Anzelm Iwanik; Jerzy Płonka
Linear independence in commutative semigroups

Matematický časopis, Vol. 25 (1975), No. 4, 333--338

Persistent URL: `http://dml.cz/dmlcz/126675`

LINEAR INDEPENDENCE IN COMMUTATIVE SEMIGROUPS

A. IWANIK—J. PŁONKA

The following definition of linear independence in abelian groups is known: The elements $a_1, \ldots, a_n$ ($a_i \neq 1$ for $i = 1, \ldots, n$) are linearly independent if for any integers $k_1, \ldots, k_n$ the implication

$$a_1^{k_1} \ldots a_n^{k_n} = 1 \quad \Rightarrow \quad a_1^{k_1} = \ldots = a_n^{k_n} = 1$$

holds [2]. In this paper we define a notion of linear independence in commutative semigroups and we examine some properties of linearly independent sets. In general we use the notation of Clifford and Preston [1].

§ 1

Let S be a commutative semigroup with identity 1. We shall write $a^0 = 1$ for each $a \in S$. We say that the set $A \subseteq S$ is linearly independent if for any different elements $a_1, \ldots, a_n$ of A and arbitrary $k_i, m_i \geqslant 0$ the implication

$$a_1^{k_1} \ldots a_n^{k_n} = a_1^{m_1} \ldots a_n^{m_n} \quad \Rightarrow \quad a_i^{k_i} = a_i^{m_i}$$

holds for every $i = 1, \ldots, n$. If S has no identity, then we say that a subset of S is linearly independent in S if it is linearly independent in S^1.

The linear independence in a semigroup S with identity 1 coincides with the G-independence (see e.g. [3]) in the monoid $(S, \cdot, 1)$.

The following properties of independent sets are simple consequences of the definition

(i) every one-element set is linearly independent,

(ii) every subset of a linearly independent set is linearly independent,

(iii) if A is linearly independent, then also is $A \cup \{1\}$,

(iv) if a two-element set $\{a, b\}$ is linearly independent, then $\langle a, 1\rangle \cap \langle b, 1\rangle = \{1\}$,

(v) if S is a subsemigroup of a commutative semigroup T with identity 1, then a subset A of S is linearly independent in T iff it is linearly independent in $S \cup \{1\}$.

Observe that if S is an abelian group, then a set A with $1 \notin A \subseteq S$ is linearly independent in S iff it is linearly independent in S in a group sense. Thus, by (v) we obtain

(vi) if $\varphi : S \to G$ is an isomorphism of a semigroup S into an abelian group G, then a set $A \subseteq S$, $1 \notin A$, is linearly independent in S iff $\varphi(A)$ is linearly independent in G in a group sense.

In particular, in the multiplicative semigroup of natural numbers, two numbers $a, b > 1$ are linearly independent iff $\log a/\log b$ is not a rational number.

We can see that a subset A of a commutative semigroup is linearly independent if each element of the semigroup $\langle A \rangle$ has a unique factorization as a product of elements from the semigroups $\langle a \rangle$, $a \in A$. We shall formulate this assertion more precisely.

Let $\{S_i : i \in I\}$ be a family of commutative semigroups with identity elements $e_i \in S_i$. Let $\sum^* S_i$ be a subdirect product of the S_i consisting of all the elements (s_i) of $\prod S_i$ with at most a finite number of components $s_i \neq e_i$. The mapping $\varphi_j(s) = (s_i)$, where $s_i = e_i$ for $i \neq j$ and $s_j = s$, is a natural embedding of S_j into $\sum^* S_i$. The semigroup $\sum^* S_i$ is generated by its subsemigroups $\varphi_j(S_j)$, $j \in I$. It is easy to see that the semigroup $\sum^* S_i$ is isomorphic to the direct sum of the S_i, amalgamating the identity semigroup $\{1\}$ (cf. [1] vol. 2, pp. 157, 161). If S_i are abelian groups, then $\sum^* S_i$ is their direct sum.

