Ladislav Skula

Special isomorphisms of $F[x_1, \dots, x_n]$ preserving GCD and their use

Czechoslovak Mathematical Journal, Vol. 59 (2009), No. 3, 759–771

Persistent URL: http://dml.cz/dmlcz/140514

Czechoslovak Mathematical Journal, 59 (134) (2009), 759–771

SPECIAL ISOMORPHISMS OF $F[x_1, \ldots, x_n]$ PRESERVING GCD AND THEIR USE

Ladislav Skula, Brno

(Received February 25, 2008)

Abstract. On the ring $R = F[x_1, \ldots, x_n]$ of polynomials in n variables over a field F special isomorphisms A's of R into R are defined which preserve the greatest common divisor of two polynomials. The ring R is extended to the ring $S\colon = F[[x_1, \ldots, x_n]]^+$ and the ring $T\colon = F[[x_1, \ldots, x_n]]$ of generalized polynomials in such a way that the exponents of the variables are non-negative rational numbers and rational numbers, respectively. The isomorphisms A's are extended to automorphisms B's of the ring S. Using the property that the isomorphisms A's preserve GCD it is shown that any pair of generalized polynomials from S has the greatest common divisor and the automorphisms B's preserve GCD . On the basis of this Theorem it is proved that any pair of generalized polynomials from the ring $T = F[[x_1, \ldots, x_n]]$ has a greatest common divisor.

Keywords: polynomials in several variables over field, generalized polynomials in several variables over field, isomorphism of the ring of polynomials, automorphism of the ring of generalized polynomials, greatest common divisor of generalized polynomials

MSC 2010: 13F20, 13A05

0. Introduction

In this paper special isomorphisms $A = A(m_1, \ldots, m_n)$ ($m_1, \ldots, m_n$ are positive integers) of the integral domain $R = F[x_1, \ldots, x_n]$ of polynomials over a field F in the indeterminates $x_1, \ldots, x_n$ into R are defined and it is shown (Theorem 2.4) that these isomorphisms preserve the greatest common divisor of two polynomials from R.

The integral domain $R = F[x_1, \ldots, x_n]$ is extended to the integral domain $S = F[[x_1, \ldots, x_n]]^+$ and $T = F[[x_1, \ldots, x_n]]$ of generalized polynomials in such a way

Published results were acquired using the subsidization of the Ministry of Education, Youth and Sports of the Czech Republic, research plan MSM0021630518 "Simulation modelling of mechatronic systems".

that the exponents of the indeterminates are non-negative rational numbers and rational numbers, respectively.

Each isomorphism $A = A(m_1, \ldots, m_n)$ is extended in the natural way to the automorphism $B = B(m_1, \ldots, m_n)$ of the ring S and, using Theorem 2.4, we prove (Theorem 3.4) that any pair of generalized polynomials from S has a greatest common divisor (GCD) in S and the automorphism B preserves GCD.

In conclusion, the GCD-Existence Theorem (Theorem 4.6) is shown for the ring $T = F[[x_1, \ldots, x_n]]$ by applying the previous theorem to the ring $S = F[[x_1, \ldots, x_n]]^+$.

Investigation of this topic is motivated by the concept of derivative and integral of real order (the order is a real number) appearing in engineering applications [1], [3]. This will be described in greater detail in the paper [4], which is being prepared.

0.1. Notation.

Throughout this paper, F denotes a field and $R = F[x_1, \ldots, x_n]$ the integral domain of polynomials over the field F in the indeterminates $x_1, \ldots, x_n$ (n is a positive integer).

It is well known that $R = F[x_1, \ldots, x_n]$ is a unique factorization domain (UFD) and, therefore, any pair of elements of R has a greatest common divisor (GCD). The group of units $U(R)$ of the ring R equals the group F^* of non-zero elements of the field F. If $f \in R$, $f \neq 0$, then we can write f uniquely (after possible relabeling) in the form

$$f = \sum_{i=1}^{N} t_i \alpha_i,$$

where N is a positive integer, $t_1, \ldots, t_N \in F^*$ and $\alpha_1, \ldots, \alpha_N$ are mutually different monomials in $F[x_1, \ldots, x_n]$. We call the monomial α_i ($1 \leqslant i \leqslant N$) a monomial of the polynomial f.

A ring will designate an integral domain.

If $\mathcal{R}$ is a ring, then $U(\mathcal{R})$ denotes the group of units of $\mathcal{R}$ and $\mathcal{R}^* := \mathcal{R} \setminus \{0_{\mathcal{R}}\}$. For $a, b \in \mathcal{R}$

$$a \underset{\mathcal{R}}{|} b$$

denotes element a dividing element b in the ring $\mathcal{R}$.

