 \in A^{(n)}(B_1)$, and the operation f_2 is defined by the identity

$$f_2(y_1, \ldots, y_n) = h f_1\big(h^{-1}(y_1), \ldots, h^{-1}(y_n)\big) \quad \text{for} \quad y_1, \ldots, y_n \in B_2,$$

then the correspondence $f_1 \to f_2$ is a one-one correspondence between $A^{(n)}(B_1)$ and $A^{(n)}(B_2)$.

Consequently all properties defined by the aid of algebraic operations in B_1 and B_2 respectively are invariant with respect to isomorphisms (of B_1 onto B_2).

2.2. Definition of independence. Equivalences. We say that a finite set $I = \{a_1, \ldots, a_n\} \subset A$ is a set of *independent* elements (or, that $a_1, \ldots, a_n$ are independent), when, for any $f, g \in A^{(n)}$, if

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

then f and g are identical. It easily follows from 1.2 (iv) that all subsets of a finite set of independent elements are also sets of independent elements. An infinite set is called a set of independent elements whenever any of its finite subsets is a set of independent elements.

The condition "I is a set of independent elements" will be denoted by (I). Further, we say that a set S satisfies conditions (H), (A), (A') or (A'') if any mapping p of S into A satisfies (h), (a), (a') or (a'') respectively (see the preceding section). We will prove that

(i) *Conditions* (I), (H), (A), (A') *and* (A'') *are equivalent.*

The equivalence of (H), (A), (A') and (A'') follows from 2.1 (ii) and 2.1 (iii). The implication (I)⇒(A'') is obvious. In order to prove that (A'')⇒(I) let us suppose that (*), where $a_1, \ldots, a_n$ are different elements of A. Let $x_1, \ldots, x_n$ be an arbitrary sequence of elements of A, and p a mapping of A into A such that $p(a_j) = x_j$ for $j = 1, 2, \ldots, n$. On account of (A'') we have

$$f(x_1, \ldots, x_n) = f\big(p(a_1), \ldots, p(a_n)\big) = g\big(p(a_1), \ldots, p(a_n)\big) = g(x_1, \ldots, x_n)$$

and thus condition (I) is satisfied. Theorem (i) is proved.

Let us write separately the most important equivalences: (I)⇔(A) and (I)⇔(H) [6]:

(ii) *I is a set of independent elements if and only if for any sequence $a_1, \ldots, a_{m+n} \in I$, if*

$$(**_*) \qquad f(a_1, \ldots, a_m) = g(a_{m+1}, \ldots, a_{m+n})$$

then, for any mapping p of I into A, we have

$$f\big(p(a_1), \ldots, p(a_m)\big) = g\big(p(a_{m+1}), \ldots, p(a_{m+n})\big).$$

(*in other words, if* $(**_*)$, *then*

$$f(x_1, \ldots, x_n) = g(x_{m+1}, \ldots, x_{m+n})$$

for any sequence $x_1, \ldots, x_{m+n}$ satisfying the condition: if $a_i = a_j$, then $x_i = x_j$, where $i, j = 1, \ldots, m+n$).

(iii) *I is a set of independent elements if and only if any mapping of I into A may be extended to a homomorphism of I into A.*

We pass to another equivalence:

(iv) *I is a set of independent elements if and only if the following two conditions are satisfied:*

(R_0) *no algebraic constant has an irreducible representation by elements of I,*

(R) *the irreducible representation of every element of $\bar{I} \setminus C$ by elements of I is determined up to the order of these elements.*

[6] See the Introduction and Marczewski [4], p. 732-723, 2 (i) and 2 (ii).

The implication (I)$\Rightarrow$(R$_0$) is obvious. In order to prove (I)$\Rightarrow$(R) let us suppose that

$$(**) \qquad d = f(a_1, \ldots, a_m), \quad d = g(b_1, \ldots, b_n)$$

are two irreducible representations of $d \in \bar{I} \setminus C$ by elements of I (see 1.3 (iii)). It must be proved that $m = n$, that the sequences $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_n)$ differ only in the order, and that f and g differ only in the corresponding permutation of variables.

