

Independent sets in topological algebras

by

Jan Mycielski (Wrocław)

1. Introduction. In his well-known paper [14], J. von Neumann has proved that the set of values of the function

$$f(x) = \sum_{n=1}^{\infty} p([nx]) - p(n^2), \quad \text{where } p(t) = 2^t,$$

over the interval $0 < x < \infty$ is algebraically independent (i.e. for every polynomial $P(t_1, \dots, t_n)$ with integral coefficients the equality $P(f(x_1), \dots, f(x_n)) = 0$ with $0 < x_1 < \dots < x_n < \infty$ implies $P \equiv 0$). The function f is obviously increasing and therefore, by well-known results, we obtain that *there exists a perfect algebraically independent set of reals.*

Von Neumann's result has been applied in many constructions and especially for obtaining independent sets of potency 2^{\aleph_0} of rotations of the space \mathfrak{R}^3 , i.e. free subgroups of the rank 2^{\aleph_0} of the real orthogonal group \mathcal{O}_3 , and in other groups, sometimes satisfying some additional conditions (see [4], [5], [6], [7], [13], [15] and [16]). Using the above mentioned consequence of von Neumann's result all these constructions yield perfect independent sets.

It is the purpose of this paper to give a more general topological construction of such sets (the proof of von Neumann has an arithmetical character). E. Marczewski has introduced [10] a general notion of independence which provides the proper schema for these studies. His definition is repeated and slightly generalized in section 2. In section 3 the main theorems on the existence of independent sets in topological algebras are proved. In section 4 we give some applications, e.g. to Lie groups, their relations to known results, and some open problems.

2. Independence in algebras and relational systems. For any set (space) A and any natural number n , A^n denotes the Cartesian (topological) product of n copies of A .

Let $\mathfrak{R} = \langle A, \mathbf{R} \rangle$ be a *relational system*, i.e. A is a not empty set and \mathbf{R} is a set of finitary relations over A , i.e. for every $R \in \mathbf{R}$ there is

a natural number r called a *rank* of R such that $R \subseteq A^r$ (1). As usual, we will write $R(x_1, \dots, x_r)$ instead of $\langle x_1, \dots, x_r \rangle \in R$.

A set $X \subseteq A$ is called *independent in \mathfrak{R}* if, for every $R \in \mathbf{R}$ and every sequence $x_1, \dots, x_r \in X$, the relation $R(x_1, \dots, x_r)$ implies $R(f(x_1), \dots, f(x_r))$ for every mapping $f: \{x_1, \dots, x_r\} \rightarrow A$.

Let $\mathfrak{A} = \langle A, F \rangle$ be an *algebra*, i.e. A is a non empty set and for every $F \in F$ there is a natural number s such that $F: A^s \rightarrow A$ (2).

\mathfrak{R}^* denotes a relational system $\langle A, \mathbf{R} \rangle$, where A is the same as in \mathfrak{A} and \mathbf{R} is the set of all relations of the form

$$G(x_1, \dots, x_r) = H(x_1, \dots, x_r),$$

where G and H are any algebraic functions of \mathfrak{A} (the set of *algebraic functions* is the smallest set including F , all the functions E_j^i ($i \leq j$; $i, j = 1, 2, \dots$), where E_j^i is a function of j variables and $E_j^i(x_1, \dots, x_j) \equiv x_i$, and is closed under any superposition of functions).

A set $X \subseteq A$ is called *independent in (the algebra) \mathfrak{A}* if it is independent in \mathfrak{R}^* (3).

A relation $S \subseteq A^m$ is said to be obtained by *identification of variables* from a relation $R \subseteq A^{m+1}$ if S is of the form

$$S(x_1, \dots, x_m) \leftrightarrow R(x_1, \dots, x_i, x_j, x_{i+1}, \dots, x_m) \quad (i, j \leq m).$$

By the *closure* of a relational system $\mathfrak{R} = \langle A, \mathbf{R} \rangle$ we mean a relational system $\overline{\mathfrak{R}} = \langle A, \mathbf{S} \rangle$, where \mathbf{S} is the set of all relations obtainable from the relations of \mathbf{R} by repeated identification of variables.