If the pair (a, b) has a greatest common divisor (GCD) in the ring $\mathcal{R}$, then it is determined uniquely up to a multiple of a unit of the ring $\mathcal{R}$. For the sake of simplicity and without danger of misunderstanding we will denote it by $(a, b)_{\mathcal{R}}$.

In addition, we use the following common notation:

$\mathbb{N}, \mathbb{N}_0, \mathbb{Q}, \mathbb{Q}^+$ is the set of all positive integers and non negative integers, rational numbers, non-negative rational numbers, respectively.

In this paper, only the basic notions and theorems of commutative algebra are used, which are presented for example in the books [2], [5].

1. Special isomorphisms of the ring $F[x_1,\dots,x_n]$

Notation 1.1. Let $m_1,\dots,m_n$ be positive integers. If $\alpha = x_1^{u_1}\dots x_n^{u_n}$ ($u_1,\dots, u_n \in \mathbb{N}_0$) is a monomial in the ring $R = F[x_1,\dots,x_n]$, put

$$A(\alpha) = A(m_1,\dots,m_n)(\alpha) = x_1^{m_1u_1}\dots x_n^{m_nu_n}.$$

Clearly, if α,β are monomials in R, then

$$A(\alpha\cdot\beta) = A(\alpha)\cdot A(\beta).$$

We extend the mapping a to an isomorphism from the ring R to itself as follows: If

$$f = \sum_{i=1}^{N} t_i\alpha_i \in R$$

($N\in\mathbb{N}$, $t_j\in F$, α_j is a monomial in R, $1\leqslant j\leqslant N$), we put

$$A(f) = A(m_1,\dots,m_n)(f) = \sum_{j=1}^{N} t_jA(\alpha_j).$$

It is easy to see that the value of $A(f)$ does not depend on the expression $\sum\limits_{j=1}^{N} t_j\alpha_j$ and then $A = A(m_1,\dots,m_n)$ is an isomorphism from the ring R to itself.

We put

$$\mathcal{A} = \mathcal{A}(F) = \{A = A(m_1,\dots,m_n)\colon\ m_1,\dots,m_n\in\mathbb{N}\}.$$

Remark. An isomorphism $A = A(m_1,\dots,m_n)$ from $\mathcal{A}$ can be characterized as the isomorphism A from the ring R to itself with the properties:

$$A(t) = t \quad \text{for each } t\in F$$

and

$$A(x_i) = x_i^{m_i} \quad \text{for each } 1\leqslant i\leqslant n.$$

For the composition $\circ$ of the isomorphisms from $\mathcal{A}$, we have

Proposition 1.2. *Let $a_1, \dots, a_n, b_1, \dots, b_n$ be positive integers. Then*

$$A(a_1, \dots, a_n) \circ A(b_1, \dots, b_n) = A(a_1 b_1, \dots, a_n b_n),$$

therefore $(\mathcal{A}, \circ)$ is a commutative monoid with a unity $A(1, \dots, 1)$ which satisfies the cancellation law.

Notation 1.3. Let p be a prime. The symbol

$$P = P(p) = P(p, F) = F[x_1^p, x_2, \dots, x_n]$$

will denote the set of all $f \in R$ that can be expressed in the form

$$f = \sum_{j=1}^{N} t_j \alpha_j$$

where $N \in \mathbb{N}$, $t_j \in F$, $\alpha_j = \prod\limits_{i=1}^{n} x_i^{a_{ij}}$, $a_{ij} \in \mathbb{N}_0$, $p \mid a_{1j}$, $1 \leqslant j \leqslant N$, $1 \leqslant i \leqslant n$.

Obviously, P is a subring of R and P is the image of the isomorphism $A(p, 1, \dots, 1) \in \mathcal{A}$; $P = A(p, 1 \dots, 1)(R)$.

Proposition 1.4. *Let p be a prime and* $\operatorname{char} F = p$*. Let $A = A(p, 1, \dots, 1) \in \mathcal{A}$. Then, for each relatively prime $f, g \in R$, we have*

$$(A(f), A(g))_R = 1_R.$$

Proof. Assume that $d \in R$, $d \underset{R}{|} A(f)$ and $d \underset{R}{|} A(g)$. Then there exists $h, l \in R$ such that $dh = A(f)$ and $dl = A(g)$. It follows that

$$d^p h^p = A(f^p), \quad d^p l^p = A(g^p).$$

Since $\operatorname{char} F = p$, we have $d^p, h^p, l^p \in P(p)$ and, applying the isomorphism A^{-1}, we get

$$f^p = A^{-1}(d^p) \cdot A^{-1}(h^p), \quad g^p = A^{-1}(d^p) \cdot A^{-1}(l^p).$$

Since $(f^p, g^p)_R = 1_R$, the polynomial $A^{-1}(d^p)$ is a unit of R, therefore $A^{-1}(d^p) = t \in F^*$ and $d^p = A(t) = t \in U(R)$. The result follows. $\square$

Notation 1.5. Let $f = f(x_1, \ldots, x_n) \in R$ and $f = \sum_{j=1}^{N} t_j \alpha_j$, where $N \in \mathbb{N}$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant N$. We define for $\tau \in F$ the polynomial $f(\tau x_1, \ldots, x_n) \in R$ as follows:

$$f(\tau x_1, \ldots, x_n) := \sum_{j=1}^{N} t_j \tau^{a_{1j}} \alpha_j.$$

In addition we need the following lemma, which can be proved by the usual technique.