Observe that for each subset A of a commutative semigroup with identity there exists a natural homomorphism φ of $\sum\limits_{a \in A}^* \langle a, 1 \rangle$ onto $\langle A, 1 \rangle$ determined by $\varphi((s_a)) = s_{a_1} \ldots s_{a_n}$, where $s_a = 1$ for $a \notin \{a_1, \ldots, a_n\}$. Now the following lemma is evident:

Lemma 1. *Let S be a commutative semigroup with identity. A subset A of S is linearly independent iff the natural homomorphism of $\sum\limits_{a \in A}^* \langle a, 1 \rangle$ onto $\langle A, 1 \rangle$ is an isomorphism.*

E.g. in the multiplicative semigroup of natural numbers N the set of primes P is linearly independent and $N = \langle P, 1 \rangle \cong \sum\limits_{a \in A}^* \langle p, 1 \rangle$.

§ 2

A linearly independent set of generators of a commutative semigroup S (if it exists) will be called a basis of S. A basis B of S is an essentially minimal set of generators in the sense that if $b \in B$ and $b \neq 1$, then $\langle B \setminus \{b\} \rangle \neq S$. Indeed, if $\langle B \setminus \{b\} \rangle = S$, then $b = b_1^{k_1} \ldots b_n^{k_n}$ for some $b_i \in B$, $b_i \neq b$, $k_i \geqslant 1$, whence $b_1^0 \ldots b_n^0 b = b_1^{k_1} \ldots b_1^{k_n} b^0$ and $b = 1$. Analogously, B is an essentially maximal linearly independent set in the sense that if $a \notin B$ and $a \neq 1$, then the set $B \cup \{a\}$ is no more linearly independent.

Example. Let S be a Gaussian semigroup (see e.g. [4], p. 115) and let us write $a \sim b$ if a and b are associates, i.e. $a|b$ and $b|a$. $\sim$ is a congruence and $S/\sim$ is a Gaussian semigroup in which every non-indentity element has a unique factorization into irreducible elements. Hence, the irreducible elements together with the identity element form a basis of $S/\sim$.

It is worth to underline that (in the group case) the notion of basis used in the group theory (see e.g. [2]) substantially differs from the notion of basis in our semigroup sense, although the notions of linear independence are in both senses essentially the same. The difference is caused by the different generating in the two senses. E.g. the infinite cyclic group has not any basis in our semigroup sense. Moreover, it cannot be embedded in any semigroup with a basis. Indeed, suppose that an infinite cyclic group generated by a is a subgroup of a semigroup with a basis B. Then $a = b_1^{k_1} \dots b_n^{k_n}$ and $a^{-1} = c_1^{m_1} \dots c_r^{m_r}$ for some b_i, $c_j \in B$ and $k_i, m_j \geqslant 1$. The equality $aa^{-1} = (aa^{-1})^2$ implies that all $b_1, \dots, b_n$ have finite periods, which is a contradiction. From this fact and from Lemma 1 we obtain:

(vii) an abelian group has a basis (in our semigroup sense) iff it is a direct sum of finite cyclic groups.

In particular, by the Frobenius and Stickelberger theorem every finite abelian group has a basis in our semigroup sense.

The following two theorems describe some semigroup theoretical properties of a semigroup with a basis.

It is known that every commutative semigroup S can be decomposed into a semilattice of its Archimedean components. This decomposition is unique and the semilattice forms a maximal semilattice homomorphic image of S [1]. We shall describe this decomposition in the case when S has a basis.

