Ladislav Skula

Prime elements in the semigroup of finite types of partially ordered sets in cardinal multiplication

Archivum Mathematicum, Vol. 4 (1968), No. 2, 97--101

Persistent URL: `http://dml.cz/dmlcz/104655`

PRIME ELEMENTS IN THE SEMIGROUP OF FINITE TYPES OF PARTIALLY ORDERED SETS IN CARDINAL MULTIPLICATION

Ladislav Skula, Brno

Received January 5, 1968

1. INTRODUCTION

Let us denote $\mathscr{G}$ a set of all types of finite non-empty partially ordered sets with an operation of cardinal product (G. Birkhoff [1], [2]). The set $\mathscr{G}$ with this operation forms a commutative semigroup in which, as M. Novotný has shown ([7], 4.6), the cancellation law holds. If $\mathscr{S}$ is the set of all connected types of $\mathscr{G}$, then $\mathscr{S}$ forms with regards to the operation of cardinal multiplication a sub-semigroup of the semigroup $\mathscr{G}$ and it follows from the theorem of Hashimoto [4] that $\mathscr{S}$ is a semigroup with a unique decomposition into irreducible elements.[1])

In the semigroup $\mathscr{G}$ evidently holds the minimum condition,[2]) J. Hashimoto and T. Nakayama, however, have shown in [5], $\mathscr{G}$ is not a semigroup with a unique decomposition into irreducible elements. The main result of this work is Theorem 3.2 which gives us all prime elements of the semigroup $\mathscr{G}$.[3]) The prime elements of the semi group $\mathscr{G}$ are just all irreducible elements of a semigroup $\mathscr{S}$ and types of antichains[4]) where the number of elements equals to the prime number.

In this paper there is being used the semigroup $\mathfrak{B}$ of all polynomials with countable set of variables, the coefficients of which are positive integers with an operation of usual multiplication. The semigroups $\mathscr{G}$ and $\mathfrak{B}$ are isomorphic, both regarding further operation $+$; the operation

---

[1]) An element g of a semigroup G is called an *irreducible element of the semigroup G* if the g is not a unity of G and it follows from the equation $g = ab$, $a, b \in G$ that a or b is a unity of G. A commutative semigroup G is called a *semigroup with a unique decomposition into the irreducible elements* if it has a unity element and no other units, and each element of G, different from the unity, may be uniquely written (excepting the order of factors) as a product of irreducible elements of G.

[2]) Say, *in the semigroup G holds the minimum condition* if for each sequence $\{g_n\}_{n=1}^{\infty}$, $g \in G$, g_{n+1}/g_n for each positive integers n (symbol / denote a usual symbol of divisibility) there exists such a positive integer m that g_m/g_{m+1}.

[3]) An element g of a semigroup G is called a *prime element of the semigroup G* if g is not a unity of G and from the relation g/g_1g_2 $(g_1, g_2 \in G)$ it follows g/g_1 or g/g_2.

[4]) An *antichain* is a partially ordered set, where each two different elements are incomparable.

$+$ on $\mathscr{G}$ denotes a cardinal sum (Birkhoff [1], [2]) and on $\mathfrak{B}$ the addition in a usual sense (J. Hashimoto and T. Nakayama [5]).

By means of the semigroup $\mathfrak{B}$, it can be shown, a cancellation law holds in $\mathscr{G}$ and the relation $g_1, g_2 \in \mathscr{G}$, n a positive integer $g_1^n = g_2^n$ implies $g_1 = g_2$ (3.1).

2. THE SEMIGROUP OF POLYNOMIALS WITH POSITIVE INTEGER COEFFICIENTS.

In this paper E is going to denote a set of all real numbers, E^∞ a Cartesian product of sets E_i ($i = 1, 2, \ldots$), where $E_i = E$ for each $i = 1, 2, \ldots$, then E^∞ will be a set of all $\mathbf{X} = (x_1, x_2, \ldots)$, $x_i \in E$ for each $i = 1, 2, \ldots$. The system of all mappings f of E^∞ into E of the form

$$f(\mathbf{X}) = \sum_{j=1}^{n} a_j \prod_{i=1}^{\infty} x_i^{n_i^j} \tag{1}$$

where $\mathbf{X} = (x_1, x_2, \ldots) \in E^\infty$, n_i^j are non-negative integers, a_j are integers and for each $1 \leqq j \leqq n$ there is $n_i^j = 0$, with an eventual exception of a finite number of i, we shall denote $\mathfrak{A}$.