Lemma 1.6. *Let $f = f(x_1, \ldots, x_n)$, $g = g(x_1, \ldots, x_n) \in R$ and $h = fg = h(x_1, \ldots, x_n) \in R$. Then, for $\tau \in F$, we have*

$$f(\tau x_1, \ldots, x_n) g(\tau x_1, \ldots, x_n) = h(\tau x_1, \ldots, x_n).$$

2. The splitting field of the polynomial $x^{p-1} + x^{p-2} + \ldots + x + 1$

Assumptions and notation 2.1. In this section we assume that p is a prime, $\operatorname{char} F \neq p$ and E is the splitting field of the polynomial $\varphi(x) := x^{p-1} + x^{p-2} + \ldots + x + 1$ over F.

Clearly

$$\begin{aligned} F[x_1^p, x_2, \ldots, x_n] &= P(p, F) = F[x_1, \ldots, x_n] \cap P(p, E) \\ &= R \cap P(p, E) = F[x_1, \ldots, x_n] \cap E[x_1^p, x_2, \ldots, x_n]. \end{aligned} \tag{1}$$

Let $\varepsilon \in E$ be a root of $\varphi(x)$ in the field E. Then $\varepsilon \neq 1$, ε^i $(1 \leqslant i \leqslant p-1)$ are different roots of the polynomial $\varphi(x)$ and the extension $E \supseteq F$ is Galois.

The Galois group of the extension $E \supseteq F$ will be denoted $\operatorname{gal}(E : F) = \Gamma$. We have, for each $\sigma \in \Gamma$,

$$\{\sigma(\varepsilon^i) \colon 1 \leqslant i \leqslant p-1\} = \{\varepsilon^i \colon 1 \leqslant i \leqslant p-1\}. \tag{2}$$

We put for $h \in E[x_1, \ldots, x_n]$, $h = \sum_{i=1}^{N} u_i \alpha_i$, $u_i \in E$, α_i a monomial in $E[x_1, \ldots, x_n]$ and $\sigma \in \Gamma$:

$$\overline{\sigma}(h) = \sum_{i=1}^{N} \sigma(u_i) \alpha_i.$$

(Note that the value $\overline{\sigma}(h)$ does not depend upon the expression $\sum\limits_{i=1}^{N} u_i\alpha_i$.) Thus $\overline{\sigma}$ is an automorphism of the ring $E[x_1,\dots,x_n]$ and we have

$$F[x_1,\dots,x_n] = \{h \in E[x_1,\dots,x_n]\colon\ \overline{\sigma}(h) = h \ \text{ for each } \ \sigma \in \Gamma\}. \tag{3}$$

Furthermore

$$\begin{aligned} &\text{if } \chi \in E[x_1,\dots,x_n], \text{ then } \chi \in P(p,E) = E[x_1^p, x_2,\dots,x_n] \\ &\qquad\qquad \text{if and only if } \chi(x_1,\dots,x_n) = \chi(\varepsilon x_1,\dots,x_n). \end{aligned} \tag{4}$$

Lemma 2.2. *Let $h \in F[x_1,\dots,x_n]$ and $h^{(i)} = h(\varepsilon^i x_1,\dots,x_n)$ for each $0 \leqslant i \leqslant p-1$. Then*

$$\prod_{i=0}^{p-1} h^{(i)} \in P(p,F) = F[x_1^p, x_2,\dots,x_n].$$

Proof. Put $\chi = \chi(x_1,\dots,x_n) = \prod\limits_{i=0}^{p-1} h^{(i)}$. Then $\chi \in E[x_1,\dots,x_n]$. Using Lemma 1.6 for the ring $E[x_1,\dots,x_n]$ yields

$$\chi(\varepsilon x_1,\dots,x_n) = \prod_{i=0}^{p-1} h(\varepsilon^{i+1}x_1,\dots,x_n) = \prod_{i=0}^{p-1} h(\varepsilon^i x_1,\dots,x_n) = \chi(x_1,\dots,x_n),$$

therefore $\chi \in P(p,E)$ by (4).