Let B be a basis of a commutative semigroup S. Denote by B_0 the set of all $b \in B$ with $b^n = 1$ for some $n \geqslant 1$. From Lemma 1 it follows that $\langle B_0 \rangle$ is a direct sum of finite cyclic groups. Let $\mathscr{A}$ denote the family of all finite subsets of $B \backslash B_0$. Let us define for arbitrary $A = \{b_1, \dots, b_n\} \in \mathscr{A}$ a semigroup S_A consisting of all elements of the form $b_0 b_1^{k_1} \dots b_n^{k_n}$, where $b_0 \in \langle B_0 \rangle$ and $k_i \geqslant 1$ for $i = 1, \dots, n$ (take $S_A = \langle B_0 \rangle$ if $A = \emptyset$ and do not write b_0 if $B_0 = \emptyset$). Observe that the semigroups S_A, $A \in \mathscr{A}$ are mutually disjoint. Indeed, if $b_0 b_1^{k_1} \dots b_n^{k_n} = c_0 c_1^{m_1} \dots c_r^{m_r}$ and, say, $b_1 \notin \{c_1, \dots, c_r\}$, then $b_0 b_1^{k_1} \dots \dots b_n^{k_n} = c_0 b_1^0 c_1^{m_1} \dots c_r^{m_r} \Rightarrow b_1^{k_1} = 1$ which is a contradiction. It is easy to see that $S_A S_C \subseteq S_{A \cup C}$ and that $S = \cup S_A$. Observe now that S_A are Archimedean semigroups. In fact, let $b = b_0 b_1^{k_1} \dots b_n^{k_n}$ and $c = c_0 b_1^{m_1} \dots b_n^{m_n}$ with $b_0, c_0 \in \langle B_0 \rangle$ and $k_i, m_i \geqslant 1$. If b_0^{-1} and c_0^{-1} are inverses of b_0 and c_0 in B_0, then $bb_0^{-1} | c^r$ for r sufficiently large. Hence $b | c^r$ and analogously $c | b^q$ for q sufficiently large. Thus, we have the following theorem which is a generalization of a known fact for the multiplicative semigroup of natural numbers:

Theorem 1. *Let S be a commutative semigroup with a basis B, let $B_0 = \{b \in B\colon b^n = 1$ for some $n \geqslant 1\}$ and let $\mathscr{A}$ be the family of all finite subsets* *of $B \setminus B_0$. Then the family $\{S_A : A \in \mathscr{A}\}$ forms the decomposition of S into the semilattice $(\mathscr{A}, \cup)$ of its Archimedean components.*

From the theorem and from the uniqueness of the decomposition it follows that an Archimedean semigroup has a basis iff it is a cyclic semigroup or a direct sum of finite cyclic groups ($B_0 = \emptyset$ and $|B \setminus B_0| = 1$ or $B_0 = B$).

The next theorem characterizes these commutative semigroups with a basis which have a kernel, i.e. a minimal ideal.

Theorem 2. *Let S be a commutative semigroup with a basis B. S has a kernel iff S is periodic and has finitely many idempotents.*

Proof. Necessity. Let K be a kernel and suppose that $b \in B$ has an infinite period. For some $c \in K$ we have $cb \in K$. Ket $cb = b^n b_1^{m_1} \dots b_n^{m_n}$ with $b_i \neq b$, $b_i \in B$ for $i = 1, \dots, n$. Now taking only these elements $d \in K$ for which $db = b^m a_1^{k_1} \dots a_r^{k_r}$ with $m > n$, $a_i \neq b$ and $a_i \in B$, we would obtain a proper subideal of K. Hence, S is periodic. Suppose that S has infinitely many idempotents. Then the set $B \setminus B_0$ is infinite. Let k be the least natural number for which there is an element $c \in K$ with k elements from $B \setminus B_0$ in its representation. Taking only these elements of K for which at least $k + 1$ elements from $B \setminus B_0$ are needed, we would obtain a proper subideal of K.

Sufficiency. We can assume that $1 \in S$. The set $B \setminus B_0$ is finite, say, $B \setminus B_0 = \{b_1, \dots, b_n\}$. Denote by G_i the maximal subgroup of $\langle b_i \rangle$. Let $\bar{K}$ be the set of these elements from $\sum^*_{a \in B} \langle a, 1 \rangle$ which have their b_i-th components in G_i, $i = 1, \dots, n$. Observe that $\bar{K}$ is a kernel. In fact it is an ideal and a subgroup of $\sum^*_{a \in B} \langle a, 1 \rangle$. By Lemma 1 the last semigroup is isomorphic to S, which ends the proof.

§ 3

Let $\mathfrak{K}$ be an equational class of commutative semigroups. For each cardinal number $\mathfrak{n} \geqslant 1$ we denote by $F(\mathfrak{n}, \mathfrak{K})$ the free semigroup of $\mathfrak{K}$ generated by $\mathfrak{n}$ free generators.