If there is $f(\mathbf{X}) = a$, where a is an integer, for each $\mathbf{X} \in E^\infty$ we shall write $f = \mathbf{a}$.

For $f, g \in \mathfrak{A}$ put $f + g = h_1$, $f \,.\, g = h_2$, where $h_1(\mathbf{X}) = f(\mathbf{X}) + g(\mathbf{X})$, $h_2(\mathbf{X}) = f(\mathbf{X}) \,.\, g(\mathbf{X})$ for each $\mathbf{X} \in E^\infty$. There is $h_1, h_2 \in \mathfrak{A}$ and $\mathfrak{A}$ forms, with regard to the operations $+$ and . , a commutative ring with the unity element $\mathbf{1}$, called the ring of polynomials with variables $x_1, x_2, \ldots$ and with integral coefficients which is known to be an integral domain. (See e.g. [3] (IV, § 1, 4, T1) Russian translation p. 18.)

Let us denote $\mathfrak{B}$ ($\mathfrak{S}$) a system of all $f \in \mathfrak{A}$ which can be written in the form (1), where all a_j are positive integers ($n = a_1 = 1$). For $\mathbf{X} = (x_1, x_2, \ldots) \in E^\infty$ put $e_i(\mathbf{X}) = x_i$. Then $e_i \in \mathfrak{S}$ and the system of all e_i, $i = 1, 2, \ldots$ be denoted $\mathfrak{E}$. Evidently each $s \in \mathfrak{S}$ may be uniquely written in the form $s = \prod_{i=1}^{\infty} e_i^{n_i}$, where n_i are non-negative integers which equal, with an eventual exception of a finite number, to 0 (by the expression e_i^0 is mentioned $\mathbf{1}$). Each $f \in \mathfrak{B}$ may be uniquely written (excepting the order of summands) in the form

$$f = \sum_{i=1}^{n} a_i f_i,$$

where a_i are positive integers and f_i are each other different elements of $\mathfrak{S}$. This form will be called a canonical form of the element f.

For $f, g \in \mathfrak{B}$ is holds true $f + g \in \mathfrak{B}$ and $f \,.\, g \in \mathfrak{B}$. The set $\mathfrak{B}$ forms with regard to the operation. a commutative semigroup with a unity element $\mathbf{1}$. In this paragraph we shall understand by the semigroup $\mathfrak{B}$ this semigroup $(\mathfrak{B},.)$ and the relation of divisibility of elements in this semigroup is being indicated / unless mentioned otherwise.

2.1. **(a)** *$f, g, h \in \mathfrak{B}$, $fh = gh \Rightarrow f = g$.*

(b) *$f, g \in \mathfrak{B}$, $f^n = g^n$, n positive integer $\Rightarrow f = g$.*

Proof. The assertion (a) follows from the fact $\mathfrak{A}$ being an integral domain and it may be possible to cancel by non-zero element in every integral domain.

From [3] (IV, § 1, 5, exercise 3, Russian translation p. 40) follows that for $h, k \in \mathfrak{A}$, $h(\mathbf{X}) = k(\mathbf{X})$ for each $\mathbf{X} = (x_1, x_2, \ldots) \in E^\infty$, where $x_i > 0$ for each $i = 1, 2, \ldots$, $h = k$ holds. And hence, the statement (b) easily follows.

2.2. *Let p be a prime number. Then $\mathbf{p}$ is a prime element in $\mathfrak{B}$.*

Proof. Let $\mathbf{p}/fg$, f, $g \in \mathfrak{B}$, $f = \sum_{i=1}^{n} a_i f_i$, $g = \sum_{i=1}^{m} b_j g_j$ be canonical forms of elements f, g. Then there exists $h \in \mathfrak{B}$ so that $f \,.\, g = h \,.\, \mathbf{p}$. If $\mathbf{p} \nmid f$, $\mathbf{p} \nmid g$, we can suppose there exist $1 \leqq i_0 < n$, $1 \leqq j_0 < m$ so that $p/a_1, \ldots, a_{i_0}$, $p \nmid a_{i_0+1}, \ldots, a_n$, $p/b_1, \ldots, b_{j_0}$, $p \nmid b_{j_0+1}, \ldots, b_m$.[5])