A relation $S \subseteq A^m$ is said to be obtained by *permutation, identification, and cylindrification* from a relation $R \subseteq A^n$ if S is of the form

$$S(x_1, \dots, x_m) \leftrightarrow R(x_{k_1}, \dots, x_{k_n}),$$

where $k_i \in \{1, \dots, n\}$ for $i = 1, \dots, n$.

For any relational system $\mathfrak{R} = \langle A, \mathbf{R} \rangle$ we denote by $\overline{\mathfrak{R}} = \langle A, \mathbf{S} \rangle$ a relational system, where \mathbf{S} is the set of all relations obtainable from the relations of \mathbf{R} by permutation, identification and cylindrification.

The following elementary facts hold:

(1) For any algebra \mathfrak{A} we have $\overline{\mathfrak{R}^*} = \overline{\mathfrak{R}^*} = \mathfrak{R}^*$.

(2) Let be $\mathfrak{R} = \langle A, \mathbf{R} \rangle$, $\overline{\mathfrak{R}} = \langle A, \mathbf{S} \rangle$ and $X \subseteq A$; then the following propositions are equivalent

(1) In the standard treatments one considers an indexed system $\{R_t\}_{t \in T}$ rather than a set \mathbf{R} . But this would be redundant for the purpose of this paper.

(2) A remark analogous to (1) applies here. However this concept of an algebra was studied by logicians, the fact that it is sufficient for a theory of independence is due to Marczewski [10], [11].

(3) This definition of algebraic independence coincides with that of Marczewski [10], [11].

- (i) X is independent in \mathfrak{R} ;
 - (ii) X is independent in $\overline{\mathfrak{R}}$;
 - (iii) X is independent in $\overline{\mathfrak{R}}$;
 - (iv) For each $S \in \mathbf{S}$ if $S(x_1, \dots, x_s)$ holds for some different elements $x_1, \dots, x_s \in X$, then $S = A^s$.
- (3) If $X \subseteq A$ is independent in $\langle A, \mathbf{R} \rangle$ and S is the closure of \mathbf{R} under arbitrary unions and intersections (of relations of the same rank) then X is independent in $\langle A, \mathbf{S} \rangle$.

3. Independent sets in topological systems.

THEOREM 1. Let $\mathfrak{R} = \langle A, \{R_1, R_2, \dots\} \rangle$ be a closed relational system (i.e. $\overline{\mathfrak{R}} = \mathfrak{R}$) with a denumerable set of relations, where A is a complete metric space dense in itself and, for each i , $R_i = A^{r_i}$ or R_i is of the first category in A^{r_i} (r_i denotes the rank of R_i), and let G_1, G_2, \dots be a sequence of open non empty subsets of A . Then there exists a sequence of non empty perfect compact sets $F_j \subseteq G_j$ such that $\bigcup_{j=1}^{\infty} F_j$ is independent in \mathfrak{R} .

Proof. We represent each R_i in the form

$$R_i = \bigcup_{j=1}^{\infty} N_{ij},$$

where each N_{ij} is nowhere dense in A^{r_i} or each $N_{ij} = A^{r_i}$.

The relational system $\langle A, \{N_{ij}\}_{i,j=1,2,\dots} \rangle$ is not necessarily closed but, since \mathfrak{R} is closed, using (2) ((i) \leftrightarrow (iv)) we obtain for any $X \subseteq A$ the following proposition

(*) If for each i, j and each sequence of different elements $x_1, \dots, x_{r_i} \in X$ the relation $N_{ij}(x_1, \dots, x_{r_i})$ implies $N_{ij} = A^{r_i}$, then X is independent in \mathfrak{R} .