Theorem 3. *Let $\mathfrak{K}$ be a non-trivial equational class of commutative semigroups. The set of free generators of $F(\mathfrak{n}, \mathfrak{K})$ is a basis of $F(\mathfrak{n}, \mathfrak{K})$ for each $\mathfrak{n} \geqslant 1$ iff $\mathfrak{K}$ is determined by an equality $x^k = x^m$ for some $k, m \geqslant 1$.*

Proof. Necessity. If an equality $x_1^{k_1} \dots x_n^{k_n} = x_1^{m_1} \dots x_r^{m_r}$ with k_i, $m_j \geqslant 0$ holds in $\mathfrak{K}$, then we can assume $n = r$ and we have $a_i^{k_i} = a_i^{m_i}$, where a_i are free generators of $F(\mathfrak{n}, \mathfrak{K})$, $n \leqslant \mathfrak{n}$, $i = 1, \dots, n$. Hence the equalities $x^{k_i} = x^{m_i}$ $i = 1, \dots, n$ hold in $\mathfrak{K}$. It is easy to see that any collection of equalities of the last form is equivalent to a single equality $x^k = x^m$ for some $k, m \geqslant 1$.

Sufficiency. If $\mathfrak{K}$ is determined by an equality $x^k = x^m$ for some $k, m \geqslant 1$, then it is easy to see that $F^1(\mathfrak{n}, \mathfrak{K}) \cong \sum^*_{i \in I} \langle a_i, 1 \rangle$, where $\{a_i : i \in I\}$ is the set of free generators. Now by Lemma 1 the proof is complete.

In particular, the class of semilattices satisfies the assumptions of Theorem 3 ($k = 2$, $m = 1$). It is easy to verify that a semilattice has a basis iff it is a free semilattice or a free semilattice with identity.

Let S be a commutative semigroup with a basis B. Each $a \in S$ can be represented in a form $a = b_1^{m_1} \dots b_r^{m_r}$ with $b_i \in B$, $m_i \geqslant 1$, $i = 1, \dots, r$. If $a_1, \dots, a_n \in S$, then we can write $a_i = b_1^{m_{i1}} \dots b_r^{m_{ir}}$ with $b_i \in B$ and $m_{ij} \geqslant 0$, where r and m_{ij} are minimal such integers. Each a_i is now determined by a finite sequence $(m_{i1}, \dots, m_{ir})$ of non-negative integers and the set $\{a_1, \dots, a_n\}$ is determined by a matrix (m_{ij}) with $i = 1, \dots, n$ and $j = 1, \dots, r$. We may identify the element a_i with the i-th row of the matrix.

Theorem 4. *Let S be a semigroup with a basis B and let $A = \{a_1, \dots, a_n\}$ be a finite subset of S determined by a matrix (m_{ij}) with $i = 1, \dots, n$ and $j = 1, \dots, r$.*

(a) *If S is periodic and $1 \notin \langle A \rangle$, then the set A is linearly independent iff a submatrix (m'_{ij}), $i, j = 1, \dots, n$, with $m'_{ij} = 0$ iff $i \neq j$ can be obtained by a permutation of rows and columns of the matrix.*

(b) *If each element of S has an infinite period, then the set A is linearly independent iff the matrix has rank n.*

Proof. (a) We shall prove first that if $a_1, \dots, a_n$ are linearly independent, then

(*) there are no disjoint non-empty sets A, C of rows of the matrix such that the sets $A^* = \{j : m_{ij} \neq 0$ for some $a_i \in A\}$, $C^* = \{j : m_{ij} \neq 0$ for some $a_i \in C\}$ were comparable by inclusion.

In fact, suppose that $A^* \subseteq C^*$ and $A = \{a_1, \dots, a_k\}$, $C = \{a_{k+1}, \dots, a_n\}$. If e_j denotes the idempotent of $\langle b_j \rangle$ then $(a_1 \dots a_k)^p = \prod_{j \in A^*} e_j$, $(a_{k+1} \dots a_n)^q = \prod_{j \in C^*} e_j$ for some $p, q > 0$. Therefore, $(a_1 \dots a_k)^p (a_{k+1} \dots a_n)^q = (a_{k+1} \dots a_n)^q$ and $a_1^p = \dots = a_k^p = 1$, which is a contradiction. It can be easily proved by induction that (*) implies the existence of a required *submatrix* (m'_{ij}). This, in turn, implies linear independence of the set A.