Assume $\sigma \in \Gamma$. Then, according to (2),

$$\overline{\sigma}(\chi) = \prod_{i=0}^{p-1} \overline{\sigma}(h(\varepsilon^i x_1,\dots,x_n)) = \prod_{i=0}^{p-1} h(\varepsilon^i x_1,\dots,x_n) = \chi$$

and, by (3), $\chi \in F[x_1,\dots,x_n]$. Hence $\chi \in P(p,E) \cap R = P(p,F)$ by (1). $\square$

Remark. The monoids $(\mathcal{A}(F),\circ)$ and $(\mathcal{A}(E),\circ)$ are isomorphic, where the isomorphism from $\mathcal{A}(E)$ onto $\mathcal{A}(F)$ is the restriction of isomorphisms from $\mathcal{A}(E)$ to the domain $F[x_1,\dots,x_n]$.

Proposition 2.3. *Let $A = A(p, 1, \dots, 1) \in \mathcal{A}(F)$, $f, g \in R$ with $(f, g)_R = 1_R$. Then*

$$(A(f), A(g))_R = 1_R.$$

P r o o f. In view of the previous remark we can consider A as an element of $\mathcal{A}(E)$.

Suppose that $d \in R$, $d \underset{R}{|} A(f)$ and $d \underset{R}{|} A(g)$. Then there exist $l, h \in R$ such that $dl = A(f)$ and $dh = A(g)$. Put $d^{(i)} = d(\varepsilon^i x_1, \dots, x_n)$, $l^{(i)} = l(\varepsilon^i x_1, \dots, x_n)$, $h^{(i)} = h(\varepsilon^i x_1, \dots, x_n)$ for each $0 \leqslant i \leqslant p-1$ and

$$\delta = \prod_{i=0}^{p-1} d^{(i)}, \quad \lambda = \prod_{i=0}^{p-1} l^{(i)}, \quad \chi = \prod_{i=0}^{p-1} h^{(i)}.$$

Using Lemma 1.6 then yields

$$d^{(i)} l^{(i)} = A(f)(\varepsilon^i x_1, \dots, x_n) = A(f),$$
$$d^{(i)} h^{(i)} = A(g)(\varepsilon^i x_1, \dots, x_n) = A(g),$$

therefore

$$\delta\lambda = A(f^p), \quad \delta\chi = A(g^p).$$

By Lemma 2.2 $\delta, \lambda, \chi \in P(p, F) = A(R)$, hence

$$A^{-1}(\delta)A^{-1}(\lambda) = f^p, \quad A^{-1}(\delta)A^{-1}(\chi) = g^p.$$

Since f, g are coprime in R, we get $A^{-1}(\delta) \in U(R) = t \in F^*$, therefore $\delta = AA^{-1}(\delta) = A(t) = t \in U(R)$. This concludes the proof. □

Remark. The proof of Proposition 2.3 affords also a proof of Proposition 1.4 (under the assumption $\operatorname{char} F = p$). In fact, Proposition 1.4 can be considered as a special case of Proposition 2.3. Then the splitting field E of the polynomial $\varphi(x)$ over F equals F and we can put $\varepsilon = 1$ the only root of $\varphi(x) = (x-1)^{p-1}$. However, for the sake of greater clearness, the case $\operatorname{char} F = p$ is presented separately.

Theorem 2.4. *Let $A = A(m_1, \dots, m_n) \in \mathcal{A}$ ($m_1, \dots, m_n \in \mathbb{N}$) and $f, g \in R = F[x_1, \dots, x_n]$. Then*

$$A((f, g)_R) = (A(f), A(g))_R.$$

P r o o f. I. Suppose that $(f, g)_R = 1_R$. By Proposition 1.4 and 2.3, we get the assertion for $A = A(p, 1, \dots, 1) \in \mathcal{A}$ where p is a prime. Since a monomial in the ring R does not depend on the order of indeterminates, the formula $(A(f), A(g))_R = 1_R$ is also valid for $A = A(1, \dots, 1, p, 1, \dots, 1) \in \mathcal{A}$.

Let $m_1, \ldots, m_n \in \mathbb{N}$, $m = m_1 \ldots m_n \neq 1$ and $m = p_1^{a_1} \ldots p_k^{a_k}$ be the canonical decomposition of m into primes. Using Proposition 1.2, we can prove Theorem 2.4 for coprime f, g by induction on $a_1 + \ldots + a_k$.