Put $h_1 = \sum_{u=1}^{n-i_0} a_{i_0+u} f_{i_0+u}$, $h_2 = \sum_{v=1}^{m-j_0} b_{j_0+v} g_{j_0+v}$. Then there exists $h_0 \in \mathfrak{B}$ so that

$$h \,.\, \mathbf{p} = h_0 \,.\, \mathbf{p} + h_1 h_2 . \tag{2}$$

If it is supposed the members f_{i_0+n} of the polynomial h_1 and the members g_{j_0+v} of the polynomial h_2 are lexicographically ordered, we get from (2) $p/a_{i_0+1} \,.\, b_{j_0+1}$,[5]) which is a contradiction.

2.3. *Let $f \in \mathfrak{B} - \mathfrak{S}$ be a prime element of a semigroup $\mathfrak{B}$. Then $f = \mathbf{p}$, where p being a prime number.*

Proof. If there is $f = \mathbf{m}$, where $m = \mathrm{u} \,.\, \mathrm{v}$, u, v positive integers > 1, then $f/\mathbf{u} \,.\, \mathbf{v}$, $f \nmid \mathbf{u}$, $f \nmid \mathbf{v}$, which is a contradiction.

If there is not $f = \mathbf{m}$, where m is a positive integer, then there exist $f_1 \in \mathfrak{S} - \{\mathbf{1}\}$ and $f_2 \in \mathfrak{B}$ so that $f = f_1 + f_2$. There exists $e \in \mathfrak{E}$ so that e/f_1. If it were e/f_2, then it would be e/f, what is not possible as f being a prime element. There exist thus $g, h \in \mathfrak{B}$ so that $f = g + h$, e/g, $e \nmid h_i$, for each $i = 1, \ldots, n$, where $h = \sum_{i=1}^{n} a_i h_i$ is a canonical form of the polynomial h.

---

[5]) The symbol / is here related to the multiplicative semigroup of positive integers.

There exists a positive integer c so that e^c/g, $e^{c+1}\dagger g$. Let $g = \sum_{j=1}^{m} b_j g_j$ be a canonical form of the polynomial g. Then e^c/g_j for each $j = 1, \ldots, m$ and there exists j_0 $(1 \leqq j_0 \leqq m)$ so that $e^{c+1}\dagger g_{j_0}$. Then

(1) $e^{c+1}/g_i g_j$ for each $i, j = 1, \ldots, m$

(2) $e^{c+1}\dagger h_1 g_{j_0}$ and $e/h_1 g_{j_0}$

(3) $e \dagger h_i h_j$ for each $i, j = 1, \ldots, n$.

Since $g^2 = \sum_{i=1}^{m} \sum_{j=1}^{m} b_i b_j g_i g_j$, $gh = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j h_i g_j$, $h^2 = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i a_j h_i h_j$,

it follows from (1)—(3) than in polynomial $g^2 - gh + h^2$ there is at least one member with a negative coefficient and hence $g^2 - gh + h^2 \notin \mathfrak{B}$. Since in the ring $\mathfrak{A}$ there is $(g + h)(g^2 - gh + h^2) = g^3 + h^3$ and in $\mathfrak{A}$ it may be possible to cancel by each non-zero element, it holds $f = (g + h) \dagger (g^3 + h^3)$.

If $h^2 = (g + h)\, k$, where $k \in \mathfrak{B}$, then $\sum_{i=1}^{n} \sum_{j=1}^{n} a_i a_j h_i h_j = \sum_{j=1}^{m} \sum_{l=1}^{r} b_j c_l g_j k_l + \sum_{i=1}^{n} \sum_{l=1}^{r} a_i c_l h_i k_l$, where $\sum_{l=1}^{r} c_l k_l$ being a canonical form of the polynomial k. Since e/g_j for each $j = 1, \ldots, m$ and (3) holds, we get a contradiction. From this we get $(g + h) \dagger h^2$ and hence $(g + h) \dagger g(g + h) + h^2$. There is $(g + h)(g^4 + g^2h^2 + h^4) = (g^3 + h^3)(g^2 + gh + h^2)$, then $f/(g^3 + h^3) \cdot (g^2 + gh + h^2)$ and $f \dagger (g^3 + h^3)$, $f \dagger (g^2 + gh + h^2)$, which is a contradiction.