Let us assume that a certain element of the first sequence, e.g. a_1, does not belong to the second. We infer that f does not depend on the first variable. If $d_1, \ldots, d_m$ is a sequence of elements of A, $d_1 \neq d_1^* \in A$, p is a mapping of I into A such that $p(a_j) = d_j$ and p^* is a mapping of I into A such that $p^*(x) = p(x)$ for $x \neq a_1$ and $p^*(a_1) = d_1^*$, then, by (ii),

$$f\big(p(a_1), \ldots, p(a_m)\big) = g\big(p(b_1), \ldots, p(b_n)\big)$$

and

$$f\big(p^*(a_1), \ldots, p^*(a_m)\big) = g\big(p^*(b_1), \ldots, p^*(b_n)\big)\,.$$

Since a_1 does not belong to b, the right-hand sides are equal here, whence

$$f(d_1, d_2, \ldots, d_n) = f(d_1^*, d_2, \ldots, d_n)\,.$$

Consequently, f does not depend on the first variable, which is impossible, the representations (**) being irreducible.

Hence, the sequences a and b differ only in the order of elements and the representation may be written in the following manner:

$$c = f(a_1, \ldots, a_m), \quad c = g^*(a_1, \ldots, a_m),$$

where g^* and g differ only in the order of variables.

In view of 1.2 (viii) the operation g^* is algebraic. Since $a_1, \ldots, a_n$ are independent, $f = g^*$.

It remains to prove (R$_0$)(R)$\Rightarrow$(I). Suppose (*), where $a_1, \ldots, a_n$ are different elements of I.

In view of (R$_0$), if one of the functions f and g is constant, then so is the other, whence $f = g$.

If neither f nor g is constant, let us reject all variables on which f and g respectively do not depend:

$$f(x_1, \ldots, x_n) \equiv f_0(x_{i_1}, \ldots, x_{i_p}), \quad g(x_1, \ldots, x_n) \equiv g_0(x_{j_1}, \ldots, x_{j_q})\,,$$

where $p \geqslant 1$ and $q \geqslant 1$. Hence, in view of (*),

$$f_0(a_{i_1}, \ldots, a_{i_p}) = g_0(a_{j_1}, \ldots, a_{j_q})$$

and, on account of (R), the systems $(i_1, \ldots, i_p)$ and $(j_1, \ldots, j_q)$ are identical, $f_0 = g_0$ and finally $f = g$.

Theorem (iv) is thus proved. Let us remark that (R$_0$) and independence are equivalent in some algebras (Boolean algebras [7], $\mathfrak{J}_k$, vector spaces, etc.).

Let us conclude with the following remark: the definition of independence given at the beginning of this section for finite sets may be applied also to finite sequences. And thus we obtain a simple relation between the notions of independence:

(v) $(a_1, \ldots, a_n)$ *is a sequence of independent elements if and only if there is no repetition in it and* $\{a_1, \ldots, a_n\}$ *is a set of independent elements.*

The sufficiency of the condition is trivial. In order to prove the necessity it suffices to show that a sequence $a_1, \ldots, a_{n-1}, a_n$ with a repetition, e.g. when $a_{n-1} = a_n$, is a sequence of dependent elements. In fact, we have

$$e_{n-1}^{(n)}(a_1, \ldots, a_n) = a_{n-1} = a_n = e_n^{(n)}(a_1, \ldots, a_n)\,,$$

although $e_{n-1}^{(n)} \neq e_n^{(n)}$.

The following example is important:

(vi) $a_1, \ldots, a_n, f(a_1, \ldots, a_n)$ *is a sequence of dependent elements.*

Let us suppose that $a_1, \ldots, a_n, f(a_1, \ldots, a_n)$ are independent and put

$$f(a_1, \ldots, a_n) = a_{n+1}\,.$$

Let be $a_{n+1}^* \neq a_{n+1}$. Then, by (ii),

$$f(a_1, \ldots, a_n) = a_{n+1}^*\,,$$

which is impossible.

2.3. Conclusions following from independence.

(i) *If* $\{a\}$ *is a one-element set of independent elements then* a *is not an algebraic constant.*

In fact, if c is an algebraic constant, then the constant function $f(x) \equiv c$ satisfies the conditions:

$$e_1^{(1)}(c) = f(c) \quad \text{and} \quad e_1^{(1)} \neq f\,,$$

whence $\{c\}$ is a set of dependent elements [8].