II. General case. Assume that $(f, g)_R = d$. Then there exist $l, h \in R$ such that $f = dl$, $g = dh$ and $(l, h)_R = 1_R$. Then $A(f) = A(d)A(l)$, $A(g) = A(d)A(h)$ and, since $A(h)$, $A(l)$ are coprime by part I, the result follows. $\square$

3. The ring $F[[x_1, \ldots, x_n]]^+$

Definition 3.1. The notion of a polynomial over the field F in the indeterminates $x_1, \ldots, x_n$ will be generalized to the notion of a generalized polynomial over the field F in the indeterminates $x_1, \ldots, x_n$ with non-negative rational exponents in such a way that the powers of indeterminates are non-negative rational numbers and, therefore, the monomials have the form

$$x_1^{a_1} \ldots x_n^{a_n}, \quad \text{where } a_1, \ldots, a_n \in \mathbb{Q}^+.$$

The set of all such generalized polynomials will be denoted $F[[x_1, \ldots, x_n]]^+$ and considered with the operations $+$ and $\cdot$ defined in the same way as for "ordinary" polynomials from $F[x_1, \ldots, x_n]$. It can easily be proved for the generalized polynomials that

$$F[[x_1, \ldots, x_n]]^+ = (F[[x_1, \ldots, x_n]]^+, +, \cdot)$$

is an integral domain, whose subring is the ring $R = F[x_1, \ldots, x_n]$. For the sake of simplicity, we put

$$S := (F[[x_1, \ldots, x_n]]^+, +, \cdot).$$

Definition 3.2. An isomorphism $A = A(m_1, \ldots, m_n) \in \mathcal{A}$ $(m_1, \ldots, m_n \in \mathbb{N})$ from R into R will be extended in the natural way to an automorphism $B = B(m_1, \ldots, m_n)$ of the ring S, more exactly, we put, for a monomial $\beta = x_1^{\beta_1} \ldots x_n^{\beta_n}$ $(b_1, \ldots, b_n \in \mathbb{Q}^+)$ in S,

$$B(\beta) = B(m_1, \ldots, m_n)(\beta) = x_1^{b_1 m_1} \ldots x_n^{b_n m_n}$$

and

$$B(f) = B(m_1, \ldots, m_n)(f) = \sum_{j=1}^{N} t_j B(\beta_j)$$

for $f = \sum\limits_{j=1}^{N} t_j \beta_j \in S$ $(N \in \mathbb{N}$, $t_j \in F$, β_j is a monomial in S, $1 \leqslant j \leqslant N)$.

The symbol $\mathcal{B}$ will denote the set $\{B = B(m_1, \ldots, m_n) \colon m_1, \ldots, m_n \in \mathbb{N}\}$. It is easy to show the following assertion:

Proposition 3.3.

(a) *For* $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{N}$, $B(a_1, \dots, a_n), B(b_1, \dots, b_n) \in \mathcal{B}$ *we have*

$$B(a_1, \dots, a_n) \circ B(b_1, \dots, b_n) = B(a_1 b_1, \dots, a_n b_n).$$

(b) $(\mathcal{B}, \circ)$ *is a commutative monoid with the unity* $B(1, \dots, 1)$ *satisfying the cancellation law which is isomorphic to the monoid* $(\mathcal{A}, \circ)$*. This isomorphism is the restriction of the automorphisms from* $\mathcal{B}$ *to the domain* $R = F[x_1, \dots, x_n]$*.*

(c) *If* $f_1, \dots, f_k \in S$ $(k \in \mathbb{N})$*, then there exists* $B \in \mathcal{B}$ *such that*

$$B(f_1), \dots B(f_k) \in R.$$

Now we will use the automorphisms from $\mathcal{B}$ and Theorem 2.4 to prove the GCD-Existence Theorem for the ring S.

Theorem 3.4. *Each pair of generalized polynomials from the ring* $S = F[[x_1, \dots, x_n]]^+$ *has a greatest common divisor in* S*.*

If $f, g \in S$ *and* $B \in \mathcal{B}$ *are such that* $B(f), B(g) \in R = F[x_1, \dots, x_n]$*, then*

$$B^{-1}((B(f), B(g))_R) = (f, g)_S.$$

P r o o f. Assume that $B \in \mathcal{B}$ with $B(f), B(g) \in R$ (such $B \in \mathcal{B}$ exists by Proposition 3.3 (c)). Let $d = (B(f), B(g))_R$ and $w = B^{-1}(d)$. We will show that w is a greatest common divisor of $\{f, g\}$ in S.