(b) Observe that by Lemma 1 there exists an isomorphism φ of the semigroup $\langle b_1, \dots, b_r \rangle$ into the additive group R of real numbers (e.g. φ may be determined by the mapping $b_i \to \log p_i$, where p_i are different primes, $i = 1, \dots, r$). The elements $a_1, \dots, a_n$ are linearly independent iff the elements $\varphi(a_1), \dots, \varphi(a_n)$ are linearly independent as the vectors of the linear space R over the field of rational numbers. Using the well-known results about linear spaces we get the proof.

In particular, Theorem 4 characterizes linearly independent sets in semigroups $F(\mathfrak{n}, \mathfrak{K})$, where $\mathfrak{n} \geqslant 2$ and $\mathfrak{K}$ is determined by an equality $x^k = x^m$.

§ 4

Now we shall outline some connections between linear and algebraic independence (see [5]).

(viii) In a commutative semigroup S with identity, the algebraic independence is stronger than the linear one.

Indeed, if $a_1, \dots, a_n \in S$ are algebraically independent and $a_1^{k_1} \dots a_n^{k_n} = a_1^{m_1} \dots a_n^{m_n}$ with, say $k_1 = \dots = k_{r-1} = 0$, $k_i > 0$ for $i \geqslant r$, and $m_j > 0$ for $j = 1, \dots, n$, then $x_r^{k_r} \dots x_n^{k_n} = x_1^{m_1} \dots x_n^{m_n}$ for any $x_1, \dots, x_n \in S$. In particular, if $x_i = a_i$ and $x_j = 1$ for $j \neq i$, then we obtain $a_i^{k_i} = a_i^{m_i}$ for $i = 1, \dots, n$.

Theorem 3 shows that, in general, (viii) is false for semigroups without identity. In the converse direction we have:

(ix) Let S be a commutative semigroup and let A be its linearly independent subset with $1 \notin \langle A \rangle$. If all elements of A have the same period m such that $m = \infty$ or the period of each element of S divides m then A is algebraic ally independent.

Indeed, if $a_1, \dots, a_n \in A$, $a_i \neq a_j$ for $i \neq j$ and $a_1^{k_1} \dots a_n^{k_n} = a_1^{m_1} \dots a_r^{m_r}$ with $k_i, m_j \geqslant 1$ then $n = r$ and $a_i^{k_i} = a_i^{m_i}$ for $i = 1, \dots, n$, whence $x^{k_i} = x^{m_i}$ and $x_1^{k_1} \dots x_n^{k_n} = x_1^{m_1} \dots x_r^{m_r}$ for any $x, x_1, \dots, x_n \in S$, which proves (ix).

Let S be a semilattice and let A be a subset of S with $1 \notin A$. The set A is algebraically independent in S iff it is algebraically independent in S^1 (see e.g. [6]) therefore iff it is linearly independent in S (by (viii) and (ix)). A complete characterization of algebraic independence in semilattices is given in [6]. If $1 \in A$ then we can consider the set $A \setminus \{1\}$ which is linearly independent iff A is. Hence we get a characterization of linear independence in semilattices.

REFERENCES

[1] CLIFFORD, A. H.—PRESTON, G. B.: The Algebraic Theory of Semigroups. Amer. Math. Soc., Providence 1961, 1967.

[2] FUCHS, L.: Abelian Groups. Budapest 1958.

[3] GŁAZEK, K.: Independence with respect to family of mappings in abstract algebras. Dissertationes Mathematicae, 81, 1971.

[4] JACOBSON, N.: Lectures in Abstract Algebra. Vol. 1, Basic Concepts. Van Nostrand, Princeton 1951.

[5] MARCZEWSKI, E.: Independence and homomorphisms of in abstract algebras. Fundam. math. 50, 1961, 45—61.

[6] SZÁSZ, G.: Marczewski independence in lattices and semilattices. Colloq. math. 10, 1963, 10—20.

Received October 17, 1973

Institute of Mathematics and Theoretical Physics
Technical University
Wrocław
Institute of Mathematics
Polish Academy of Sciences
Wrocław