The theorem converse to (i) is not true: in the algebra $\mathfrak{J}_4$ the element 2 is not an algebraic constant while $\{2\}$ is a set of dependent elements.

(ii) *If* $\{a, b\}$ *is a set of two independent elements and* $f(a) = g(b)$, *then* f *and* g *are constant and equal.*

---

[7] Marczewski [6], p. 140, theorem 4 (i).

[8] Or, in other terms, c is a *self-dependent* element. Some properties of self-dependent elements have been proved by Nitka [9] and Goetz and Ryll-Nardzewski [2], p. 161, Theorem 8.

In fact, theorem 2.2 (ii) and the equality $f(a) = g(b)$ imply the equality $f(x) = g(y)$ for any $x, y \in A$.

(iii) *If I is a set of independent elements of A, B — a subalgebra of A, and $I \subset B$, then I is a set of independent elements in B.*

This follows from the fact that any two operations identical in A are identical in B.

The converse of (iii) is not true. The set $\{0, 2\}$ is a subalgebra of $\mathfrak{J}_4$, in which $\{2\}$ is a set of independent elements, while it is not in $\mathfrak{J}_4$.

In a certain special case the converse of (iii) is valid:

(iv) *If A is a homomorphical image of a subalgebra B of A, then independence in B implies independence in A.*

That is a direct consequence of the definition of independence and proposition 2.1 (i).

Proposition 2.2 (vi) implies

(v) *If I is a set of independent elements, then*

(G) *I is a minimal set of generators of $\bar{I}$, or, in other words, for any $a \in I$ we have $a \notin \overline{I \setminus \{a\}}$* (9).

The converse implication is not true: the set $\{2, 3\}$ is a minimal set of generators of $\mathfrak{J}_6$ while 2 and 3 are dependent. In fact, the operations $f(x) \equiv 2x$ and $g(x) \equiv 3x$ are algebraic in $\mathfrak{J}_6$ and $f(3) = g(2)$.

We shall consider one more conclusion of independence, which is interesting but will be not used in the sequel.

(vi) *If I is a set of independent elements, then*

(T) *for any subsets U and V of I we have $\overline{U} \cap \overline{V} = \overline{U \cap V}$.* (10)

The relation

$$\overline{U} \cap \overline{V} \subset \overline{U \cap V}$$

being trivial, it remains to prove that

$$\overline{U} \cap \overline{V} \supset \overline{U \cap V}.$$

This inclusion is true if $U = 0$ or $V = 0$. Thus, let us suppose $U \neq 0 \neq V$ and $d \in \overline{U} \cap \overline{V}$. Hence

$$(\dagger) \qquad d = f(a_1, \ldots, a_m) = g(b_1, \ldots, b_n)$$

where $a = (a_1, \ldots, a_m)$ is a sequence of different elements of U and $b = (b_1, \ldots, b_n)$ a sequence of different elements of V. First let us consider the case where a and b are disjoint. Since I is a set of independent elements, we have, in view of 2.2 (ii),

$$f(x_1, \ldots, x_m) = g(b_1, \ldots, b_n)$$

(9) See Marczewski [4], p. 733, 2 (iii).

(10) Condition (T) is considered by J. Schmidt, *Mehrstufige Austauschstrukturen*, Zeitschr. Math. Logik Grundlagen Math. 2 (1956), pp. 233-249, in particular p. 248. (Added in proof.)

for any sequence $x_1, \ldots, x_m$ of elements of A. Consequently f is constant and d an algebraic constant in A. Hence $d \in \overline{U} \cap \overline{V}$, by the definition of the algebraic closure.