First, we will define inductively a system of open non empty sets $V_{i_1, \dots, i_m} \subseteq A$, where $i_j = 1, \dots, j$ and $m = 1, 2, \dots$, such that

- (i) $\overline{V_{i_1, \dots, i_m, i_{m+1}}} \subseteq V_{i_1, \dots, i_m}$ for $i_{m+1} < m+1$ (4) and $V_{i_1, \dots, i_m, m+1} \subseteq G_{m+1}$;
- (ii) $V_{i_1, \dots, i_m, i_{m+1}} \cap V_{i'_1, \dots, i'_m, i'_{m+1}} = \emptyset$, for $(i_1, \dots, i_{m+1}) \neq (i'_1, \dots, i'_{m+1})$;
- (iii) $\delta(V_{i_1, \dots, i_m}) \leq 1/m$; (5)
- (iv) if $i, j < m$ and x_1, \dots, x_{r_i} are any members of r_i different sets V_{i_1, \dots, i_m} then $N_{ij}(x_1, \dots, x_{r_i})$ implies $N_{ij} = A^{r_i}$.

We put $V_1 = G_1$.

(4) \overline{V} denotes the topological closure of V in the space A .
 (5) $\delta(V)$ denotes the diameter of V .

Suppose that all V_{i_1, \dots, i_m} are already defined and satisfy (i)-(iv). Since A is dense, we immediately obtain sets $V_{i_1, \dots, i_m, i_{m+1}}$ satisfying (i)-(iii). Let N_1, \dots, N_s denote the sequence of all these N_{ij} , with $i, j < m$, which are nowhere dense. Let $r(i)$ be the rank of N_i . Since N_1 is nowhere dense and each product $V_{i_1, \dots, i_1}^0 \times \dots \times V_{i_1^{r(1)}, \dots, i_{m+1}^{r(1)}}$ is open in $A^{r(1)}$, then there exist such non empty sets $V_{i_1, \dots, i_{m+1}}^1 \subseteq V_{i_1, \dots, i_{m+1}}^0$ that for any sequence of $r(1)$ different among them, say $V_{i_1^1, \dots, i_{m+1}^1}, \dots, V_{i_1^{r(1)}, \dots, i_{m+1}^{r(1)}}$, we have

$$N_1 \cap V_{i_1^1, \dots, i_{m+1}^1}^1 \times \dots \times V_{i_1^{r(1)}, \dots, i_{m+1}^{r(1)}}^1 = \emptyset.$$

Hence the system $V_{i_1, \dots, i_{m+1}}^1$ satisfies (i)-(iii) and (iv) pertaining to N_1 . Repeating this operation s times we obtain a system $V_{i_1, \dots, i_{m+1}}^s (= V_{i_1, \dots, i_{m+1}}^s)$ satisfying (i)-(iv), which concludes our inductive definition of the system V_{i_1, \dots, i_m} .

Now we put

$$F_j = \bigcup_{i_2=1}^2 \dots \bigcup_{i_{j-1}=1}^{j-1} \bigcap_{m=j+1}^{\infty} \bigcup_{i_{j+1}=1}^j \bigcup_{i_{j+2}=1}^{j+1} \dots \bigcup_{i_m=1}^{m-1} V_{1, i_2, \dots, i_{j-1}, i_j, i_{j+1}, i_{j+2}, \dots, i_m}.$$

Since A is complete, and by (i)-(iii), we see that F_j is perfect and compact (a homeomorph of Cantor's discontinuum) and $F_j \subseteq G_j$.

Now we have to prove the supposition of (*) for the set $X = \bigcup_{j=1}^{\infty} F_j$;

i.e. if x_1, \dots, x_r are different elements of $\bigcup_{j=1}^{\infty} F_j$ then $N_{ij}(x_1, \dots, x_r)$ implies $N_{ij} = A^r$. By (iii) there is an $m > i, j$ such that no two of these elements are in the same set V_{i_1, \dots, i_m} . Then, by (iv), we get this fact. Hence the conclusion of (*) concludes our proof.

Remarks. 1. It can be seen on the examples given in section 4 that in general if an independent set is borelian or only has the property of Baire, then it must be of the first category in A . But if A has a denumerable basis then we can obtain an independent set dense in A (taking as $\{G_1, G_2, \dots\}$ a basis of A).