Since $d \underset{R}{|} B(f)$, $d \underset{R}{|} B(g)$, we have $w \underset{S}{|} f$, $w \underset{S}{|} g$, therefore w is a common divisor of f and g in S. Suppose that $h \in S$ with $h \underset{S}{|} f$, $h \underset{S}{|} g$. Then there exist $u, v \in S$ such that $hu = f$, $hv = g$. By Proposition 3.3 (c), there exists $C \in \mathcal{B}$ with $C(h), C(u), C(v) \in R$, thus

$$BC(h) \underset{R}{|} BC(f) \quad \text{and} \quad BC(h) \underset{R}{|} BC(g).$$

We get from Theorem 2.4

$$(BC(f), BC(g))_R = (CB(f), CB(g))_R = C((B(f), B(g))_R) = C(d)$$

and then $BC(h) \underset{R}{|} C(d)$. Thus there exists $r \in R$ with $r \cdot BC(h) = C(d)$. Applying the automorphism $(BC)^{-1}$ of the ring S, we get $(BC)^{-1}(r) \cdot h = B^{-1}(d) = w$ and $h \underset{S}{|} w$, which is what we wanted to prove. $\square$

Corollary 3.5. *If $f, g \in S = F[[x_1, \ldots, x_n]]^+$ and $C \in \mathcal{B}$, then*

$$(C(f), C(g))_S = C((f, g)_S).$$

In other words, the automorphisms of the ring S from $\mathcal{B}$ preserve the greatest common divisor of pairs of elements from S.

P r o o f. By Proposition 3.3 (c), there exists $B \in \mathcal{B}$ with $BC(f), BC(g) \in R$. Using Theorem 3.4, we obtain

$$BC((f, g)_S) = (BC(f), BC(g))_R = B((C(f), C(g))_S),$$

which proves that

$$C((f, g)_S) = (C(f), C(g))_S.$$

$\square$

4. The ring $F[[x_1, \ldots, x_n]]$

Definition 4.1. Similarly to a generalized polynomial with non-negative rational exponents in Definition 3.1, we will define a generalized polynomial over the field F in the indeterminates $x_1, \ldots, x_n$ with rational exponents. The monomials have the form

$$x_1^{a_1} \ldots x_n^{a_n}, \quad \text{where } a_1, \ldots, a_n \in \mathbb{Q}.$$

$F[[x_1, \ldots, x_n]]$ will denote the set of all such generalized polynomials with rational exponents and the operations $+$ and $\cdot$ are defined on this set in the same way as in the case of "ordinary" polynomials. It can be proved that $F[[x_1, \ldots, x_n]] := (F[[x_1, \ldots, x_n]], +, \cdot)$ is an integral domain, which, for the sake of simplicity, will be denoted T. Then

$$R = F[x_1, \ldots, x_n] \subseteq S = F[[x_1, \ldots, x_n]]^+ \subseteq T = F[[x_1, \ldots, x_n]],$$

where the inclusion $\subseteq$ is considered to be a subring.

In addition, we define the lexicographic order $\leqslant$ of monomials in $F[[x_1, \ldots, x_n]]$ in the usual way (under the assumption that the indeterminates $x_1, \ldots, x_n$ are linearly ordered.)

Suppose that $f = \sum\limits_{i=1}^{N} t_i \alpha_i \in T^*$, where $N \in \mathbb{N}$, $t_i \in F^*$ $(1 \leqslant i \leqslant N)$ and $\alpha_1, \ldots, \alpha_n$ are mutually different monomials in T. Let $1 \leqslant u, v \leqslant N$ such that $\alpha_i < \alpha_u$ for each $1 \leqslant i \leqslant N$, $i \neq u$ and $\alpha_v < \alpha_i$ for each $1 \leqslant i \leqslant N$, $i \neq v$. We call the monomial term $t_u \alpha_u$, $t_v \alpha_v$ the *highest term in* f, the *lowest term in* f, respectively writing $\alpha_u = \mathrm{ht}(f)$, $\alpha_v = \mathrm{lt}(f)$.

It is easy to see (as for "ordinary" polynomials):

Proposition 4.2. *If $f, g \in F[[x_1, \ldots, x_n]]$, $f \neq 0$, $g \neq 0$, then*

$$\mathrm{ht}(fg) = \mathrm{ht}(f) \cdot \mathrm{ht}(g), \quad \mathrm{lt}(fg) = \mathrm{lt}(f) \cdot \mathrm{lt}(g).$$

Proposition 4.3.

$$U(F[[x_1, \ldots, x_n]]) = \{t\alpha \colon t \in F^*, \ \alpha \text{ is a monomial in } F[[x_1, \ldots, x_n]]\}.$$

Proof. Suppose $f \in T$. If $f = t\alpha$ where $t \in F^*$ and α is a monomial in $F[[x_1, \ldots, x_n]]$ then, obviously, $f \in U(T)$ ($f^{-1} = t^{-1}\alpha^{-1}$).

Let $f \in U(T)$ and $f = \sum\limits_{i=1}^{N} t_i\alpha_i$ where $N \in \mathbb{N}$, $t_i \in F^*$ and α_i is a monomial in T for each $1 \leqslant i \leqslant N$. Let $\alpha_N < \alpha_{N-1} \ldots < \alpha_1$ in the lexicographic order of the monomials.