Let us pass to the case where there is an element in the sequence a, say a_1, which belongs to the sequence b. In the sequence

$$c = (a_1, \ldots, a_m, b_1, \ldots, b_n)$$

we replace by a_1 every element of b not belonging to a. Thus we obtain a new sequence

$$c^* = (a_1, \ldots, a_m, a_1^*, \ldots, a_n^*)$$

such that if two elements of c are equal, then the corresponding two elements of c^* are also equal. Consequently, the elements of I being independent, we have in view of (+) and 2.2 (ii):

$$f(a_1, \ldots, a_m) = g(a_1^*, \ldots, a_n^*).$$

Every element of the sequence $a_1^*, \ldots, a_n^*$ belongs simultaneously to a and b, whence

$$d = g(a_1^*, \ldots, a_n^*) \in \overline{U} \cap \overline{V}, \qquad \text{q.e.d.}$$

It is easy to see that the converse of (v) is not true. Namely a set satisfying (T) also satisfies (T) after a set of algebraic constant has been added, while a set containing an algebraic constant is a set of dependent elements (see (i)). There are also examples of sets of dependent elements containing no algebraic constant but satisfying (T), e.g. the set $\{2, 3\}$ in the algebra $\mathfrak{J}_6$.

Finally, let us remark that

(vii) *If a set I satisfies* (T) *and contains no algebraic constants, then I satisfies* (G).

In fact, in view of (T),

$$\{a\} \cap \overline{I \setminus \{a\}} \subset \overline{\{a\}} \cap \overline{I \setminus \{a\}} = \overline{0}$$

and, since a is not an algebraic constant, we obtain $a \notin \overline{I \setminus \{a\}}$, q.e.d.

The converse implication is not true: in the algebra $(a, b, c, d; f)$ where $f(a) = f(b) = c$ and $f(c) = f(d) = d$ the set $\{a, b\}$ satisfies (G) without satisfying (T).

2.4. Exchange theorem and bases.

(i) *If $I = I_1 \cup J$ is a set of independent elements of A, where I_1 and J are disjoint, and if h_1 is a homomorphism of $\bar{I}_1$ into A, and p an arbitrary mapping of J into A, then there exists a homomorphism h of $\bar{I}$ into A which is a common extension of h_1 and p.*

Since I is a set of independent elements, it follows from 2.2 (iii) that there exists a homomorphism h of $\bar{I}$ into A such that $h|J = p$ and $h|I_1 = h_1$. Consequently $h|\bar{I}_1 = h_1$ and theorem (i) is proved.

And now we can prove the following "exchange theorem":

(ii) *If $I = I_0 \cup J$ is a set of independent elements of A, where I_0 and J are disjoint, and if I_1 is a set of independent elements of A with $\bar{I}_0 = \bar{I}_1$, then $I_1 \cup J$ is a set of independent elements.*

Let p denote a mapping of $I_1 \cup J$ into A. The elements of I_1 being independent, we can apply 2.2 (iii) and we obtain a homomorphism h_1 of $\bar{I}_1 = \bar{I}_0$ into A with $h_1|I_1 = p|I_1$. Since I is a set of independent elements, there exists, by (i), a homomorphism h of $\bar{I} = \overline{I_0 \cup J} = \overline{I_1 \cup J}$ into A such that $h|I_1 = h_1|I_1 = p|I_1$ and $h|J = p|J$. Therefore h is an extension of p, whence, by 2.2 (iii), $I_1 \cup J$ is a set of independent elements, q.e.d.

(iii) *If I and J are two sets of elements independent in the algebra A and have the same cardinal number, then the subalgebras $\bar{I}$ and $\bar{J}$ are isomorphic.*

Let p denote a one-one mapping of I onto J. In view of 2.2 (iii) there exist a homomorphism h of $\bar{I}$ into A such that $h|I = p$ and also a homomorphism h^* of $\bar{J}$ into A such that $h^*|J = p^{-1}$. Obviously $h(\bar{I}) = \bar{J}$. We have

$$h^*\big(h(x)\big) = x \tag{0}$$

for $x \in I$, whence also for $x \in \bar{I}$. On account of (0) h is one-one, q.e.d.