2. The supposition ' A is metric and complete' could be replaced by ' A is locally compact' and then the theorem would be valid, if the conclusion ' F_j are perfect and compact' is replaced by ' F_j are of potency 2^{\aleph_0} '. This modification can be obtained by nearly the same proof only condition (iii) should be replaced by 'each set V_{i_1, \dots, i_m} is compact' and the definition of F_j should be replaced by ' F_j is any choice set for the family of sets $\{\bigcap_{m=1}^{\infty} V_{i_1, \dots, i_m} \mid i_1, i_2, \dots \text{ is any infinite sequence with } i_j = j \text{ and } i_{j+k} \in \{1, \dots, j+k-1\} \text{ for } k = 1, 2, \dots\}$ '.

3. In the proof of Theorem 1 and of the above modification the axiom of choice was used (e.g. in the construction of the system V_{i_1, \dots, i_m}). On the supposition that A is metric and has a well-ordered basis (e.g. a denumerable one, as in most applications given in this paper) and if the system of decompositions (=) is effectively given (e.g. in the proof of Theorem 2), then the axiom of choice is not needed in the proof.

A topological algebra is an algebra $\mathfrak{A} = \langle A, F \rangle$, where A is a Hausdorff topological space and all the functions $F \in F$ are continuous.

We will consider topological algebras with the following property:

\mathcal{P} . If G and H are any algebraic functions of r variables and there exist open non empty sets $V_1, \dots, V_r \subseteq A$ such that $G(x_1, \dots, x_r) = H(x_1, \dots, x_r)$ for any $x_1 \in V_1, \dots, x_r \in V_r$ then $G \equiv H$.

THEOREM 2. Let $\mathfrak{A} = \langle A, \{F_1, F_2, \dots\} \rangle$ be a topological algebra with property \mathcal{P} , where A is a complete metric space dense in itself, and let G_1, G_2, \dots be a sequence of open non empty subsets of A . Then there exists a sequence of non empty perfect compact sets $F_j \subseteq G_j$ such that $\bigcup_{j=1}^{\infty} F_j$ is independent in \mathfrak{A} .

Proof. In topological algebras property \mathcal{P} implies that for any algebraic functions G and H the relation

$$G(x_1, \dots, x_r) = H(x_1, \dots, x_r)$$

is equal to A^r or is nowhere dense in A^r . Hence, by (1), the relational system \mathfrak{A}^* satisfies the conditions of Theorem 1 and by this theorem we get Theorem 2. Q. E. D.

Remarks. 4. Theorem 2 has an obvious refinement in the spirit of Theorem 1 (to suppose only that \mathfrak{A}^* satisfies the conditions of Theorem 1). But the actual form seems natural and is adequate for applications.

5. Modifications of Theorem 2, analogous to the modifications of Theorem 1 given in Remarks 1 and 2, are also valid.

6. Remark 3 applies here also.

4. Applications and open problems. 1. The conditions of Theorem 2 are obviously satisfied if A is a connected real (or complex) analytic manifold and all the functions $F \in F$ are analytic mappings. This is the case of such algebras as the ring of real numbers $\mathfrak{R} = \langle \mathfrak{R}, \{+, \cdot\} \rangle$ or a connected Lie group $\mathfrak{G} = \langle \mathfrak{G}, \{\cdot, ^{-1}\} \rangle$. Hence, in both cases we obtain perfect independent sets, of course in the case of \mathfrak{R} this is an alternative proof of the consequence of von Neumann's result mentioned in section 1.

It was proved in [12] that any connected locally compact group \mathfrak{G} has property $\mathcal{P}^{(*)}$. Hence, by Remark 5, all such groups have independent sets of potency 2^{\aleph_0} (7). It is interesting that, in view of Remark 6, for the case of Lie groups this theorem is obtained without the axiom of choice, and the independent set is borelian (8).

This result on Lie groups (or connected locally compact groups) suggests the problem of studying the algebraic structure of their subgroups generated by the independent sets. It is clear that these subgroups are reduced free groups, i.e. they are of the form F/N , where F is a free group (of the rank 2^{\aleph_0}) and N is a fully invariant subgroup of F (the group of words vanishing on \mathfrak{G}). It is also obvious that they have no elements of finite order. Moreover, by the results of [2], if \mathfrak{G} is non solvable (e.g. compact and non abelian) then such subgroups of \mathfrak{G} are free. Hence, in general, these subgroups are free or solvable. Of course, some of these solvable groups are also nilpotent but no classification of these groups seems to be known (however it should be quite related to known results in the classification of Lie groups). (9)

2. If Y is a set of irrational numbers of the first category on the real line then there exists a perfect algebraically independent set X (and an independent dense union of such sets) such that the field generated by X is disjoint with Y .