Assume that $N \geqslant 2$ and $\varphi = u\alpha$, $\psi = v\beta$ are the highest term in f^{-1} and the lowest term in f^{-1}, respectively ($u, v \in F^*$, α, β are monomials in T). By Proposition 4.2, we have

$$\begin{aligned} 1 &= \mathrm{ht}(f \cdot f^{-1}) = \mathrm{ht}(f) \cdot \mathrm{ht}(f^{-1}) = ut_1\alpha\alpha_1, \\ 1 &= \mathrm{lt}(f \cdot f^{-1}) = \mathrm{lt}(f) \cdot \mathrm{lt}(f^{-1}) = vt_N\beta\alpha_N, \end{aligned}$$

therefore $\alpha\alpha_1 = \beta\alpha_N$. However (since $\alpha_1 > \alpha_N$ and $\alpha \geqslant \beta$), we have $\alpha\alpha_1 > \beta\alpha_N$, which is a contradiction. Thus $N = 1$ and the result follows. □

Proposition 4.4. *Let $f, g \in S = F[[x_1, \ldots, x_n]]^+$, $f \neq 0$, $g \neq 0$ and $\delta \in T = F[[x_1, \ldots, x_n]]$. If $\delta \mathrel{\underset{T}{|}} f$ and $\delta \mathrel{\underset{T}{|}} g$, then there exists $\varepsilon \in U(T)$ such that*

$$\varepsilon\delta \in S, \quad \varepsilon\delta \mathrel{\underset{S}{|}} f, \quad \varepsilon\delta \mathrel{\underset{S}{|}} g.$$

Proof. There exist $\alpha, \beta \in T^*$ with $\alpha\delta = f$ and $\beta\delta = g$. Let

$$\delta = \sum_{j=1}^{J} t_j\delta_j, \quad \alpha = \sum_{k=1}^{K} u_k\alpha_k, \quad \beta = \sum_{l=1}^{L} v_l\beta_l,$$

where $J, K, L \in \mathbb{N}$, $t_j, u_k, v_l \in F^*$ for each $1 \leqslant j \leqslant J$, $1 \leqslant k \leqslant K$, $1 \leqslant l \leqslant L$, and $\delta_1, \dots, \delta_J$ are different monomials in T, $\alpha_1, \dots, \alpha_K$ are different monomials in T, and $\beta_1, \dots, \beta_L$ are also different monomials in T. Let

$$\delta_j = \prod_{\nu=1}^{n} x_\nu^{d(j,\nu)}, \quad \alpha_k = \prod_{\nu=1}^{n} x_\nu^{a(k,\nu)}, \quad \beta_l = \prod_{\nu=1}^{n} x_\nu^{b(l,\nu)}$$

where $d(j,\nu)$, $a(k,\nu)$, $b(l,\nu) \in \mathbb{Q}$, $1 \leqslant j \leqslant J$, $1 \leqslant k \leqslant K$, $1 \leqslant l \leqslant L$, $1 \leqslant \nu \leqslant n$.

Suppose now that $1 \leqslant \nu \leqslant n$ is fixed and the monomials in T are lexicographically ordered under the assumption $x_\nu > x_\mu$ for each $1 \leqslant \mu \leqslant n$, $\mu \neq \nu$. Let $d(\nu)$ be the exponent of x_ν in the lowest term $\mathrm{lt}(\delta)$ in the generalized polynomial δ. Then

$$d(\nu) \leqslant d(j,\nu) \quad \text{for each } 1 \leqslant j \leqslant J. \tag{5}$$

By Proposition 4.2, $\mathrm{lt}(f) = \mathrm{lt}(\alpha) \cdot \mathrm{lt}(\delta)$, therefore the exponent of x_ν in $\mathrm{lt}(f)$ is less than or equal to $d(\nu) + a(k,\nu)$ for each $1 \leqslant k \leqslant K$. Consequently, $(f \in S)$

$$0 \leqslant d(\nu) + a(k,\nu) \quad \text{for each } 1 \leqslant k \leqslant K. \tag{6}$$

Analogously

$$0 \leqslant d(\nu) + b(l,\nu) \quad \text{for each } 1 \leqslant l \leqslant L. \tag{7}$$