Let us add that, in proposition (iii), the hypothesis of independence in A can not be replaced by independence in $\bar{I}$ or $\bar{J}$. In the following example I is a set of elements independent in $\bar{I}$, J is a set of elements independent in A, I and J are one-element sets and yet $\bar{I}$ and $\bar{J}$ are not isomorphic. Let $\mathfrak{A} = (A; \oplus)$ be the Cartesian product of $\mathfrak{J}_2$ and $\mathfrak{J}_4$, in the sense that A is the set of all pairs of integers (j, k), where $j = 0, 1$ and $k = 0, 1, 2, 3$, and

$$(j_1, k_1) \oplus (j_2, k_2) = \big(j_1 + j_2 (\mathrm{mod}\, 2), k_1 + k_2 (\mathrm{mod}\, 4)\big).$$

It suffices to put $I = \{(1, 0)\}$ and $J = \{(0, 1)\}$.

A set of independent generators of A is called a *basis* of A. There exist algebras with bases and algebras with no bases, e.g. it is easy to prove that the Boolean algebra $\mathfrak{B}_k$ of all subsets of an k-element set has a basis if and only if k is of the form 2^n [11].

Each basis is a minimal set of generators, but not conversely (cf. proposition 2.3 (v) and the example following it). Each basis is a maximal set of independent elements (in view 2.2 (vi)) but not conversely (e.g. the set $\{a\}$ in the Boolean algebra of all subsets of the set $\{a, b, c\}$).

[11] That is connected with the well-known theorem that $\mathfrak{B}_k$ is a free Boolean algebra if and only if $k = 2^n$. See e.g. Birkhoff [1], p. 163.

For any algebra $\mathfrak{A} = (A; F)$, the algebra $(A^{(n)}, F)$ (i.e. the algebra of all n-ary algebraic operations in A) has an n-element basis; namely it is not difficult to verify that the trivial n-ary operations in A form a basis.

This fact permits us to define an algebra having bases with different cardinal numbers. Here is an outline of this construction [12]. Let us put $A = \{1, 2, \ldots\}$ and denote by f a one-one transformation of A^2 onto A and by φ, ψ the inverse transformation:

$$(x, y) \to f(x, y), \qquad x \to \big(\varphi(x), \psi(x)\big).$$

For the algebra $\mathfrak{A} = (A; \varphi, \psi, f)$, the algebras of algebraic operations $\mathfrak{A}^{(1)} = (A^{(1)}; \varphi, \psi, f)$ and $\mathfrak{A}^{(2)} = (A^{(2)}, \varphi, \psi, f)$ are isomorphic and since $\mathfrak{A}^{(1)}$ has a one-element basis and $\mathfrak{A}^{(2)}$ a two-element basis, the algebra $\mathfrak{A}^{(1)}$ has bases with different cardinal numbers.

In this connection we shall prove that [13]

(iv) *If an algebra has bases with different cardinal numbers, then all these numbers are finite and form an infinite arithmetical progression.*

The finiteness of the numbers under consideration follows from 1.3 (iv) and consequently it only remains to prove that if there are in A bases with m, $m+k$ and n elements $(k, m, n = 1, 2, \ldots)$, then there exists a $n+k$-element basis of A.

Let us denote by $B_1 \cup B_2$ a $m+k$-element basis, where B_1 has m elements and B_2 k elements. In view of (iii) the algebras A and $\bar{B}_1$ are isomorphic and, consequently, $\bar{B}_1$ has a n-element basis B_1^*. The elements of B_1^* are independent in B_1 and, by 2.3 (iv), in A.

Since $\bar{B}_1^* = \bar{B}_1$, we may apply the exchange theorem (ii). Therefore $B_1^* \cup B_2$ is a set of independent elements. Obviously

$$\overline{B_1^* \cup B_2} = \overline{B_1 \cup B_2} = A;$$

in other words $B_1^* \cup B_2$ is an $n+k$-element basis of A.

The theorem is thus proved.

The converse theorem is also true: *Any arithmetical progression is the set of numbers of elements of all bases of a certain algebra* [14].

[12] Cf. Jónnson and Tarski [3], and Goetz and Ryll-Nardzewski [2], p. 159.

[13] That is a strengthening of a theorem by Świerczkowski ([1], Theorem 2, p. 750). I use here some ideas of Ryll-Nardzewski. Another proof of (iv) is contained in the paper of Goetz and Ryll-Nardzewski [2], p. 157-159, Theorem 5. Recently S. Świerczkowski proved a theorem on free algebras containing (iv) as a special case ([13], Theorem 1).