The assertion is then proved.

2.4. Theorem. *$f \in \mathfrak{B}$ is a prime element of a semigroup $\mathfrak{B}$ if and only if $f \in \mathfrak{E}$ or $f = \mathsf{p}$, where p is a prime number.*

Proof. It follows from 2.2 and 2.3 and from that $f \in \mathfrak{S}$ being a prime element in $\mathfrak{B}$ just when $f \in \mathfrak{E}$.

3. APPLICATION ON FINITE TYPES OF PARTIALLY ORDERED SETS.

Let $\mathscr{G}, \mathscr{S}$ and $\mathfrak{B}$ have the same meaning as in the preceding part of this paper. The semigroup $\mathscr{S}$ evidently has a countable set of irreducible elements and let they be denoted $s_1, s_2, \ldots$. Let *1* denote the type of one-element partially ordered set. Put $\mathsf{F}(1) = \mathbf{1}$ and for $s \in \mathscr{S}$, $s = s_{i_1}^{n_1} \ldots s_{i_j}^{n_j}$, where $i_1, \ldots, i_j, n_1, \ldots, n_j$ $(j \geqq 1)$ are positive integers, put $\mathsf{F}(s) = e_{i_1}^{n_1} \ldots e_{i_j}^{n_j}$. Let $g \in \mathscr{G}$. Then g may be uniquely written (excepting the order of summands) in the form $g = g_1 + \ldots + g_n$, where $g_1, \ldots, g_n \in \mathcal{S}$, $n \geqq 1$ (the operation $+$ denotes a cardinal sum) Put $\mathsf{F}(g) = \mathsf{F}(g_1) + \ldots + \mathsf{F}(g_n)$. Then F is a one-to-one mapping of $\mathcal{G}$ on $\mathfrak{B}$ preserving the operations $+$ and . (J. Hashimoto and T. Nakayama [5]). Hence and from 2.1 the following assertion follows:

3.1. (a) *If there is* $g_1, g_2, g \in \mathcal{G}$, $g_1 g = g_2 g$, *then* $g_1 = g_2$.

(b) *If there is* $g_1, g_2 \in \mathcal{G}$, *n positive integer*, $g_1^n = g_2^n$, *then* $g_1 = g_2$.

Without the help of the semigroup $\mathfrak{B}$, the assertion (a) has been proved by M. Novotný in [7] and the assertion (b) for $n = 2$ by Š. Mikoláš in [6].

The following theorem follows from 2.4:

3.2. Main Theorem. *The element* $\pi \in \mathcal{G}$ *is a prime element of the semigroup* $\mathcal{G}$ *if and only if* π *is an irreducible element of the semigroup* $\mathcal{S}$ *or a type of an antichain*[4]) *whose number of elements equals to a prime number.*

REFERENCES

[1] G. Birkhoff, *Lattice Theory*, rev. ed., New York 1948.

[2] G. Birkhoff, *Generalized arithmetic.* Duke Math. Journ. 9 (1942), 283—302.

[3] Bourbaki, *Éléments de Mathématique, Algèbre,* Livre II, Paris, Russian translation:
Н. Бурбаки, *Элементы математики, Алгебра,* многочлены и поля, упорядоченные группы, издательство Наука, Москва 1965.

[4] J. Hashimoto, *On direct product decomposition of partially ordered sets.* Annals of Math., 54 (1951), 315—318.

[5] J. Hashimoto and T. Nakayama, *On a problem of G. Birkhoff,* Proceedings of the American Mathematical Society, vol. 1 (1950), 141—142.

[6] Š. Mikoláš, *Über ein Problem aus der Kardinalarithmetik,* Publ. Fac. Sci. Univ. J. E. Purkyně, Brno, Tchécoslovaquie, No 478 (1966), 427—431.

[7] M. Novotný, *Über Kardinalprodukte,* Zeitsch. f. math. Logik und Grundlagen d. Math., Bd. 9 (1963), 13—20.

Katedra algebry a geometrie
Universita J. E. Purkyně, Brno
Czechoslovakia