Put $\varepsilon = \prod\limits_{\nu=1}^{n} x_\nu^{-d(\nu)}$. Summarizing (5), (6), (7), and 4.3 we have $\varepsilon \in U(T)$ and

$$\begin{aligned}
\varepsilon\delta_j &= \prod_{\nu=1}^{n} x_\nu^{d(j,\nu)-d(\nu)} \in S \quad \text{for each } 1 \leqslant j \leqslant J,\\
\varepsilon^{-1}\alpha_k &= \prod_{\nu=1}^{n} x_\nu^{d(\nu)+a(k,\nu)} \in S \quad \text{for each } 1 \leqslant k \leqslant K,\\
\varepsilon^{-1}\beta_l &= \prod_{\nu=1}^{n} x_\nu^{d(\nu)+b(l,\nu)} \in S \quad \text{for each } 1 \leqslant l \leqslant L,
\end{aligned}$$

which implies $\varepsilon\delta \in S$, $\varepsilon^{-1}\alpha \in S$, $\varepsilon^{-1}\beta \in S$. Since $(\varepsilon\delta)(\varepsilon^{-1}\alpha) = f$ and $(\varepsilon\delta)(\varepsilon^{-1}\beta) = g$, we get $\varepsilon\delta \underset{S}{|} f$ and $\varepsilon\delta \underset{S}{|} g$, which is what we wanted to prove. $\square$

Before stating and proving the GCD-Existence Theorem for the integral domain $T = F[[x_1, \dots, x_n]]$, we prove a general theorem for rings satisfying the property given in Proposition 4.4.

Theorem 4.5. *Let $\mathcal{S}$ be a subring of an integral domain $\mathcal{T}$ and let, for any $f, g \in \mathcal{S}^*$, $\delta \in \mathcal{T}$, the following implication be valid:*

$$\delta \underset{\mathcal{T}}{|} f,\ \delta \underset{\mathcal{T}}{|} g \Rightarrow \exists\, \varepsilon \in U(\mathcal{T}) \text{ such that } \varepsilon\delta \underset{\mathcal{S}}{|} f,\ \varepsilon\delta \underset{\mathcal{S}}{|} g.$$

Then we have

$$\text{if } l, h \in \mathcal{S} \text{ and } d = (l,h)_{\mathcal{S}},\ \text{ then } d = (l,h)_{\mathcal{T}}.$$

P r o o f. Assume that $l, h \in \mathcal{S}^*$ and $d = (l,h)_{\mathcal{S}}$. Since $d \underset{\mathcal{S}}{|} l$, $d \underset{\mathcal{S}}{|} h$, we see that $d \underset{\mathcal{T}}{|} l$, $d \underset{\mathcal{T}}{|} h$ as well.

Let $\delta \in \mathcal{T}$, $\delta \underset{\mathcal{T}}{|} l$ and $\delta \underset{\mathcal{T}}{|} h$. By the assumption of the Theorem, there exists $\varepsilon \in U(\mathcal{T})$ such that $\varepsilon\delta \in \mathcal{S}$, $\varepsilon\delta \underset{\mathcal{S}}{|} l$ and $\varepsilon\delta \underset{\mathcal{S}}{|} h$. This yields $\varepsilon\delta \underset{\mathcal{S}}{|} d$, thus $d = (l,h)_{\mathcal{T}}$ and we are done. □

Theorem 4.6. *In the integral domain $T = F[[x_1, \ldots, x_n]]$, each pair of elements has a greatest common divisor.*

If $f, g \in T$ and $\eta \in U(T)$ with $\eta f, \eta g \in S = F[[x_1, \ldots, x_n]]^+$, then $(f,g)_T = (\eta f, \eta g)_S$.

P r o o f. Let $f, g \in T$ and let $\eta \in U(T)$ with $\eta f, \eta g \in S$ (obviously such η exists). By Theorem 3.4, there exists a greatest common divisor d of ηf, ηg in S.

Setting $\mathcal{S} = S$ and $\mathcal{T} = T$ and applying Theorem 4.5 (the assumption of Theorem 4.5 is valid by Proposition 4.4), we obtain $d = (\eta f, \eta g)_T$. Thus $d = (f,g)_T$. This completes the proof. □

References

[1] *J. Karásek, J. Šlapal*: Polynomials and Generalized Polynomials for the Theory of Control. Special Monograph. Academic Publishing House CERM, Brno, 2007. (In Czech.)

[2] *W. K. Nicholson*: Introduction to Abstract Algebra. PWS-KENT Publishing Company, Boston, 1993.

[3] *K. B. Oldham, J. Spanier*: The Fractional Calculus. Theory and Applications of Differentiation and Integration to Arbitrary. Academic Press, New York, 1974.

[4] *L. Skula*: Realization and GCD-Existence Theorem for generalized polynomials. In preparation.

[5] *O. Zariski, P. Samuel*: Commutative Algebra, Vol. 1. D. van Nostrand Company, Princeton-Toronto-New York-London, 1958.

Author's address: L. S k u l a, Institute of Mathematics, Faculty of Mechanical Engineering, University of Technology, Technická 2, 616 69 Brno, Czech Republic, e-mail: `skula@fme.vutbr.cz`.