[14] The theorem first proved by Goetz and Ryll-Nardzewski [2] under some additional hypotheses concerning the progression considered and then, without restriction, by Świerczkowski [13].

2.5. Independence and mappings.

(i) *If a homomorphism h of $\bar{J}$ into A is one-one on J and if $h(J)$ is a set of independent elements, then J is also a set of independent elements.*

In fact, if $a_1, \ldots, a_n$ are different elements of J and

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

then

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

whence

$$f\big(h(a_1), \ldots, h(a_n)\big) = g\big(h(a_1), \ldots, h(a_n)\big).$$

Since $h(a_i)$ are different and independent by hypothesis, we have $f = g$, q.e.d.

(ii) *Let $a_1, \ldots, a_s \in A$ and $f_1, \ldots, f_n \in A^{(s)}$. If $f_1(a_1, \ldots, a_s), \ldots, f_n(a_1, \ldots, a_s)$ are independent and $b_1, \ldots, b_s$ are independent, then $f_1(b_1, \ldots, b_s), \ldots, f_n(b_1, \ldots, b_s)$ are independent.*

Let us suppose that

$$g\big(f_1(b_1, \ldots, b_s), \ldots, f_n(b_1, \ldots, b_s)\big) = g^*\big(f_1(b_1, \ldots, b_s), \ldots, f_n(b_1, \ldots, b_s)\big).$$

Hence, in view of the independence of $b_1, \ldots, b_s$,

$$g\big(f_1(a_1, \ldots, a_s), \ldots, f_n(a_1, \ldots, a_s)\big) = g^*\big(f_1(a_1, \ldots, a_s), \ldots, f_n(a_1, \ldots, a_s)\big),$$

and, finally $g = g^*$ by the independence of $f_1(a_1, \ldots, a_s), \ldots, f_n(a_1, \ldots, a_s)$.

References

[1] G. Birkhoff, *Lattice theory*, New York 1945.

[2] A. Goetz and C. Ryll-Nardzewski, *On bases of abstract algebras*, Bulletin de l'Académie Polonaise des Sciences, Série des Sc. Math. Astr. et Phys. 8 (1960), pp. 157-162.

[3] B. Jónnson and A. Tarski, *Two general theorems concerning free algebras*, Bulletin of the Americal Mathematical Society 2 (1956), p. 554.

[4] E. Marczewski, *A general scheme of the notions of independence in mathematics*, Bulletin de l'Académie Polonaise des Sciences, Série des Sc. Math. Astr. et Phys. 6 (1958), pp. 731-736.

[5] — *Independence in some abstract algebras*, ibidem, 7 (1959), pp. 611-616.

[6] — *Independence in algebras of sets and Boolean algebras*, Fundamenta Mathematicae 48 (1960), pp. 135-140.

[7] — and K. Urbanik, *Algebras in which all elements are independent*, Bulletin de l'Académie Polonaise des Sciences, Série des Sc. Math. Astr. et Phys. 8 (1960), pp. 157-161.

[8] J. C. C. McKinsey and A. Tarski, *The algebra of topology*, Annals of Mathematics 45 (1944), pp. 144-191.

[9] W. Nitka, *Self-dependent elements of abstract algebras*, Colloquium Mathematicum 8 (1961), pp. 15-17.

[10] 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), pp. 749-752.

[11] — *Algebras independently generated by every n elements*, ibidem 7 (1959), pp. 501-502.

[12] — *On algebras which are independently generated by every n elements*, Fundamenta Mathematicae 49 (1960), pp. 93-104.

[13] — *On isomorphic free algebras*, Bulletin de l'Académie Polonaise des Sciences, Série Math. Astr. et Phys. 8 (1960), pp. 587-588, and Fundamenta Mathematicae, this volume, pp. 35-44.

[14] K. Urbanik, *Representation theorem for Marczewski's algebras*, Bulletin de l'Académie Polonaise des Sciences, Série Math. Astr. et Phys. 7 (1959), pp. 617-619, and Fundamenta Mathematicae 48 (1960), pp. 147-167.

Reçu par la Rédaction le 2. 8. 1960