Proof. Consider the relational system $\mathfrak{R} = \langle \mathcal{R}, \mathbf{R} \rangle$, where \mathcal{R} is the real line and \mathbf{R} is the set of all relations of the form

$$Q(x_1, \dots, x_n) = 0 \quad \text{or} \quad \frac{P(x_1, \dots, x_n)}{Q(x_1, \dots, x_n)} \in Y,$$

where P and Q are any polynomials with integral coefficients, $n = 1, 2, \dots$. It is easy to check that \mathfrak{R} satisfies all the suppositions of Theorem 1, and that the field generated by the independent set given by this theorem is disjoint with Y . Q. E. D.

The problem is open if the above result can be established with the supposition 'Y is of the first category' replaced by 'Y is of meas-

(6) In fact, the result of [12] is slightly stronger, but the problem if every connected topological group has property \mathcal{P} is still open.

(7) A special case of this result was proved in [2] (for non-solvable groups).

(8) While the method employed in [2] (even in the case of non-solvable Lie groups) was essentially non effective and yield only sets of potency 2^{\aleph_0} . The proof of [2] used also a refinement of the method of category for the case of analytic sets in analytic manifolds given in [1], and the present proof does not need this tool. However the result of [1] seems essential in another construction given in [3] quite related to those of the present paper.

(9) See also the problem stated in [2] section 6.3, which is still open.

ure 0^+ (10). The only known result in that case is the existence of an algebraically independent set of potency \aleph_1 generating a field disjoint with Y (unlike the previous result, this one requires the axiom of choice).

Proof. This follows by an obvious induction based on the axiom of choice and the following lemma:

If U is a denumerable real field disjoint with a set Y of measure 0 then there is a number x transcendental with respect to U and such that the field generated by $U \cup \{x\}$ is disjoint with Y .

Proof. Let A be the set of numbers algebraic in U . Of course, $\bar{A} \leq \aleph_0$. Let Φ be the set of all rational functions of one variable with coefficients in U . Of course $\bar{\Phi} \leq \aleph_0$ and $\text{mes}(\varphi^{-1}(Y)) = 0$ for every $\varphi \in \Phi$. Hence $\text{mes}(A \cup \bigcup_{\varphi \in \Phi} \varphi^{-1}(Y)) = 0$. It is enough to take $x \notin A \cup \bigcup_{\varphi \in \Phi} \varphi^{-1}(Y)$. Q.E.D.

In connection with this, since the set of Liouville numbers is of measure 0 but not of the first category, the following problem of P. Erdős remains open (if the continuum hypothesis is not supposed): Does there exist a real field of power 2^{\aleph_0} which does not contain any Liouville number? Another simple question of that kind (mine) is the following. Does there exist a perfect set of real numbers F such that the set of all numbers $x+y$ with $x, y \in F$ is disjoint with a given set of measure 0?

3. Let C be the complete metric space of real continuous periodic functions with period 1, the metric being $\max |f(x) - g(x)|$. Let $R_m(f, g)$ ($m = 1, 2, \dots$) denote the following relations:

There exist a real number x and a natural number n such that, for every $h > 0$,

$$|f(x+h) - f(x)|^m \leq |g(x+h) - g(x)| + nh.$$

It is easy to check that R_m are of the first category in $C \times C$ (11) and, of course, $R_m(f, f)$ holds for every $f \in C$. Therefore, by Theorem 1 we get a set $X \subseteq C$ perfect and compact and such that for every $f, g \in X$, $f \neq g$ and $m = 1, 2, \dots$ we have non- $R_m(f, g)$. The set X has great singularities, e.g. none of the functions $f \in X$ has both right derivatives finite and the same holds if we consider derivatives of one of these functions with respect to another (12).

(10) This problem and the following remarks of this point were kindly communicated to me by E. G. Straus. See also his review of a paper of P. Erdős in Math. Rev. 17 (1956), p. 460.

(11) Compare [9], § 30, VIII (references to related results are given there).

(12) A set with analogous properties was constructed by J. de Groot [8]. A problem concerning this subject given in [1] section 4.2 is still open. Note about paper [8] that like several papers quoted in section 1 it uses von Neumann's function. However, in opposite to the other papers, in [8] this is not essential since it is applied only to get a family of potency 2^{\aleph_0} of almost disjoint sets of natural numbers and this can be done in a more elementary way (see, e.g., [17] p. 77).

4. Other algebras satisfying the conditions of Theorem 2 are: (1) connected metric complete abelian groups (see [12]); (2) Boolean algebras of measurable sets divided by the ideal of sets of measure 0 with the metric $\text{mes}((A \cup B) \setminus (A \cap B))$.

5. Finally we give an application of Theorem 1 which has a more geometrical character in opposite to the algebraic character of most of the previous applications. A relevant case of this result was proved independently by A. Lelek.

If X is a set of the first category on the real line, $0 \in X$, and if A is a complete separable metric space such that for any open non-empty sets $U, V \subseteq A$ the set $\{\text{dist}(x, y) \mid x \in U, y \in V\}$ has interior points, then there exists a denumerable union of perfect sets, say U , which is dense in A and such that $\text{dist}(x, y) \in X$ for any $x, y \in U$.

Proof. Since the closure of the relational system $\langle \mathcal{R}, \{R\} \rangle$, where

$$R(x, y) \leftrightarrow \text{dist}(x, y) \in X$$

satisfies the conditions of Theorem 1.

An analogous theorem is also valid:

If A is a complete connected infinite metric space and X is as above then there exists a perfect compact set $F \subseteq A$ such that $\text{dist}(x, y) \in X$ for any $x, y \in F$.

The proof is quite analogous to that of Theorem 1, but this result is not a special case of the theorem. In fact, here a refinement with a sequence F_1, F_2, \dots satisfying some conditions like in Theorem 1 would not be valid in general.

References

- [1] S. Balcerzyk, Jan Mycielski, *On the method of category in analytic manifolds*, Fund. Math. 44 (1957), pp. 295-299.
 [2] — — *On the existence of free subgroups in topological groups*, ibidem, pp. 303-308.
 [3] — — *On faithful representations of free products of groups*, ibidem, 50 (1961), pp. 63-71.
 [4] Th. J. Dekker, *Decompositions of sets and spaces I, II*, Indag. Math. 18 (1956), pp. 581-595, and *III*, ibidem, 19 (1957), pp. 104-107.
 [5] — *On free groups of motions without fixed points*, ibidem, 20 (1958), pp. 348-353.
 [6] — *On free products of cyclic rotations groups*, Canadian J. Math. 11 (1959), pp. 67-69.
 [7] J. de Groot, *Orthogonal isomorphic representations of free groups*, ibidem, 8 (1956), pp. 256-262.
 [8] — *A system of continuous, mutually non-differentiable functions*, Math. Zeitschr. 64 (1956), pp. 192-194.
 [9] K. Kuratowski, *Topologie*, I, Warszawa 1958.

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

[11] — *Independence and homomorphisms in abstract algebras*, Fund. Math. 50 (1961), pp. 45-61.

[12] Jan Mycielski, *On the extension of equalities in connected topological groups*, ibidem, 44 (1957), pp. 300-302.

[13] — and S. Świerczkowski, *On free groups of motions and decompositions of the Euclidean space*, ibidem, 45 (1958), pp. 283-291.

[14] J. von Neumann, *Ein System algebraisch unabhängiger Zahlen*, Math. Ann. 99 (1928), pp. 134-141.

[15] W. Sierpiński, *Sur le paradoxe de la sphère*, Fund. Math. 33 (1945), pp. 235-244.

[16] — *Sur un ensemble plan qui se décompose en 2^{\aleph_0} ensembles disjoints superposables avec lui*, ibidem, 34 (1947), pp. 9-13.

[17] — *Cardinal and ordinal numbers*, Warszawa 1958.

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

Reçu par la Rédaction le 12. 3. 1963